НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
«ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»

ІТ-ПРАВО ПІД ЧАС ГІБРИДНОЇ ВІЙНИ: ВІД ПОШУКУ ПАРАДИГМИ ДО ПРАГМАТИЧНИХ РІШЕНЬ

Колективна монографія

За редакцією
Є. Харитонова, О. Харитонової, І. Давидової

Одеса
Фенікс
2025

УДК 340:004:327:355
І-87

Рекомендовано рішенням вченої ради
Національного університету «Одеська юридична академія»
(протокол № 9 від 30 червня 2025 р.)

Рецензенти:

Майданик Р. А. – академік НАПрН України, доктор юридичних наук, професор, професор кафедри цивільного процесу Навчально-наукового інституту права Київського національного університету імені Тараса Шевченка;

Соколов А. В. – доктор технічних наук, професор, професор кафедри кібербезпеки Національного університету «Одеська юридична академія»;

Маковій В. П. – кандидат юридичних наук, професор, завідувач кафедри цивільно-правових дисциплін Одеського державного університету внутрішніх справ.

І-87 **ІТ-право під час гібридної війни: від пошуку парадигми до прагматичних рішень** : кол. монографія / за заг. ред. проф.: Є. Харитонова, О. Харитонової, І. Давидової. – Одеса : Фенікс, 2025. – 588 с.
ISBN 978-617-8430-70-2

Монографія є продовженням циклу праць колективу кафедри цивільного права Національного університету «Одеська юридична академія», присвячених результатам досліджень цивілістичних шкіл університету від часу їхнього формування до гібридної війни, що триває нині. У третьому томі аналізуються в контексті гібридної війни: проблеми визначення концепту «ІТ-право», особливості правового регулювання відносин, що виникають у зв'язку з використанням інформаційних технологій, особливості механізму цивільно-правового регулювання у сфері ІТ, чинник симулякру, значення та роль інформаційного середовища як стратегічного ресурсу, правові рамки для цифрових активів і перспективи цифрової власності, ІТ-правочини, порушення прав інтелектуальної власності в Інтернет, протидія кіберзагрозам у гібридній кібервійні, загрози вербування неповнолітніх через соцмережі та месенджери та юридичні заходи запобігання таким загрозам, правове регулювання стартапів, е-кредитування, цивільно-правова відповідальність за шкоду, завдану кібератаками, забезпечення інформаційної безпеки електронного судочинства в умовах гібридної війни в Україні та ін.

Авторський колектив концентрував увагу на обґрунтуванні необхідності комплексного вирішення практичних питань впорядкування інформаційно-технологічні відносини в умовах гібридної російсько-української війни. Автори прагнули розкрити особливості правового регулювання цих відносин і запропонувати власне бачення шляхів вирішення проблем, що виникають у цій сфері. Усвідомлюючи спірність низки висновків і пропозицій, автори розраховують на продовження плідних дискусій з проблем правового регулювання інформаційних технологій, зокрема в умовах гібридної війни.

Монографія може бути цікавою науковцям, практикуючим юристам, викладачам, аспірантам, здобувачам вищої освіти, а також широкому загалу небайдужих українців, які цікавляться проблемами правового регулювання у сфері ІТ, зокрема під час гібридної війни.

УДК 340:004:327:355

ISBN 978-617-8430-70-2

© Колектив авторів, 2025

ЗМІСТ

Авторський колектив 5

Розділ 1. Прагматична (соціологічна) школа «ІТ-права» –
відповідь цивілістики на виклики інформаційного суспільства
(Євген Харитонов, Олена Харитонова, Ірина Давидова) 7

Розділ 2. Концепт ІТ-права
(Євген Харитонов, Олена Харитонова). 30

Розділ 3. Гібридна інформаційна війна та інформаційні технології
(Євген Харитонов, Олена Харитонова). 65

Розділ 4. ШІ як бінарна категорія ІТ
(Євген Харитонов, Олена Харитонова). 93

Розділ 5. Симулякр, гібридна (інформаційна) війна і потенціал ІТ
(Євген Харитонов, Олена Харитонова). 119

Розділ 6. Інформаційне середовище як стратегічний ресурс
у гібридних конфліктах (Оксана Калітенко) 143

Розділ 7. Правові рамки для цифрових активів: перспективи
цифрової власності (Катерина Некіт) 175

Розділ 8. Захист немайнових прав у медіапросторі в період гібридної війни
(Алла Кирилюк, Лариса Галупова) 203

Розділ 9. ІТ-правочини в умовах гібридної війни (Ірина Давидова) 250

Розділ 10. Порушення прав інтелектуальної власності в мережі інтернет
під час гібрідної агресії в умовах воєнного стану (Наталія Бааджи). 279

Розділ 11. Кіберзагрози у гібридній кібервійні: дія і протидія
(Євген Харитонов, Олена Харитонова). 323

Розділ 12. Етико-юридичні аспекти використання штучного інтелекту
в мережі інтернет в умовах гібридної війни (Олександр Омельчук). 351

Розділ 13. Застосування систем автоматизованого прийняття рішень
під час збройного конфлікту (Віра Токарева). 378

Розділ 14. Гібридна війна і кіберзброя
(Євген Харитонов, Олена Харитонова) 388

Розділ 15. Вербування неповнолітніх через соцмережі та месенджери
в умовах гібридної війни: загрози, механізми та заходи запобігання
(Вікторія Рябченко) 420

Розділ 16. Правове регулювання діяльності стартапів в умовах гібридної війни:
виклики, можливості та перспективи (Дмитро Розумейко) 435

Розділ 17. Е-кредитування у період воєнного стану
(Олена Берназ-Лукавецька) 453

Розділ 18. Цивільно-правова відповідальність за шкоду, завдану кібератаками
(Богдан Фасій) 483

Розділ 19. Сімейні правовідносини в сфері інформаційних технологій
в умовах гібридної війни (Оксана Сафончик) 514

Розділ 20. Забезпечення інформаційної безпеки електронного судочинства
в умовах гібридної війни в Україні (Крістіна Дрогозюк) 545

Розділ 21. Кіберспортивна дипломатія: перспективи для України
(Максим Ткалич, Юлія Толмачевська) 557

Список основних праць представників школи 565

Авторський колектив

Харитонов Євген (ORCID ID: 0000-0001-5521-0839), доктор юридичних наук, професор, член-кореспондент НАПрН України, зав. кафедри цивільного права НУ «ОЮА»: розділ 1 (у співав. з О. Харитоновою, І. Давидовою); розділ 2 (у співав. з О. Харитоновою); розділ 3 (у співав. з О. Харитоновою); розділ 4 (у співав. з О. Харитоновою); розділ 5 (у співав. з О. Харитоновою); розділ 11 (у співав. з О. Харитоновою); розділ 14 (у співав. з О. Харитоновою);

Харитонова Олена (ORCID ID: 0000-0002-9681-9605), докторка юридичних наук, професорка, членкиня-кореспондент НАПрН України, зав. кафедри права інтелектуальної власності і патентної юстиції НУ «ОЮА»: розділ 1 (у співав. з Є. Харитоновим, І. Давидовою); розділ 2 (у співав. з Є. Харитоновим); розділ 3 (у співав. з Є. Харитоновим); розділ 4 (у співав. з Є. Харитоновим); розділ 5 (у співав. з Є. Харитоновим); розділ 11 (у співав. з Є. Харитоновим); розділ 14 (у співав. з Є. Харитоновим);

Давидова Ірина (ORCID ID: 0000-0001-5622-671X), докторка юридичних наук, професорка, професорка кафедри цивільного права НУ «ОЮА»: розділ 1 (у співав. з Є. Харитоновим, О. Харитоновою); розділ 9;

Некіт Катерина (ORCID ID: 0000-0002-3540-350X), докторка юридичних наук, професорка, професорка кафедри цивільного права НУ «ОЮА»: розділ 7;

Сафончик Оксана (ORCID ID: 0000-0001-6781-8219), докторка юридичних наук, професорка, професорка кафедри цивільного права НУ «ОЮА»: розділ 19;

Бааджи Наталія (ORCID ID: 0000-0002-9889-4879), кандидатка юридичних наук, доцента, доцентка кафедри права інтелектуальної власності та патентної юстиції НУ «ОЮА»: розділ 10;

Берназ-Лукавецька Олена (ORCID ID: 0000-0002-2133-1672), кандидатка юридичних наук, доцента, доцентка кафедри цивільного права НУ «ОЮА»: розділ 17;

Галупова Лариса (ORCID ID: 0000-0001-6263-2773), кандидатка юридичних наук, доцентка кафедри права інтелектуальної власності та патентної юстиції НУ «ОЮА»: розділ 8 (у співав. з А. Кирилюк);

Дрогозюк Крістіна (ORCID ID: 0000-0001-9254-9575), кандидатка юридичних наук, доцента, доцентка кафедри цивільного, нотаріального та виконавчого процесу НУ «ОЮА»: розділ 20;

Калітенко Оксана (ORCID ID: 0000-0003-1001-3561)**,** кандидатка юридичних наук, доцентка, професорка кафедри цивільного права НУ «ОЮА»: розділ 6;

Кирилюк Алла (ORCID ID: 0000-0002-3051-6599), кандидатка юридичних наук, доцентка, доцентка кафедри права інтелектуальної власності та патентної юстиції НУ «ОЮА»: розділ 8 (у співав. з Л. Галуповою);

Омельчук Олександр (ORCID ID: 0000-0002-0082-3619), кандидат юридичних наук, доцент, доцент кафедри цивільного права НУ «ОЮА»: розділ 12;

Ткалич Максим (ORCID ID: 0000-0003-4224-7231), кандидат юридичних наук, доцент, доцент кафедри цивільного права Запорізького національного університету: розділ 21 (у співав. з Ю. Толмачевською);

Токарева Віра (ORCID ID: 0000-0002-8409-1477), кандидатка юридичних наук, доцентка, доцентка кафедри цивільного права НУ «ОЮА»: розділ 13;

Толмачевська Юлія (ORCID ID: 0000-0002-7964-8875), докторка філософії (081 право): розділ 21 (у співав. з О. Ткаличем);

Фасій Богдан (ORCID ID: 0000-0002-8715-930X), кандидат юридичних наук, доцент, декан факультету судового та міжнародного права НУ «ОЮА»: розділ 18;

Розумейко Дмитро (ORCID ID: 0000-0001-8206-1031)**,** аспірант кафедри цивільного права НУ «ОЮА»: розділ 16;

Рябченко Вікторія (ORCID ID: 0009-0007-1542-6492)**,** аспірантка кафедри цивільного права НУ «ОЮА»: розділ 15.

Розділ 1

ПРАГМАТИЧНА (СОЦІОЛОГІЧНА) ШКОЛА «ІТ-ПРАВА» – ВІДПОВІДЬ ЦИВІЛІСТИКИ НА ВИКЛИКИ ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА

DOI

Євген Харитонов
доктор юридичних наук, професор,
член-кореспондент НАПрН України

Олена Харитонова
докторка юридичних наук, професорка,
членкиня-кореспондент НАПрН України

Ірина Давидова
докторка юридичних наук, професорка

Попередні зауваження

Технічний прогрес, в основі якого беззаперечно є результати інтелектуальної діяльності, в свою чергу створює нові можливості для розширення сфер і способів використання об'єктів права (права інтелектуальної власності, цивільного права), вираження їх у нових формах, зокрема цифровій. Позитивною рисою цифрової форми є не лише спрощення тиражування та розповсюдження об'єктів інтелектуальної власності на матеріальних носіях, а й створення умов для їх передачі в електронних мережах. Розміщення об'єктів права інтелектуальної власності у Всесвітній мережі Інтернет наразі стало чи не найбільш використовуваним способом їх поширення. У зв'язку з цим дослідження правових проблем, пов'язаних із використанням інформаційних технологій, набуває усе більшої актуальності.

Природно, що зазначенні питання привертають увагу вітчизняних правознавців, і передусім, цивілістів, фахівців у галузі інформаційного права, прав інтелектуальної власності (Т. В. Бачинський, О. О. Баранов, О. Е. Сімсон, Є. О. Харитонов, О. І. Харитонова, О. С. Явор-

ська). Обговорювалися вони й на конференціях, присвячених проблемам ІТ-права.[1] Разом із тим, поки що не розглядалися питання формування та розвитку вітчизняних шкіл ІТ-права, хоча з публікацій та матеріалів наукових конференцій виразно помітне існування розбіжностей у підходах до розуміння його основних категорій у провідних юридичних вищих навчальних закладах України.

Метою цього розділу є визначення особливостей Одеської школи ІТ-права, сформованої на базі кафедр цивільного права і права інтелектуальної власності та патентної юстиції Національного університету «Одеська юридична академія».

І Етап. Початок формування школи. Сьогодні, навряд чи, знайдеться суб'єкт суспільних відносин, який у своїй діяльності так чи інакше не використовував би інформаційні технології, об'єкти інтелектуальної власності тощо. Попит на «нематеріальний товар» з кожним днем дедалі зростає. Це значною мірою пов'язане з формуванням інформаційного суспільства, осторонь якого не може залишитися й Україна. Інформаційне суспільство – це суспільство, яке створюється внаслідок нової індустріальної революції на базі інформаційних і телекомунікаційних технологій та на базі інформації, яка є виразником знання людей. Завдяки технологічному прогресу в такому суспільстві оброблення, накопичення, отримання і обмін інформацією в будь якій її формі – звуковій, письмовій або візуальній – не обмежені за відстанню, часом і обсягами. Ця революція додає великих можливостей людському інтелекту і створює ресурси, що змінюють спосіб суспільної праці і суспільного життя [2]. Вважається, що в «інформаційному суспільстві» створення, розповсюдження, використання,

[1] Захист права інтелектуальної власності у мережі Інтернет: теоретичні та практичні аспекти: матеріали Інтернет-конференції (Одеса, 22 травня 2015 р.). Одеса: Юридична література, 2015; ІТ право: проблеми і перспективи розвитку в Україні: зб. матер. наук.-практ. конф. (м. Львів, 18 лист. 2016 р.). Львів: Львівська політехніка, 2016. 396 с.; Правове регулювання ІТ-відносин: матер.всеукр. кругл. столу (м. Одеса, 18 травня 2017 р.). Одеса: Фенікс, 2017; ІТ-право: проблеми і перспективи розвитку в Україні: збірник матеріалів ІІ науково-практичної конференції (Львів, 17 листопада 2017 р.). Львів: Львівська політехніка, 2017. 318 с.

[2] Європа та Глобальне інформаційне суспільство. Рекомендації Європейській раді. Брюссель, 26 травня 1994 р. (Europe and the Global Information Society. Recommendations to European Council. Brussels, 26 May 1994). В зб. «Європа на шляху до інформаційного суспільства. Матеріали Європейської Комісії 1994-1995 рр. Київ, Державний комітет зв'язку та інформатизації України. Вид. «Зв'язок», 2000.

узагальнення і маніпулювання інформацією становить значну частину економічної, політичної та культурної діяльності. Економіка знань стає економічною копією цієї діяльності, оскільки добробут суспільства створюється через експлуатацію знань або розуміння суті речей та процесів. Люди які мають засоби і можливості для участі в такому суспільстві, отримують певні додаткові вигоди, порівняно з тими, хто таких можливостей або засобів не має. «Інформаційне суспільство» вважається наступником «індустріального суспільства», через що його часто називають суспільством «постіндустріальним».

Оскільки інформація тісно пов'язана з правом інтелектуальної власності, дослідження проблем останнього належить до найактуальніших завдань сучасного правознавства. Однією з перших на Півдні України до розгляду згаданих проблем звернулися кафедра права інтелектуальної власності та корпоративного права НУ «ОЮА» (тепер – кафедра права інтелектуальної власності та патентної юстиції) і кафедра цивільного права НУ «ОЮА», колективи яких більш ніж десять років тому почали дослідження теоретичних та практичних проблем охорони та захисту права інтелектуальної власності в Інтернеті. Ще з 2012 р. предметом наукових досліджень співробітників кафедри стали проблеми, пов'язані із питаннями права на інформацію в електронному вигляді, встановлення її змісту, свободи її поширення тощо; інформаційної безпеки; правової природи мережі, сутності інтернет-відносин, Інтернет-права; укладення електронних угод; неправомірної поведінки користувачів Інтернету (несанкціонований доступ, порушення норм суспільної моралі тощо; охороноздатності розміщених в Інтернеті матеріалів; передачі та захисту авторських прав при копіюванні; захисту авторських та суміжних прав при діяльності електронних видавництв; захисту прав на комп'ютерні програми тощо).

Однією з проблем теоретичного характеру, що потребували вирішення, було визначення правової природи Всесвітньої мережі, правовідносин, що виникають, кола учасників, їх специфіки, змісту тощо. Відносини, що виникають у Інтернеті, мають специфіку, яка зумовлена віртуальним простором, його міжнародним, транскордонним, децентралізованим характером. Цей простір має власні правила функціонування, мову, мережеву культуру. Інформація передається у мережі Інтернет переважно у вигляді творів, які підлягають охороні авторським правом будь-якої з країн Бернського Союзу нарів-

ні з творами, закріпленими в більш традиційних формах, за умови відповідності встановленим законодавством країни критеріям охорони, незалежно від виконання яких-небудь формальностей та факту опублікування. Власники авторських прав стикаються зі значними ризиками, обумовленими існуванням інформаційних технологій. Транскордонний характер Інтернету та цифрова форма фіксації розміщених в ньому творів значно ускладнюють здійснення авторами та їх правонаступниками своїх прав.

Щодо Інтернету, як правової категорії, в юридичній доктрині досі немає єдиного розуміння його правової природи – як об'єкта права чи суб'єкта права, об'єкта чи предмету правового регулювання, що зумовило дослідження відповідної проблематики колективом кафедри.[1] Проведене комплексне дослідження доктринальних підходів до визначення поняття категорій «Інтернет», «Інтернет відносини», правових засад їх регулювання, в межах якого отримані результати, що вирізняються науковою новизною. Було запропоноване авторське визначення категорії «Інтернет» як глобальної загальнодоступної інформаційно-телекомунікаційної мережі зі складною багаторівневою інфраструктурою, що функціонує на засадах транскордонного управління та надає можливості для створення, розміщення інформації та доступу до неї, а також надання пов'язаних з цим інформаційних послуг.

Поступово формується розуміння Інтернет-відносин, як відносин, що виникають між користувачами всесвітньої інформаційної мережі.[2] Під час проведеного науковцями кафедри права інтелектуаль-

[1] Харитонова О. І., Позова Д. Д. До проблеми визначення правової природи мережі Інтернет. *Вісник Південного регіонального центру Національної академії правових наук України.* 2015. № 4. С. 80-89; Кирилюк А. В. Юридична природа мережі Інтернет: історія створення, будова та можливості. *Часопис цивілістики.* 2014. Вип. 17. С. 204-209, та ін.

[2] Харитонова О. І. До питання про коректність вживання терміно-поняття «Інтернет-відносини». *«Римське право і сучасність» (Шерешевські читання):* матеріали Міжнародної наукової конференції. Частина І. (11 травня 2012 року. м. Одеса). Одеса: Говерла. С. 111-112; Харитонова О. І. До проблеми визначення суб'єктного складу відносин у мережі Інтернет. *Проблеми вдосконалення цивільного законодавства України:* матеріали Круглого столу (12 травня 2012 року, м. Одеса). Одеса: Фенікс, 2012. С.143-145; Харитонова О. І. Специфіка регулювання відносин у всесвітній мережі Інтернет: до проблемні питання. *Римське право і сучасність*: матер. Міжнар. наук. конф. (Одеса, 29 травня 2015 р.). Одеса: Фенікс, 2015. С. 90-91; Харитонова О. І., Харитонов Є. О. «Інтернет-відносини» – віртуальна нереальність. *Від засад римського права до принципів приватного права ЄС:* матер. круглого столу (м. Одеса, 29 травня 2015 р.). Одеса: Фенікс, 2015. 27-30; Позова Д. Д. Особливості правовідносин у мережі Інтернет. *Часопис цивілістики.* 2015. № 20; Харитонова О. І., Ульянова Г. О., Кирилюк А. В.,

ної власності комплексного дослідження було розкрите поняття та особливості таких відносин, співвідношення відносин, які виникають в Інтернеті та правовідносин інтелектуальної власності; визначені особливості суб'єктного складу відносин, які виникають в Інтернеті. Встановлено, що поняття Інтернет-відносин не є коректним, а має йтися про відносини у Інтернеті, оскільки відносини, що складаються у Мережі, існують паралельно з реальними відносинами, водночас співпадаючи з останніми за змістом. Таким чином, віртуальні відносини можна класифікувати за предметним критерієм так само, як і відносини реальні. Тут виникають правовідносини різної галузевої приналежності. Так, у цифровому середовищі можуть виникати цивільно-правові відносини, адміністративно-правові відносини, фінансово-правові відносини тощо. За межами відносин, що виникають у цифровому середовищі, залишаються відносини, що виникають при порушенні прав і обов'язків у Мережі – відносини цивільної, адміністративної відповідальності, карної відповідальності.

На підставі проведеного дослідження об'єктів права інтелектуальної власності, які поширюються, використовуються в Інтернеті[1], виділено новий критерій для їх класифікації: цільове призначення результатів інтелектуальної власності, на підставі якої останні розділяються на дві категорії: об'єкти, які створюються з метою забезпечення функціонування мережі Інтернет, інші об'єкти, які поширюються в мережі. Досліджено об'єкти, які забезпечують функціонування Інтернету. До таких об'єктів відносять веб-сайти та доменні імена, особливість яких полягає в тому, що вони забезпечують можливість розміщення інформації в Мережі. Не менш важливе значення для забезпечення поширення інформації в Мережі, у тому числі й об'єктів прав інтелектуальної власності, мають і комп'ютерні програми. Спе-

Симонян Ю. Ю., Бааджи Н. П., Позова Д. Д., Григор'янц Г. І., Бурова Л. І., Мартинюк І. В. Проблемні питання визначення правової природи і структури правовідносин інтелектуальної власності, що виникають у мережі Інтернет. *Наукові праці Національного університету «Одеська юридична академія».* 2015. Вип.17; Еннан Р. Є. Поняття, ознаки, сутність, специфіка та види відносин у мережі Інтернет. *Теорія і практика інтелектуальної власності.* 2013. № 3. С. 10-19.

[1] Харитонова О. І. Категорії «інформація» та «об'єкт авторських прав»: до проблеми співвідношення. *Традиції та новації юридично минуле, сучасність, майбутнє*: Матеріали міжнародної науково-практичної конференції (м. Одеса, 19 травня 2017 р.); Кирилюк А. В. Особливості розміщених в Інтернеті творів як предмета авторського права. *Часопис цивілістики.* 2012. Вип. 13. С.120-123.

цифіка кожного із зазначених об'єктів права інтелектуальної власності зумовлює необхідність вироблення спеціальних умов їх охорони та правил використання.[1]

Запропонована також класифікацію результатів інтелектуальної, творчої діяльності, які використовуються в Інтернеті; визначено статус Інтернет-провайдерів, як спеціального учасника відносин, що виникають в Інтернеті[2]; розкрито особливість захисту авторських прав залежно від категорії сайтів, на яких вони розміщені (платні або безоплатні сайти).

Спеціальним напрямком досліджень проблем, пов'язаних з широким використанням інформаційних технологій, стало дослідження захисту прав інтелектуальної власності в Інтернеті від піратства, плагіату та інших порушень.[3] Крім поширеного підходу до піратства

---

[1] Кирилюк А. В. Різновиди сайтів. *Priority a strategie pre rozvoj pravnej vedy vo svete vedy.* Zbornik prispevkov z medzinarodna vedecko-prakticka konferencia (28-29 oktobra 2016) Sefredaktor: prof. JUDr. Stanislav Mraz, CSc. – Vysoka skola Danubius, Sladkovicovo; Бааджи Н. П. Доменне ім'я як об'єкт права інтелектуальної власності. *Правове життя сучасної України*: Матеріали Міжнародної науково-практичної конференції (16-17 травня 2013 р.). Т. 2. С. 669-672; Симонян Ю. Ю. Удосконалення правової охорони комп'ютерних програм і баз даних. *Правове життя сучасної України:* Матеріали Міжнародної науково-практичної конференції, присвяченої ювілею академіка С. В. Ківалова (16-17 травня 2014 р., м. Одеса). у 2 т. Т.1. Одеса: Юридична література, 2014. С.493-496 та ін.

[2] Кирилюк А. В. Провайдери як учасники інформаційних відносин. *Верховенство права та правова держава*: Матеріали міжнародної науково-практичної конференції (м. Ужгород, 16-17 жовтня 2015 р.). Ужгород: Ужгородський національний університет, 2015. С. 151-153; Бурова Л. І. Відповідальність Інтернет провайдерів за порушення прав на результати інтелектуальної діяльності в мережі Інтернет. *Сучасний розвиток державотворення та правотворення в Україні: проблеми теорії та практики:* III Всеукраїнська науково-практична конференція (11 березня 2011 р., м. Маріуполь). С. 174-176; Кулініч О. О. Порушення прав та інтересів фізичних осіб при проведенні зйомки у режимі он-лайн за допомогою Всесвітньої мережі Інтернет. *Римське право і сучасність*: матеріали Міжнародної наукової конференції (11 травня 2012 р., м. Одеса), 2012. С. 120-121.

[3] Харитонова О. І. Проблемні питання порушення авторських прав у Всесвітній мережі Інтернет. *Правове життя сучасної України:* матер. Міжнар. наук.-практ. конф. (16-17 травня 2013 р.). Т.2. Одеса: Фенікс, 2013. С.652-654; Харитонова О. І. Піратство у всесвітній мережі Інтернет. *Правові та інституційні механізми забезпечення сталого розвитку України*: матеріали Міжнародної науково-практичної конференції (15-16 травня 2015 р., м. Одеса): у 2 т. Т.2. Одеса: Юридична література, 2015. С. 507-509; Симонян Ю. Ю. Проблеми комп'ютерного піратства в Україні. *Правове життя сучасної України:* мат. Міжнар. наук. конф. проф.-викл. складу 20-21 квітня 2012 р. Одеса, 2012. С. 184-186; Кирилюк А. В. Деякі аспекти захисту авторських прав в мережі Інтернет. *Актуальні проблеми цивільного, житлового та сімейного законодавства: матеріали міжнар.* Наук.-практ. конф., присвяч. 90-річчю з дня народження д-ра юрид. наук, проф. В. П. Маслова (16 березня 2012 р.). Х.: Право, 2012. С. 166-169.

як суто негативного явища, досліджено також ставлення до поширення піратської продукції в Мережі з позиції споживачів такої продукції.[1] Визначені основні напрями, цілі створення та діяльності піратських партій, як спеціальних учасників відносин, які виникають в мережі Інтернет. Підготована та захищена кандидатська дисертація Грігор'янц Г. І. «Піратство як порушення авторських і суміжних прав в мережі Інтернет».[2]

Результатом дослідження питань порушення прав інтелектуальної власності від плагіату, зокрема, в Мережі, став захист докторської дисертації Г. О. Ульянової «Методологічні проблеми цивільно-правового захисту прав інтелектуальної власності від плагіату».[3]

Крім того, були розроблені пропозиції до проєкту Закону «Про внесення змін до деяких законодавчих актів щодо захисту авторського права і суміжних прав у мережі Інтернет» щодо удосконалення захисту авторських та суміжних прав в Мережі. Результати науково-дослідної роботи були представлені на науково-практичних конференціях, а також викладені в монографіях, підручниках та більш ніж 400 наукових публікаціях.[4]

Досліджувалися також інші питання, пов'язані із застосуванням ІТ, зокрема, електронна комерція, електронні бібліотеки, електронний документообіг та ін.[5]

---

[1] Грігор'янц Г. І. Деякі проблемні питання захисту об'єктів авторського права в мережі Інтернет. *Юридичний науковий електронний журнал.* 2015. № 4. С. 68-70.

[2] Грігор'янц Г. І. Піратство як порушення авторських і суміжних прав в мережі Інтернет: дис. … канд. юрид. наук: 12.00.03. Одеса, 2016. 195 с.

[3] Ульянова Г. О. Методологічні проблеми цивільно-правового захисту прав інтелектуальної власності від плагіату: дис. … д-ра. юрид. наук: 12.00.03. Одеса, 2015. 433 с.

[4] Опис див.: у Списку публікацій представників Школи, вміщеному у Додатку до цієї монографії

[5] Правове регулювання використання зображень у електронних бібліотеках за законодавством України: монографія/ О. І. Харитонова, О. О. Кулініч, С. В. Мазуренко, І. В. Менсо. Одеса: Юридична література, 2017. 72 с.; Менсо І. В. Правові аспекти створення електронних бібліотек. *Матеріали міжнародної науково-практичної конференції* (16-17 травня 2014 року). Одеса: Юридична література, 2014 р. Том І. С. 510-512; Бааджи Н. П. Цифровий ідентифікатор DOI як дієвий спосіб захисту авторського права і суміжних прав у цифровому середовищі. *Актуальні проблеми політики.* 2015. Вип. 55. С. 267-274; Еннан Р. Є. Електронний (мережевий) договір: поняття, ознаки, види, порядок укладання. *Цивільний кодекс України: досвід 10 років застосування:* матеріали Всеукраїнської наукової конференції «Цивілістичні читання, присвячені пам'яті професора І. В. Шерешевського (м. Одеса, 6 грудня 2013 р.). Одеса: Фенікс, 2013. С. 114-116.

На підставі аналізу проекту Закону України «Про електронну комерцію», прийнятого постановою Верховної Ради України від 3 червня 2014 р. за основу, обґрунтовано доцільність закріплення в майбутньому законі положень щодо дотримання прав інтелектуальної власності під час виготовлення та (або) розповсюдження, зберігання, перевезення, перетинання митного кордону України відповідного товару як умову належного виконання своїх зобов'язань продавцем (виконавцем, постачальником) товарів, робіт, послуг в електронній комерції.

Новий період формування Одеської школи ІТ-права, який можна вважати етапом зростання її цивілістичної концептуальної складової почався після участі правознавців НУ «ОЮА» у всеукраїнській конференції з проблем і перспектив розвитку ІТ-права в Україні, яка відбулася у Львові в листопаді 2016 р.[1]

Після дискусій на згаданій конференції та за її матеріалами настала доба теоретичного осмислення і систематизації досліджень викликів, які постали перед приватним правом і цивілістикою у зв'язку із широким впровадженням ІТ у повсякденне життя.

У 2017 році О. О. Кулініч захищає докторську дисертацію «Теоретичні проблеми реалізації та захисту права фізичної особи на власне зображення»,[2] у якій піддає аналізу також і відповідні правовідносини у Мережі.

Починають досліджуватися проблеми ІТ-права, інформаційної безпеки тощо[3]. Вивчаються проблеми віртуальної власності, резуль-

---

[1] ІТ право: проблеми і перспективи розвитку в Україні: зб. матер. наук.-практ. конф. (м. Львів, 18 лист. 2016 р.). Львів: Львівська політехніка, 2016. 396 с.

[2] Кулініч О. О. Теоретичні проблеми реалізації та захисту права фізичної особи на власне зображення: автореф. дис. … д-ра. юрид. наук: 12.00.03. Одеса, 2017. 40 с.

[3] Харитонова О. І. Проблемні питання визначення системи (структури) ІТ-права. *ІТ-право: проблеми і перспективи розвитку в Україні*: збірник матеріалів науково-практичної конференції.(м. Львів, 18 листопада 2016 р.); Харитонова О. І. Інформаційно-комунікаційні технології і деякі проблеми авторського права. *Правове регулювання ІТ-відносин:* матеріали міжнародної науково-практичної конференції (м. Одеса, 18 трав. 2017 р.); Грігор'янц Г. І. ІТ-піратство та інформаційна безпека. *Правове регулювання ІТ-відносин:* матеріали міжнародної науково-практичної конференції (м. Одеса, 18 трав. 2017 р.); ІТ-право: поняття та сутність: монографія. За ред. О. І. Харитонової, Є. О. Харитонова. Одеса: Фенікс, 2017. 316 с.; ІТ-право та інформаційна безпека: монографія. За ред.. д.ю.н., проф. О. І. Харитонової, проф. Є. О. Харитонова. Одеса: Фенікс, 2017. 176 с.; Information ecurity and IT law in conditions of integration processes: [Collective monograph]. Riga: Izdevnieciba Baltija Publishing, 2017. 213 p. та ін.

тати досліджень якої представлені на міжнародній конференції у м. Вроцлав (Польща)[1], проблеми штучного інтелекту тощо.

Таким чином, можна говорити про створення методологічного підґрунтя для подальшого розвитку школи ІТ-права разом з науковцями кафедри цивільного права.

Однак, попри те, що термін «ІТ-право» вже широко використовувався як науковцями, так і практиками для позначення норм, що стосувалися сфери ІТ-відносин, загального розуміння сутності цього явища у вітчизняній юриспруденції на той час ще не сформувалося. Більш того, у процесі дискусій з'ясувалося існування серйозних розбіжностей щодо бачення юридичної природи, змісту та обсягу поняття «ІТ-право». Ситуація, що склалася, зумовлює необхідність пошуку відповіді на згадані та інші питання, оскільки від того, які результати будуть отримані, залежить формування концепції ІТ-права і впровадження її в життя.

Зазначеними обставинами зумовлювалася необхідність подальших наукових досліджень на цих теренах, пошуків та обґрунтування парадигми ІТ-права.

На нашу думку, вирішення саме цього завдання було ГОЛОВНИМ ВИКЛИКОМ ПРАВОЗНАВЦЯМ З БОКУ ІТ (ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА).

Перехід до пошуку відповіді на нього означав також початок ІІ етапу розвитку (трансформації) наукової школи ІТ-права, котрий потребував вирішення завдань, що виникали, за допомогою, головним чином, методів концептного, системного та логічно-структурного аналізу.

ІІ Етап. Розгалуження і поглиблення сфери досліджень

Отже Відповідь на головний Виклик часу (інформаційного суспільства) – встановлення і доведення необхідності дослідження інформаційних, інформаційно-комунікаційних технологій (ІТ, ІКТ), як правового феномену, і встановлення його придатності стати об'єктом правового регулювання на певних засадах, була не завершенням, а лише початком наукових досліджень у цій сфері. Адже тепер було необхідно дослідити адекватність концептів правового регулювання

[1] Charytonowa H., Charytonow Y. Własność wirtualna jako intelektualna własność.

окремих категорій, інститутів цивільного права відповідним «категоріальним», «інституційним» Викликам Інформаційного суспільства. Тобто мало відбутися «розгалуження» (спеціалізація, конкретизація) досліджень наукової школи у межах проблематики регулювання ІТ-відносин.

У загальному вигляді напрямки подальших досліджень та проблеми, які вартують глибокого вивчення, були окреслені у частині ІУ «Традиційні цивілістичні категорії і виклики інформаційного суспільства» монографії Євгена та Олена Харитонових, де, зокрема, з погляду необхідності врахування викликів інформаційного суспільства характеризувалися проблеми з'ясування сутності ІТ-права, з'ясування його місця у правовій системі, трансформації розуміння цивільних правовідносин у цифрову добу, викликів інформаційного суспільства вітчизняній концепції права власності та прав інтелектуальної власності, юридична характеристика категорії «штучний інтелект» та з'ясування правової сутності останнього тощо.[1]

Відповідно до названих та супутніх з ними напрямів логіка наступних досліджень виглядала наступним чином.

По-перше, дослідження співвідношення категорій «інформаційне суспільство», «громадянське суспільство», «інтерактивне мережеве громадянське суспільство», «приватне право», «цивільне право» та «ІТ-право».

Головним завданням, яке вирішувалося на цьому напряму, було визначення співвідношення розуміння та особливостей інформаційного суспільства та громадянського суспільства, як категорій невід'ємно пов'язаних у сучасних умовах з використанням інформаційних технологій.

При цьому, оскільки вираз «інтерактивне громадянське суспільство» наразі є недоконаним концептом, що перебуває у процесі формування, зазначалася доцільність вести мову про «громадянське суспільство цифрової доби», маючи на увазі, що зміст цього поняття залежить від ступеню долучення ІТ до функціонування спільноти, котра є людським субстратом громадянського суспільства.

[1] Харитонов Є. О., Харитонова О. І. Приватне право як концепт. Том ІІІ. Концепт приватного права і рекодифікації цивільного законодавства в Україні: рефлексії фронтиру: монографія. Одеса: Фенікс, 2019. С. 590-673.

Врахування згаданого ступеню долучення ІТ до функціонування громадянського суспільства припускає проведення досліджень у цій сфері з розрізненням кількох «рівнів» долучення. Перший рівень (найпростіший) – використання ІТ як засобу спілкування членів громадянського суспільства (домовленості про зустрічі,повідомлення про заходи, інформація про події, що відбулися, тощо). Другий рівень – підвищення ефективності діяльності громадянського суспільства за рахунок використання можливостей інформаційних технологій (прикладом може бути розширення **соціальною мережею Facebook можливостей сервісу Safety Check, котрий автоматично активується у разі виникнення кризових ситуацій.** Кожен користувач Facebook, який опинився у районі, де автоматично активується опція Safety Check, зможе запропонувати оточуючим або замовити у них їжу, напої, дах над головою та можливість скористатися транспортним засобом).[1]

Найближчим до «повноцінного» концепту «інтерактивного громадянського суспільства» (третім рівнем), є тип соціальних мереж, котрі мають цілі, властиві громадянському суспільству, зокрема, вплив на соціальні зв'язки, який вчиняється шляхом оприлюднення інформації та здійснення на такій основі суспільно-корисної діяльності. (Прикладом такої форми діяльності є соціальна мережа Авааз («голос» на фарсі).[2]

Крім того, завданнями науковців, які працювали у цьому напрямі досліджень було те, що із врахуванням того, що буття громадянського суспільства має підґрунтям приватне право, вони мали додатково вивчити значення цієї обставини для функціонування інтерактивного громадянського суспільства, соціальних мереж тощо, а також проаналізувати зв'язок приватного права, як концепту, з впорядкуванням ІТ-відносин у сфері цивільно-правового регулювання.

По-друге, належна увага мала приділятися визначенню сутності ІТ-права, що, у свою чергу, потребувало обрання методологічних засад розуміння права взагалі, від чого, власне, і залежить бачення сутності ІТ-права, як частини цілого (як конкретного прояву абстрактного поняття).

[1] Facebook запроваджує функцію взаємодопомоги під час стихійних лих. URL: https://ru.slovoidilo.ua/2017/02/09/novost/obshhestvo/facebook-vvodit-funkciyu-vzaimopomoshhi-vo-vremya-stixijnyx-bedstvij

[2] https://uk.wikipedia.org/wiki/Avaaz

У зв'язку з цим обґрунтувалася необхідність розділення праворозуміння на загальносоціальне, коли правом визнаються суспільні явища недержавного походження й функціонування, і спеціальносоціальне, коли правом визнаються явища виключно державного походження,[1] а відтак базовим методологічним імперативом досліджень ставав висновок, що спроби кваліфікувати комплексне правове регулювання інформаційних відносин постіндустріального суспільства, як формування особливої нової галузі права, з позицій нормативістського» праворозуміння. є некоректним.

Тому пропонувалося виходити з того, що «ІТ-право» слід характеризувати з позицій не нормативістського праворозуміння, а цивілізаційного підходу, розуміючи його як сукупність уявлень, понять, знань, асоціацій, емоцій, що виникають у зв'язку з правовим впорядкуванням суспільних відносин, пов'язаних зі створенням та використанням інформаційних технологій.

Таке розуміння «ІТ-права» не заперечувало «нормативне» (законодавче) наповнення цього поняття, але позбавляло необхідності обов'язкової оцінки його як системи правових норм, що утворюють галузь права, відповідні правові інститути тощо. При цьому за межами «ІТ-права» знаходяться норми адміністративного, карного, митного, податкового тощо права, оскільки зазначені галузі, як управлінські та охоронні, можуть стосуватися різних видів суспільних відносин, забезпечуючи їхнє впорядкування та охорону.

По-третє, важливим напрямом був аналіз трансформації цивільних правовідносин у цифрову добу. Крім характеристики категорії «інтернет-правовідносин» (правовідносин в Інтернеті), котра досліджувалася вже на попередньому етапі, актуальними стають вивчення особливостей складу цивільних правовідносин, що виникають та функціонують у ІТ-сфері

Відтак дослідники відповідних питань мали з'ясувати виправданість віднесення Інтернет-відносин до нового типу суспільних відносин, які виникають, змінюються і припиняються у кіберпросторі, необхідність чого мотивувалася тезою про самодостатність технічних та технологічних засобів регулювання (саморегулювання) сфери ІТ.

[1] Рабінович П. М. Основи загальної теорії права та держави. Навч. посібник. Вид. 10-е, доповнене. Львів: Край, 2008. С. 13.

На відміну від зазначених пропозицій, представники Одеської школи виходили з того, що основна частина правовідносин, які виникають у ІТ-сфері («ІТ-правовідносини»), є цивільними регулятивними правовідносинами, котрі у сфері ІТ, однак, стикаються з такими Викликами, як необхідність оновленого розуміння суб'єктів та об'єктів таких правовідносин.

Таке рішення, у свою чергу, ставило перед правознавцями завдання визначення юридичної сутності таких об'єктів, особливостей їхнього правового режиму. При цьому, розширення кола специфічних об'єктів цивільних правовідносин, пов'язаних зі сферою інформаційних технологій, відбувається не лише внаслідок врахування інноваційних результатів інтелектуальної творчої діяльності, але й внаслідок поширювального інноваційного тлумачення видів матеріальних та нематеріальних благ, пов'язаних зі сферою ІТ. Зокрема, наслідком такого підходу стала поява поняття «ІТ-активів», під якими розуміється будь-який ресурс або здатність, що включає в себе ІТ-інфраструктуру, людей, гроші і все, що може сприяти наданню ІТ-послуги. Здатністю є можливість організації, людини, процесу, додатку, конфігураційної одиниці або ІТ-послуги здійснювати діяльність. Здатність – це нематеріальні ресурси організації. Узагальнюючи та залишаючи осторонь питання персоналу, який забезпечує ІТ-діяльність організації, можна зазначити, що ІТ-активом є будь-який ІТ-ресурс або сукупність здатностей здійснювати ІТ-діяльності, які представляють цінність для основної діяльності підприємства.[1]

Низка проблем була зумовлена необхідністю визначення та характеристики особливостей суб'єктивного складу цивільних правовідносин в умовах інформаційного суспільства, аби з'ясувати виправданість тренду фактичного розширення кола їх «учасників» за рахунок «віртуальних суб'єктів» (використання різних форм штучного інтелекту, на які покладаються функції, котрі раніше (і поки що) виконували люди: медичні, юридичні та інші послуги, підготовка та обробка інформації про новини тощо). Завдання актуалізувалося тим, що вже йшлося не просто про використання ІТ як інструментарію в руках людини, а про, значною мірою, автономне функціонування штучного інтелекту в межах і умовах визначених

[1] Про розвиток цієї концепції детальніше див.: розділ К. Некіт у цій монографії

завдань з метою виконання останніх. Наступним кроком мало стати створення, так званого, «загального штучного інтелекту», здатного запам'ятовувати отримані навички та використовувати їх для вирішення наступних проблем, що до останнього часу вважалося відмінною рисою людини.

У зв'язку з цим представниками школи було запропоноване і обґрунтоване (зокрема, з посиланням на існуючий досвід використання «теорії фікції» для вирішення аналогічних завдань) при визнанні «штучного інтелекту» у випадках його «самостійної» діяльності учасником відносин у ІТ-сфері, – квазі-суб'єктом цивільних правовідносин. Відтак доводилося, що найпростішим (з прагматичного погляду) рішенням в теперішніх умовах було б доповнення переліку учасників цивільних відносин у ст. 2 ЦК України згадкою про існування четвертого виду суб'єктів, назвавши їх, скажімо, «нібито особи» (зі згадкою при цьому, що до їх числа належать «генеративний штучний інтелект», «віртуальні особи» тощо).

У контексті дослідження трансформацій загальної категорії цивільних правовідносин в інформаційному суспільстві потребували також уваги науковців особливості підстав виникнення, зміни та припинення цивільних прав та обов'язків (юридичних фактів). Поміж таких юридичних фактів провідне місце займають правочини, котрі є найбільш типовими діями, що тягнуть виникнення цивільних правовідносин, як з погляду громадянського суспільства, так і з погляду приватного права взагалі. Одним з найбільш важливих викликів, у цій сфері у зв'язку з формуванням інформаційного суспільства, було питання про роль і значення інформаційних технологій: чи то вони є просто новітньою формою вчинення та фіксації правочину, внаслідок якого виникали правовідносини, чи то у сфері ІТ правовідносини можуть виникати внаслідок правочину не просто оформленого інакше, а інакшого за своєю сутністю. Простішим, на перший погляд, здається перший варіант відповіді. Але дослідження цієї та суміжних з нею проблем представниками наукової школи дало підстави для висновку, що обидва розуміння можуть співіснувати разом. І якщо зміна форми правочину є нормальним явищем і протягом тисячоліть існування цієї категорії відбувалося неодноразово, то виникнення терміно-поняття «електронний правочин» є знаковою подією і знаменує собою початок «прориву» у новий «світ

цифрової доби». Ця важлива проблема, стан та перспективи її вирішення стала об'єктом дослідження у дисертації доктора юридичних наук, виконаної І. В. Давидовою «Правочини та їх недійсність в інформаційному суспільстві».[1]

По-четверте, з огляду на реалії формування інформаційного суспільства, потребувала перегляду класична/ традиційна концепція права власності (речевих прав), згідно які й це відносини, у яких одні особи – власники – ставляться до речей як до своїх, а всі інші – не власники – мають ставитися до них як до чужих й утримуватися від будь-яких зазіхань на ці речі.

Відповідно до такого підходу сформульована дефініція права власності у ст. 316 ЦК України, яка встановлює, що правом власності є право особи на річ (майно), яке вона здійснює відповідно до закону за своєю волею, незалежно від волі інших (ст. 314 проєкту ЦК України від 25 серпня 1996 р., передбачала, що правом власності є найбільш повне право, що його особа має на майно, а усі інші особи зобов'язані утримуватися від вчинення будь-яких дій, що можуть порушувати право власності).

Виклик традиційній концепції права власності полягає, передусім, у формуванні концепції, так званої, «віртуальної власності», яка своєю появою завдячує іншій категорії – «віртуальна реальність».

Методологічним підґрунтям появи та існування концепту «віртуальне середовище» є ідея, згідно якій ми існуємо у віртуальному світі, підставою виникнення якого вважається «комп'ютерна симуляція».

Віртуальна соціальна реальність складається з віртуальних соціальних інститутів. У свою чергу, саме завдяки таким інститутам набуває цінності «віртуальна власність», котра сьогодні у багатьох випадках є предметом вже не віртуальних, а реальних товарно-грошових відносин.

Сутність віртуальної власності полягає навіть не в віртуальності середовища, в якому виникають відповідні відносини, а у звільненні ідей від загальних обмежень простору, часу, матерії, а також цензури. Конкуруючи з книгою, яка за своєю природою матеріальна, Інтернет повернув світу думок його початкову віртуальність. Стихія Інтерне-

[1] Давидова І. В. Правочини та їх недійсність в інформаційному суспільстві: автореф. дис. … д-ра. юрид. наук: 12.00.03. Одеса, 2018. 40 с.

ту – це інновації і комунікації, а не матеріальні речі. Традиційний світ і його правова система ґрунтуються на матеріальній економіці матеріальних благ, тоді як у Інтернеті основою добробуту є творчість людей, нематеріальна за своєю природою.

Враховуючи викладене вище, можемо вести мову про «двоїстість» права віртуальної власності, розрізняючи таке право віртуальної власності, що існує у реальному світі, і таке, що існує у нереальному (уявному, віртуальному) світі.

Право віртуальної власності у реальному світі – це, передусім, право інтелектуальної власності, сутність котрого полягає у тому, що йдеться не про право на річ, а про «право на права».

Право віртуальної власності у віртуальному світі – це право власності на ігрові предмети, створені або придбані гравцем за віртуальну валюту або реальні гроші, віртуальну нерухомість, і все те, що перебуває у віртуальному світі, і може бути об'єктом правочинів.

Наразі поширеним є перший з названих вище феноменів – право віртуальної власності у реальному світі, що, фактично є тотожним концепту «право інтелектуальної власності» Можна припустити, що саме урахування цієї особливості інтелектуальної власності стало методологічними підґрунтям віднесення прав інтелектуальної власності до права власності (пропріетарна теорія).

Пропріетарна теорія права інтелектуальної власності достатньо послідовно проводиться у чинних міжнародно-правових актах і впливає на моделювання національних законодавств.

Отже, інтелектуальна власність за своєю юридичною природою є власністю віртуальною і в такій якості найбільш органічно пристосована до нового світу інформаційних технологій. Основна відмінність між ними полягає в тому, що більшість з віртуальних об'єктів є об'єктами інтелектуальної власності, які учасник віртуального світу використовує на підставі невиключної ліцензії, однак віртуальні предмети все частіше стають предметом правочинів купівлі-продажу, а не уступки прав з ліцензійного договору. Тому віртуальна власність може бути інтелектуальною, а може й не бути такою.

Ведучи мову про віртуальну власність, слід виходити з того, що вона за своєю природою є нематеріальною, як правило, є об'єктом ав-

торського права і виникає у віртуальному середовищі. Застереження про те, що віртуальна власність є, як правило, об'єктом авторського права, свідчить про можливість розподілу всіх об'єктів віртуальної власності на такі, що є об'єктами права інтелектуальної власності і такі, що ними не є.

З цих позицій віртуальна власність може характеризуватися як інформаційний об'єкт, права на який належать одному або декільком власникам. Таким чином, право власності втрачає свою ознаку суто речевого права (зберігаючи, втім, певною мірою зв'язок з майновими правами), а відтак має розглядатися як більш широка, ніж нині, категорія.[1]

Викликом традиційному розумінню права власності, як правоможностей суб'єктів цивільних відносин, наразі також є «Інтернет речей», котрий у найбільш загальному вигляді характеризують як концепцію комунікації об'єктів («речей»), які використовують технології для взаємодії між собою та з навколишнім середовищем, припускаючи при цьому виконання пристроями певних дій без втручання людини. Інтернет речей визначають також як сукупність взаємодіючих технічних систем і комплексів, призначених для реалізації суспільних відносин, у тому числі, пов'язаних з наданням послуг або проведенням робіт, на основі використання різноманітних даних та Інтернету за безпосередньої участі або без участі суб'єктів цих відносин (юридичних або фізичних осіб).[2]

Інтернет речей припускає можливість певної діяльності, спрямованої на певний результат (і очевидно, настання певних не лише фактичних, а й правових наслідків) в інформаційному суспільстві без участі суб'єктів цивільних відносин, що згадуються у ЦК України. І хоча у більшості випадків оцінка Інтернету речей є позитивною (особливо з боку розробників), однак у зв'язку з поширенням цього явища виникає низка ризиків, що потребує впорядкування відповідних суспільних відносин. Разом із тим, не з'ясованим поки що залишається навіть питання, чи виправдано вважати Інтернет речей об'єктом чи

[1] Харитонова О. І., Харитонов Є. О. Віртуальна власність та право інтелектуальної власності. *Спогади про Людину, Вченого, Цивіліста-епоху* (до 85-річчя від Дня народження академіка Ярославни Миколаївни Шевченко). За заг. ред. Р. О. Стефанчука. К.: АртЕк, 2017. С. 335-347.

[2] Баранов О. «Інтернет речей» як правовий термін. *Юридична Україна.* 2016. № 5-6. С. 96-103.

суб'єктом правовідносин.[1] У другому випадку виникає необхідність перегляду суб'єктного складу правовідносин власності та розширення його за рахунок роботів.

Наразі не існує готових відповідей на згадані Виклики. Однак необхідність перегляду традиційної концепції права власності сумнівів не викликає.[2]

Висновок про те, що вітчизняна концепція права власності не враховує Викликів інформаційного суспільства, став тригером для активізації досліджень Одеської наукової Школи на цьому напряму.

Відтак, крім проведення низки наукових заходів, аналізу цих питань у низці публікацій, результатом досліджень у цій сфері стала підготовка і захист дисертації доктора юридичних наук К. Г. Некіт «Право приватної власності в інформаційному суспільстві».[3]

По-п'яте, важливим напрямом досліджень стали питання забезпечення інформаційної безпеки у сфері інформаційних технологій. Якщо на початку російської інвазії 2014 року гібридна російсько-українська (зокрема, інформаційна) війна точилася значною мірою за допомогою загальних, більш традиційних засобів інформаційного впливу (друковані медіа, телевізійні передачі, кінофільми тощо), то з часом вона усе більше переходила у сферу он-лайн, що актуалізувало питання використання, поряд з іншими, юридичних заходів протистояння агресії у мережі Інтернет. Це зумовило активізацію досліджень відповідної проблематики.[4]

---

[1] Харитонова О. І., Харитонов Є. О. Інтернет речей: об'єкт чи суб'єкт правовідносин. *ІТ-право та цифрове суспільство:* матеріали Всеукр. конференції (м. Одеса, 24 листопада 2017 р.). За заг. ред. д.ю.н., проф. Є. О. Харитонова. Одеса: Юрид. література, 2017. С. 5-8.

[2] Харитонов Є. О., Харитонова О. І. Категорія «право власності» перед викликами цифрового світу. *Цивільне судочинство у світлі судової реформи в Україні.* Всеукр. наук.-практ.конф.до 90-річчя від дня народження Ю. С. Червоного (м. Одеса, 6 листоп. 2017 р.). За заг.ред. Н. Б. Голубєвої. Одеса: Фенікс, 2017. С. 21-25.

[3] Некіт К. Г. Право приватної власності в інформаційному суспільстві: цивілістична теорія і практика реалізації: дис. … д-ра. юрид. наук: 12.00.03. Одеса, 2021. 574 с.

[4] Харитонов Є. О. Інформаційна безпека з погляду цивілістики. *Цивільне право та інформаційна безпека в умовах інтеграційних процесів:* мат. кругл. столу (3 червня 2017 р., м. Одеса). Збірник матеріалів Міжнародного Конгресу «Правові проблеми державно-правового партнерства в умовах євроінтеграції», присвяченого 20-річчю Національного університету «Одеська юридична академія», м. Одеса, 2-4 червня 2017 р. Одеса: Юридична література, 2017. С. 64-68; Харитонов Є. О. Проблема асекурація інформаційної безпеки неповнолітніх у ІТ-сфері в контексті немайнових правовідносин батьків та дітей. *Сучасний стан і перспективи розвитку сімейного права України в*

Слід зазначити, що на певний час цілеспрямовані дослідження у цій сфері були перервані ще одним, «стороннім», здавалось, щодо розвитку інформаційного суспільства Викликом – пандемією «коронавірусу». Цей виклик певною мірою змінив вектор дослідження правових проблем використання інформаційних відносин. Варто зауважити, що поряд з негативними наслідками для суспільства, пандемія стала потужним поштовхом до розвитку, а відтак вивчення, таких засобів ІТ-сфери як електронна торгівля, дистанційне навчання, електронне обслуговування тощо. Відповідною була і реакція науковців Школи, які протягом 19-20 років підготували і видали низку публікацій (зокрема, монографій) присвячених цим проблемам.[1]

умовах адаптації до Європейського права: мат. всеукр. кругл. столу (26 травня 2017 р., м. Одеса). Одеса: Фенікс, 2017. С. 4-9; Харитонов Є. О., Харитонова О. І. Проблеми правового регулювання в ІТ-сфері в умовах інформаційної війни. *Проблеми відновлення конституційного ладу в Україні*: Матеріали міжнародної науково-практичної конференції. м. Київ. 19-20 травня 2017 р. Київ: Таврійський національний університет ім. В. І. Вернадського. 2017. С.159-163; ІТ-право та інформаційна безпека: монографія. За ред. О. І. Харитонової, Харитонова Є. О. Одеса: Фенікс, 2017. 176 с.; Інформаційна безпека: проблеми приватного права: навчальний посібник. Голов. ред. Є. О. Харитонов. Одеса: Юридична література, 2019; Харитонова О., Харитонов Є. Інформаційна безпека як один з чинників національної безпеки України: загрози під час війни. *Незалежність України: права людини та національна безпека:* збірник матеріалів Четвертої міжнародної науково-практичної конференції (Львів, 12 квітня 2024 року). Київ: КНТ. 2024. С. 53-56; Харитонова О., Харитонов Є. Віртуальний світ, віртуальна ідентичність, симулякри та гібридна війна. *Цифрова трансформація в Україні: ШІ, метавсесвіт і суспільство 5.0.* Наукова апробація. моногр. Відредаговано: Олексій Костенко, канд. в праві Юрій Єхануров, канд. в економіці SciFormat Publishing Inc. Канада, 2024 рік . P. 14-20.DOI:10.69635/978-1-0690482-1-9 https:// sciformat . ca / books / index . php / sf / catalog / view /3/2/16? fbclid = IwZXh 0 bgNhZW 0 CMTEAAR 3 U 0 hRu 8 KJjNZMoD 6 mUb 2 AKm 2 dW 54 pcXOTiLiuciDaCbUnDKQa 8 gLwtDAY _ aem _ Eehovn 1 QlO 3 G 9 O 7 xV 6 JyWg & sfnsn = mo

[1] Права приватної особи в умовах пандемії COVID-19: проблеми здійснення і захисту: моногр. / За ред. Харитонова Є. О., Харитонової О. І., Некіт К. Г. Одеса: Гельветика, 2020; Харитонов Є. О., Харитонова О. І. COVID-19 і делікти створення небезпеки. *Часопис цивілістики.* 2020. № 38. С. 5-11; Харитонов Є. О. Пандемія COVID-19 та деякі актуальні проблеми цивілістики. *Проблеми правового регулювання цивільних відносин в умовах COVID-19:* матер. Всеукр. науково-практичної онлайн-конференції (23 квітня 2020 р.). Одеса: Фенікс, 2020. С. 5-7; Харитонов Є. О., Харитонова О. І. Примус і цивільно-правова відповідальність як засоби подолання конфлікту інтересів при COVID-19. *Цивілістичні проблеми колізії приватних та публічних інтересів в умовах пандемії COVID-19*: матер. Всеукр. наук.- практ. конференції. Одеса, 2020. С. 6-11; Харитонов Є. О., Харитонова О. І. Конфлікт та солідарність інтересів в умовах пандемії COVID-19. *Часопис цивілістики.* 2021. № 40. С. 5-11; Харитонов Є. О., Харитонова О. І. Деякі проблеми вакцинації від Ковід-19 з погляду цивільного права. *Часопис цивілістики.* 2021. № 43. С. 5-14; Харитонов Є. О., Харитонова О. І. Механізм цивільно-правового регулювання

Нарешті, ще одним (і найбільш потужним та небезпечним) Викликом стало повномасштабне вторгнення російських військ 24.2.2222 року), котре перевело гібридну російсько-українську війну у нову якість, змінило розуміння понять «кіберзброя» і «кіберзагроз», характер і ступінь вимог до «кібербезпеки», а також стрімко прискорило розвиток «штучного інтелекту», незмірно посиливши його «бінарність» і створивши колізію допустимості його «наступального» і «оборонного» застосування.

У таких умовах зросло значення оперативного вирішення практичних питань у сфері ІТ, які потребують правового забезпечення.

Враховуючи цю потребу, Школа у своїх дослідженнях почала активно використовувати розуміння права і методи дослідження, ефективні з погляду практичних результатів під час гібридної війни.

Це дає підстави наразі характеризувати її як «прагматичну/ соціологічну школу ІТ-права».

Крім того, активно розвивається напрям (**ІІІ етап) досліджень Штучного інтелекту,** що має тенденцію до виокремлення в окрему школу, здобутки якої наразі відображені у низці публікацій – від тез на конференціях і наукових статей до монографій і дисертацій, спеціально присвячених правовим проблемам штучного інтелекту.

Зокрема, наразі увага у цій галузі приділяється, головним чином, таким категоріям, як «симулякри»[1], «цифрова людина, цифрова

відносин в умовах пандемії COVID-19: антропологічний коректив. *Часопис цивілістики.* 2021. № 44. С. 5-18; Вакцинація від COVID-19: соціальні та правові проблеми: моногр. За ред. Є. О. Харитонова, О. І. Харитонової, К. Г. Некіт. Одеса: Гельветика, 2022. 374 с.

[1] Харитонова О. І., Харитонов Є. О. Дещо про симулякри, нову реальність і політичні процеси в Україні. *Актуальні проблеми інтелектуального, інформаційного та ІТ права:* матеріали третьої всеукраїнської науково-практичної конференції (Львів, 17-18 травня 2019 р.). Львів: Юрид. ф–т Львів. нац. ун–ту ім. І. Франка, 2019. С. 176-191. 218 с.; Харитонов Є. О., Харитонова О. І. Віртуальний світ, віртуальна особистість і симулякри. *Цифрова трансформація та цифрова економіка в умовах воєнного стану: аспекти інтелектуальної власності.* збірник матеріалів V Всеукр. наук.-практ. конф. з проблем економіки інтелектуальної власності, 27 травня 2022 р., Київ: Науково-дослідний інститут інтелектуальної власності НАПрН України, 2022.С. 225-229; Харитонова О., Харитонов Є. Віртуальний світ, віртуальна ідентичність, симулякри та гібридна війна. *Цифрова трансформація в Україні: ШІ, метавсесвіт і суспільство 5.0. Наукова апроб ація.* Моногр . Відредаговано: Олексій Костенко, канд. в праві, Юрій Єхануров, канд. в економіці SciFormat Publishing Inc. Канада, 2024 рік . P. 14-20.DOI:10.69635/978-1-0690482-1-9. https:// sciformat . ca / books / index . php / sf / catalog / view /3/2/16? fbclid = IwZXh 0 bgNhZW 0 CMTEAAR 3 U 0 hRu 8 KJjNZMoD 6 mUb 2 AKm 2 dW 54 pcXOTi LiuciDaCbUnDKQa 8 gLwtDAY _ aem _ Eehovn 1 QlO 3 G 9 O 7 xV 6 JyWg & sfnsn = mo

особистість»[1], «віртуальна власність»[2], «інтернет речей»[3], «цифрові права»[4], «об'єкти, створені штучним інтелектом»[5], «правова природа штучного інтелекту»[6] тощо. В цьому сенсі відбувається дослідження ІТ-відносин з подальшим їх перенесенням у віртуальну сферу, ана-

[1] Харитонова О. І., Харитонов Є. О. Цифрова людина, цифрова особа та цифрова особистість: до проблеми співвідношення. *Часопис цивілістики.* 2023. № 49. С. 5-13; Харитонова О., Харитонов Є. Категорії нової реальності: цифрова людина, цифрова особа, цифрова особистість та цифрова ідентичність: до проблеми співвідношення. *Правове регулювання цифрової економіки та штучного інтелекту: національний та міжнародний виміри:* матеріали міжнародної науково-практичної конференції 16 листопада 2023 р.; Науково-дослідний інститут інтелектуальної власності НАПрН України. К.: Інтерсервіс, 2023. 308 с.; Харитонова О. І., Харитонов Є. О. Проблеми визначення правового статусу особи у цифровому середовищі. *Проблеми правового регулювання забезпечення особистих немайнових прав особи та прав на віртуальні активи в умовах цифровізації:* матеріали Міжнародної науково-практичної конференції (10 травня 2025 р., Ужгород-Піза). Ужгород, 2025. С. 178-181.

[2] Харитонова О. І. Віртуальна власність». *ІТ-право:* практ. посіб. Київ: Норма права, 2025. С. 69-94; Харитонов Є. О., Харитонова О. І. Концепція «комп'ютерної симуляції» як методологічна основа виникнення «віртуальної власності». *ІТ-право:* практ. посібн. Київ: Норма права, 2025. С. 69-74; Харитонова О. І., Харитонов Є. О. Віртуальна (цифрова) власність у світлі рекодифікації речового права. *Рекодифікація речового права*: збірник матеріалів XIV Міжнародного цивілістичного форуму (м. Київ, 16 травня 2025 р.). Одеса: Юридика, 2025. С. 162-167; Харитонова О. І., Харитонов Є. О. Віртуальна власність та право інтелектуальної власності. Спогади про Людину, Вченого, Цивіліста-епоху (до 85-річчя від Дня народження академіка Ярославни Миколаївни Шевченко). За заг. ред. Р. О. Стефанчука. К.: АртЕк, 2017. С. 335-347; Харитонов Є. О., Харитонова О. І. Категорія «право власності» перед викликами цифрового світу. *Цивільне судочинство у світлі судової реформи в Україні.* Всеукр.наук.-практ.конф.до 90-річчя від дня народження Ю. С. Червоного (м. Одеса, 6 листоп. 2017 р.). Одеса: Фенікс, 2017. С. 21-25.

[3] Харитонова О. І., Харитонов Є. О. Інтернет речей: об'єкт чи суб'єкт правовідносин. *ІТ-право та цифрове суспільство:* матеріали Всеукр.конференції (м. Одеса, 24 листопада 2017 р.). Одеса: Юридична література, 2017. С. 5-8.

[4] Харитонова О. І., Харитонов Є. О. Цифрові права: до проблеми питання. *Незалежність України: права людини та національна безпека:* збірник матеріалів П'ятої міжнародної науково-практичної конференції (Львів, 4 квітня 2025 року). Львів-Острог: 4Фемілі, 2025. С. 55-58.

[5] Харитонова О. І. Актуальні проблеми штучного інтелекту в праві інтелектуальної власності. *Юридичний вісник.* 2024. № 5; Харитонова О. І., Кирилюк А. В., Галупова Л. І. Правові аспекти використання творів, створених штучним інтелектом. *The 23rd International scientific and practical conference "World ways and methods of improving outdated theories and trends"* (June 11 – 14, 2024) Zagreb, Croatia. International Science Group. 2024. 393 p. С. 143-146.

[6] Харитонова О., Харитонов Є., Харитонова Т., Григорьєва Х. Штучний інтелект як правова категорія. *Костенко О., Харитонова О., Харитонов Є.* Ц*ифровізація, метавсесвіт, штучний інтелект у контексті захисту прав людини та особи в Україні та світі.* 2025. С. 68-89. URL: https://doi.org/10.69635/978-1-0690482-4-0-ch4

ліз тих трансформацій, які відбуваються з традиційними категоріями цивільного права під впливом технологій штучного інтелекту. Розробляються проблеми віртуальної власності, результати досліджень якої представлені на міжнародній конференції у м. Вроцлав (Польща)[1], проблеми штучного інтелекту тощо. Одним із здобутків є дисертація В. О. Токарєвої на здобуття наукового ступеня доктора юридичних наук, присвячена проблемам правосуб'єктності особи у відносинах у мережі Інтернет.

Як зазначалося, на цих теренах активно розвивається перспективний напрямок досліджень стосовно бінарності (дуалізму) штучного інтелекту, який наразі формується у «Школу бінарності штучного інтелекту **(ЦИВІЛІСТИЧНА ШКОЛА БІНАРНОСТІ (ДУАЛІЗМУ) ШТУЧНОГО ІНТЕЛЕКТУ**)».

Цей напрям (школа) буде репрезентований у окремій книзі, де будуть зібрані наукові праці правознавців, присвячені правовим проблемам штучного інтелекту як концепту.

Висновки

Наукова цивілістична школа ІТ-права, що почала формуватися в НУ ОЮА, як реакція правознавців-науковців на Виклики інформаційного суспільства, близько 10 років тому, пройшла у своєму розвитку кілька етапів, чутливо реагуючи на запити теорії і практики у цій сфері, зокрема пов'язані з гібридною інформаційною війною, пандемією коронавірусу, повномасштабним вторгненням російських в Україну 24. 2022 року.

У процесі пошуку оптимальної методології дослідження науковцями використовувалися різні наукові методи у залежності від тих завдань, що поставали перед ними. Наразі базові засади наукових пошуків визначаються умовами гібридної війни, у якій інформаційним технологіям відводиться надзвичайно важлива роль. Відповідно до цього Школу найбільш точно характеризує найменування її як «прагматичної» або ж «соціологічної» цивілістичної школи ІТ-права, і з таких позицій визначаються її завдання на майбутнє.

[1] Charytonowa H., Charytonow Y. Własność wirtualna jako intelektualna własność.

Ключові слова: інформаційне суспільство, інформаційні технології, школа ІТ-права, гібридна війна, прагматична школа права, Інтернет, соціальні мережі, право власності, віртуальна власність, штучний інтелект.

Розділ 2

КОНЦЕПТ ІТ-ПРАВА[1]

DOI

Євген Харитонов
доктор юридичних наук, професор,
член-кореспондент НАПрН України

Олена Харитонова
докторка юридичних наук, професорка,
членкиня-кореспондент НАПрН України

Попередні зауваження

Формування інформаційно-комунікаційних технологій істотно вплинуло на розвиток суспільства, стало чинником інформаційної революції, зумовивши виникнення єдиного світового інформаційного простору. Інтернет перетворився на засіб передачі інформації, доступний кожному, хто має персональний комп'ютер. Інформаційно-комунікаційні технології розвиваються у небаченому досі темпі. Так, за перше десятиріччя XXI ст. кількість користувачів Інтернету зросла з 350 мільйонів до понад двох мільярдів.[2] Ще ніколи в історії людства так багато людей не були пов'язані між собою в мережі, що працює в режимі реального часу; безпрецедентними є можливості колективної дії через спільні Інтернет-платформи (для споживачів, творців, дослідників, активістів і багатьох інших). Плоди такого грандіозного масштабу, що ми їх бачимо сьогодні, – від вірусного музичного кліпу до міжнародного електронного торговельного майданчика – тільки натяк на те, що нас чекає далі.[3]

---

[1] Використані матеріали та ідеї, сформульовані раніше і викладені у ІТ-право: теорія та практика

[2] Ерік Шмідт, Джаред Коен. Новий цифровий світ Переклала з англ. Ганна Лелів. Львів: Літопис, 2015. С. 10.

[3] Ерік Шмідт, Джаред Коен. Новий цифровий світ Переклала з англ. Ганна Лелів. Львів: Літопис, 2015. С. 16.

У переважній більшості випадків оцінка зростання значення інформаційно-комунікаційних технологій є позитивною, підтвердженням чого є прийняття країнами «Великої вісімки» в Окінаві у 2000 році Хартії глобального інформаційного суспільства (Окінавська хартія). В Україні основні напрямки державної політики у галузі інформатизації визначені Указом Президента України «Про заходи щодо розвитку національної складової глобальної інформаційної Мережі та забезпечення широкого доступу до цієї мережі в Україні», яким, зокрема, передбачається вдосконалення правового регулювання діяльності суб'єктів інформаційних відносин, виробництва, використання, поширення та зберігання електронної інформаційної продукції, захисту прав на інтелектуальну власність, посилення відповідальності за порушення встановленого порядку доступу до електронних інформаційних ресурсів всіх форм власності, за навмисне поширення комп'ютерних вірусів тощо.

Разом із тим, загрози, що виникають внаслідок поширення ІТ,[1] не можуть залишатися поза увагою суспільства. Якість і кількість таких загроз істотно зросли під час гібридної війни, які через насиченість інформаційно-комунікативними технологіями часто-густо (особливо до повномасштабного російського вторгнення) ототожнювали з інформаційною війною.

Природно, що проблематика «ІТ-права» останнім часом викликає усе більший інтерес, що зумовлено поширенням ІТ-відносин та зростанням питомої ваги юридичної активності у цій галузі на практиці.

Соціальне управління, правове регулювання та правовідносини в інформаційному суспільстві

Терміном «інформація», який є ключовим у понятті «інформаційне суспільство», позначається багато явищ (іноді споріднених між собою, а іноді пов'язаних лише позірно), котрі існують у різних галузях і супроводжуються тлумаченнями та оцінками під різними кутами

[1] Е-бандити. *Український тиждень.* 2017. № 21. (26.05-1.06). С. 28-29; Кікерчук Р. Наркобарони тепер сидять за комп'ютером… *Високий замок.* 2017. № 52. С.1, 10; Війна з кіберджихадом. *Український тиждень.* 2017. № 24.(16-22. 06). С. 24-26; Макаревич Е. ТОП-10 цифровых угроз XXI века. *Фокус.* 2017. № 27. С. 20-23.

зору, що значно утруднює формування єдиного підходу до оцінки цієї категорії.[1]

У свою чергу терміно-поняття «інформаційне суспільство», як таке, що має безпосередній стосунок до інформації та інформаційних технологій, останнім часом широко вживається у різноманітному контексті у вузькому та широкому значеннях.

У вузькому значенні інформаційне суспільство – це: 1) суспільство, в якому виробництво, розподіл і споживання інформації є основною сферою діяльності; 2) суспільство нового типу, що формується внаслідок вибухового розвитку та конвергенції інформаційних та комунікаційних технологій, в якому головною умовою добробуту стає знання, здобуте завдяки безперешкодному доступу до інформації та вмінню працювати з нею; глобальне суспільство, в якому обмін інформацією не має меж; яке сприяє взаємопроникненню культур, водночас відкриваючи кожному співтовариству нові можливості для самоідентифікації; 3) вид постіндустріального суспільства, основою умовою формування якого є високотехнологічні глобальні інформаційні мережі, де інформація розглядається як товар, основна соціальна цінність.

У широкому розумінні інформаційне суспільство – це складова громадянського суспільства, що функціонує в рамках єдиного інформаційно-комунікаційного простору, в якому домінують нові технологічні уклади, котрі базуються на масовому використанні перспективних інформаційних технологій, засобів комп'ютерної техніки і телекомунікацій, створено якісно новий ринок знань та інформації як визначальних чинників виробництва інформаційних ресурсів та трансформації їх у реальні ресурси соціально-економічного розвитку, а також задоволення потреб суспільства і окремої людини в інформаційних продуктах, послугах тощо.[2] Національною стратегією сприяння розвитку громадянського суспільства в

---

[1] Кормич Б. А. Інформаційне право: підручник. Харків: БУРУН і К, 2011. С.5-32; Пилипчук В. Г., Цимбалюк В. С. Історико-правові проблеми становлення і розвитку інформаційної сфери та інформаційного права в Україні (кінець XX – початок XXI століття). *Вісник національної академії правових наук України.* 2016. № 4. С. 39; Тугарова О. К. Інформація як основний об'єкт інформаційних правовідносин. *Юридичний науковий електронний журнал.* 2022. № 8. С. 358-361.

[2] Попова Т. В., Ліпкан В. А. Стратегічні комунікації [словник]; за заг. ред. В. А. Ліпкана. К.: ФОП О. С. Ліпкан, 2016. С. 160-161.

Україні на2021-2026 роки серед інших, названо такі стратегічні напрями: удосконалення з урахуванням розвитку інформаційно-комунікаційних технологій та принципів безбар'єрності законодавчого регулювання порядку та способів подання звернень, у тому числі юридичними особами, до органів державної влади, органів місцевого самоврядування, їх посадових осіб, а також розгляду таких звернень, відповідальності за їх неналежний розгляд та зловживання правом на звернення; удосконалення правового регулювання процедури подання та розгляду електронних петицій, що набрали необхідну кількість підписів, у тому числі передбачення їх розгляду на засіданнях органів місцевого самоврядування з наданням слова ініціатору петиції або його уповноваженому представнику; удосконалення законодавчого регулювання та впровадження нових інформаційно-комунікаційних технологій для забезпечення механізмів місцевої демократії та доступних форматів для осіб з інвалідністю[1].

Таким чином, фактично пропонується розглядати інформаційне та громадянське суспільства як кореляти, тобто, як поняття, що невід'ємно пов'язані одне з одним (до цього питання ми ще повернемося далі).

З практичних міркувань можна обмежуватись стислим визначенням інформаційного суспільства як фази еволюційного розвитку цивілізації, в якій інформація і знання продукуються за допомогою інформаційних і комунікаційних технологій в єдиному інформаційному просторі.

У кожному разі, ключовими словами концепту «інформаційне суспільство» є: «інформація» та «суспільство».

Разом із тим, варто звернути увагу на те, що, хоча інформаційне поле, на думку Кріфа Коха, не є унікальною особливістю лише біологічних організмів, а існує взагалі у Всесвіті, як такому, [2] однак при сучасному рівні знань вплив на це поле з метою його впорядкування реально можливий лише у частині його біологічного (людського) субстрату.

---

[1] Про Національну стратегію сприяння розвитку громадянського суспільства в Україні на 2021-2026 роки: Указ Президента України від 27 вересня 2021 року № 487/2021. (rada.gov.ua)

[2] http://nv.ua/techno/science/bog-povsjudu-amerikanskij-fizik-vydvinul-teoriju-o-tom-chto-vselennaja-obladaet-soznaniem-1546675.html

Чим, власне, і зумовлюється наголошування на значенні не лише «інформації», «інформаційних технологій» тощо, а саме «інформаційного суспільства» (що, зокрема, знайшло відображення у резолюції Генеральної Асамблеї ООН 27 березня 2006 р., якою 17 травня проголошене Міжнародним днем інформаційного суспільства). Цими обставинами зумовлені і можливості та завдання соціального управління в інформаційному суспільстві.

Характеристику соціального управління доцільно почати зі з'ясування того, що мається на увазі під «регулюванням» (або ж «впорядкуванням»), як таким. Адже від того, що ми вкладаємо в поняття «регулювання», залежить розуміння можливості правового впливу на правомірну поведінку приватних осіб, визначення суб'єкта, котрий може здійснюватися такий вплив: держава, фігуранти держави, самоврядні органи, інші суб'єкти публічного права тощо.

Отже, візьмемо за відправну тезу відображене, практично, у будь-якому тлумачному словнику розуміння дієслова «регулювати» як синоніму виразу «впорядковувати що-небудь, керувати чимось, підкоряючи його, певній системі».

Одним з видів соціального регулювання є правове регулювання, предметом якого виступають суспільні відносини, впорядкування яких неможливе без використання норм права. Враховуючи це, «правове регулювання» можна визначити як один із основних засобів державного впливу на суспільні відносини з метою їхнього упорядкування в інтересах людини, суспільства і держави.

Елементами механізму правового регулювання є: 1) норми права, зафіксовані в законах та інших правових актах, якими визначається модель можливої та необхідної поведінки суб'єктів суспільних відносин; 2) юридичні факти; 3) власне правовідносини; 4) акти реалізації прав та обов'язків суб'єктів суспільних відносин, тобто дії цих суб'єктів у межах приписів відповідних правових норм; 5) правові санкції щодо порушників норм права. [1]

Оскільки метою правового регулювання є впорядкування суспільних (тобто, соціальних) відносин, то йдеться про «соціальне регулювання» або ж «соціальне управління», котре може бути визначене як вплив на суспільство і окремі його ланки (членів су-

[1] Юридична енциклопедія: В 6 т. Редкол.: Ю. С. Шемшученко (голова редкол.) та ін. К.: Укр. енцикл. Т. 5. 2003. С. 40-41.

спільства та їхні об'єднання) з метою впорядкування суспільних відносин, збереження якісної специфіки, вдосконалення та розвитку.

Наголосимо на діалектичній єдності суб'єктивних та об'єктивних чинників, котрі зумовлюють потребу в соціальному регулюванні.

Суб'єктивний чинник соціального регулювання – це прагнення колективів і окремих особистостей втілити цінності, які вони визнають і яких прагнуть) у процесі функціонування соціальної системи.

Об'єктивним чинником є те, що суспільству, яке за своїм характером є системним об'єктом, властива органічна тенденція впорядковувати своє існування. Така тенденція є об'єктивним процесом і в кінцевому підсумку не залежить від волі людей, хоча, звісно, вони можуть впливати на вибір тієї чи іншої форми впорядкування суспільного життя (наприклад, на встановлення форми держави, правових норм тощо).

Таким чином, впорядкування буття суспільства – це об'єктивна його потреба, але досягається ця мета за допомогою і в результаті взаємодії різноманітних об'єктивних та суб'єктивних факторів, впливу елементів системи один на одне. Внаслідок такого впливу і взаємодії вся система в цілому і кожен її елемент, зокрема, в певних умовах часу і простору існують найбільш оптимальним чином, що дозволяє говорити про певне саморегулювання суспільства або, у кожному разі, про існування такої тенденції.

Разом із тим, наявність певної тенденції суспільства до саморегуляції ще не дає підстав стверджувати, що закони функціонування та розвитку суспільства реалізуються автоматично.

Звідси випливає, що соціальне регулювання є предметом свідомої діяльності людей, яка ґрунтується на існуючих об'єктивних законах та, разом із тим, враховує їхні бажання.

Засобами соціального регулювання є: надання права робити щось; покладення обов'язку вчиняти певні дії; заборона вчиняти певні дії; застосування засобів соціального примусу та інших заходів впливу до порушників встановлених правил. Ці основні способи соціального регулювання доповнюються допоміжними: рекомендаціями, як те чи інше робити чи не робити; заохоченням, тобто заходами морального і матеріального стимулювання за виконання чи невиконання якихось дій.

Сукупність завдань соціального регулювання вирішується шляхом узгодження інтересів публічних (державних), колективних та приватних. У випадках неефективності соціального регулювання суперечності між цими інтересами можуть поглиблюватись у зв'язку, наприклад, зі зміною характеру політичних, культурних та економічних відносин, зміни умов господарювання, побутового життя тощо.

Результатом правового регулювання є виникнення правовідносин, котрі за сутністю є правовим зв'язком між суб'єктами правового впливу.

Класифікуючи правовідносини за різними підставами, їх можна поділити на:

1) відносини приватного та публічного права,

2) галузеві правовідносини: конституційно-правові, цивільно-правові, адміністративно-правові, карно-правові тощо,

3) відносини регулятивні та охоронні,

4) відносини матеріальні та процесуальні,

5) відносини правозастосовчі та правотворчі (правостворюючі).

При цьому базовим є поділ правовідносин на ті, що виникають у галузі приватного права, і ті, що виникають у галузі публічного права. Значення такої класифікації полягає в тому, що у залежності від того, чи є відносини публічно-правовими чи приватноправовими, визначається їхній зв'язок з певною галуззю національного права, а відтак, якими є їхні властивості. Отже, при аналізі правовідносин, що складаються у ІТ-сфері, у першу чергу, мають бути визначені властивості правовідносин з урахуванням їхнього існування у контексті дихотомії «приватне право – публічне право».

Крім того, беремо до уваги ту обставину, що, зазвичай, правовідносини у ІТ-сфері за своєю сутністю є регулятивними, котрі, у свою чергу, є частиною дихотомії «регулятивні правовідносини – охоронні правовідносини». Критеріями поділу у цьому випадку є врахування функцій та завдань, властивих галузі права, в межах якої виникають певні правовідносини. Із врахуванням цих чинників, згадані види правовідносин можна охарактеризувати наступним чином:

1) регулятивні правовідносини – це правовідносини, через які здійснюється безпосереднє правове регулювання (впорядкування) суспільного життя – встановлення юридичних прав та обов'язків тощо;

2) охоронні правовідносини – це правові відносини, які «оформлюють» кримінальну, адміністративну та інші види юридичної відповідальності, забезпечують застосування інших юридичних санкцій тощо.

Відповідно до того, чи є правовідносини регулятивними чи охоронними, визначаються підстави їхнього виникнення: перші виникають з правомірних дій суб'єктів, другі – є наслідком протиправних дій і пов'язані з застосуванням державного примусу.

У звичайних умовах функціонування ІТ-сфери внаслідок правового регулювання (впорядкування) відносин, які до неї належать, виникають регулятивні цивільні правовідносини, котрі є засобом і результатом соціального регулювання. У зв'язку з цим виникає необхідність розмежування регулятивних цивільних правовідносин та регулятивних адміністративно-правових відносин, з якими пов'язують виконання управлінських функцій державою та її фігурантами.

Порівнюючи ці види правовідносин, передусім, слід звернути увагу на таку характерну рису, властиву для всіх публічних правовідносин взагалі, як те, що вони є свого роду «первинними» стосовно суспільних (владних) відносин. Правові відношення у галузі публічного права взагалі, а отже і в галузі адміністративного права, що є головним проявом права публічного на рівні національному, виникають, змінюються та припиняються тільки на підставі (за умови наявності) правових норм, що містяться в актах законодавства, котрі безпосередньо породжують правові відношення і реалізуються через них. Між цими явищами (нормою, що встановлена актом адміністративного законодавства, та адміністративно-правовими відносинами) існує причинний зв'язок.

Саме у публічних, зокрема, адміністративно-правових відносинах досягається мета правової норми, проявляється її реальна сила та ефективність.

Зазначимо, що суспільні відносини у галузі приватного права за певних умов можуть опосередковуватися іншими (не юридичними) нормами. Тому у цій галузі можлива ситуація, коли цивільні відносини сторін взагалі можуть не потребувати правового втручання, якщо між учасниками таких відносин не виникло суперечки, або суперечка, яка виникла, урегульована за взаємною згодою сторін цих відносин.

Викладені положення слугують підґрунтям аналізу сутності правовідносин у галузі «ІТ-права» та їхнього співвідношення з категоріями «ІТ-відносини», «ІТ-правовідносини», «Інтернет-правовідносини» тощо, знімаючи, до речі, питання про доцільність характеристики відносин у цій сфері, як «не правових в чистому вигляді» і не «фактичних» відносин.

ІТ-право та інтерактивне громадянське суспільство

Розглядаючи «ІТ-право» як концепт, іманентно властивий сучасній цивілізації, сучасному постіндустріальному (інформаційному) суспільству, не можна залишити поза увагою його співвідношення з іншим популярним концептом – «громадянське суспільство», розбудова якого в Україні у сучасних умовах набула значення одного з чинників стійкості і перемоги у гібридній війні.

У сфері громадянського суспільства діють не громадяни як суб'єкти політично-владних відносин і публічного права, а приватні особи зі своїми інтересами, суб'єкти приватного права, учасники громадянсько-правових відносин.

При цьому йдеться про появу нового типу особи, існування високих вимог громадянського суспільства до його громадян, котрі вирізняють їх поміж людей, як таких… Основу громадянського суспільства становлять правосвідомі громадяни та їх добровільні об'єднання, існування яких регулює не політична влада, а самоуправління, вільне волевиявлення громадян і правовий закон. Громадянське суспільство має складну і плинну структуру: це комплекс соціальних груп, приватних осіб, їхніх асоціацій та інституцій (сім'я, школа, церква, добровільні об'єднання, клуби, спілки, громадські організації, рухи, політичні партії), взаємодія яких регулюється правом.[1]

Сутність громадянського суспільства полягає в тому, що воно є результатом узгодження інтересів та відносин, які формуються між приватними особами і створеними ними об'єднаннями, котрі існують та діють в умовах ринку.

[1] Біленчук П. Д., Гвоздецький В. Д., Сливка С. С. Філософія права: навчал. посібн. За ред. П. Д. Біленчука. К.: Атіка, 1999. С. 58-59.

Найбільш суттєві принципи громадянського суспільства склалися історично і сформульовані науковцями як його загальні ідеї: по-перше, економічна свобода, багатоманітність форм власності та ринкові відносини; по-друге, безумовне визнання і захист природних прав людини і громадянина, що передбачає рівність усіх перед законом; по-третє, відкритість та саморегуляція; по-четверте, розвиток демократії як політичного ідеалу і механізму життєдіяльності цієї системи; по-п'яте, наявність (розбудова) правової держави, яка ґрунтується на ідеї верховенства права, принципах поділу і взаємодії гілок влади та невтручання держави у приватне життя[1]. Держава не керує громадянським суспільством, але, якщо вона є правовою державою, зобов'язана забезпечити умови його функціонування і життєдіяльності, [2] оскільки принцип пріоритетного функціонування громадянського суспільства стосовно державної влади є характерним для генеральної динаміки розвитку сучасної світової цивілізації.[3]

Враховуючи названі ознаки громадянського суспільства, можна зробити висновок, що оцінка інформаційного суспільства як складової частини суспільства громадянського виглядає дещо ідеалізованою. Очевидно, «інформаційним» суспільству стати набагато простіше, ніж «громадянським» (звісно, за наявності належного рівня технологій). Тому інформаційне суспільство може бути частиною громадянського суспільства, але й може взагалі не мати сукупності ознак останнього.

Конструкція «інформаційне суспільство = громадянське суспільство стосується лише західної моделі інформаційного суспільства, де вони існують одночасно, що можна вважати «ідеальним випадком». Для такого випадку справедливим є твердження, з котрого, разом із тим, випливає, що інформаційне та громадянське суспільства співвідносяться як частина й ціле. Зауважимо, що таке бачення виглядає цілком логічним, оскільки «інформаційні прориви» чи «інформаційні

[1] Громадянське суспільство: політичні та соціально-правові проблеми розвитку: монографія. За ред. М. П. Требіна. Х.: Право, 2013. 536 с.

[2] Кузнєцова Н. Громадянське суспільство, держава, приватне право: проблеми співвідношення та взаємодії. *Право України.* 2014. № 4. С. 66.

[3] Оніщенко Н. До питання про пошук балансу у співвідношенні громадянського суспільства та держави: теоретико-методологічні аспекти. *Право України.* 2014. № 4. С. 55. Огляд та ґрунтовний перелік ознак громадянського суспільства див.: Колодій А. Громадянське суспільство: ознаки, структурні елементи, співвідношення із державою. *Право України.* 2014. № 4. С. 9-12.

революції» не є перманентними явищами, завдяки чому суспільство взагалі і громадянське суспільство, зокрема, може бути «інформаційним» різною мірою, і навіть, може не мати достатніх ознак останнього, тобто, бути «неінформаційним».

Принагідно зазначимо, що й тут не все у взаєминах інформаційної та громадянської частини суспільства виглядає так просто: у «комп'ютеризації суспільства» вбачають загрозу транснаціональної антиутопії, коли Інтернет з інструменту звільнення може перетворитися у небезпечний засіб тотального контролю. При цьому виникає колізія інтересів держави і особи, яку пропонується вирішити таким чином, аби гарантувати свободу волевиявлення там, де це можливо, і стримувати наступ антиутопії там, де перше неможливе.[1] Хоча існує і протилежна точка зору.[2]

Не зупиняючись на цьому питанні детальніше, оскільки воно заслуговує на окреме дослідження, зазначимо тут лише визначальні риси громадянського суспільства. Зокрема те, що воно: 1) є результатом договору (консенсусу) між приватними особами, 2) виникає та існує на підґрунті лібералізму, 3) існує в умовах розвиненого цивілізованого ринку, 4) притримується формули свободи, вираженої як соціальні імперативи демократії, 5) має основою взаємин між людьми активність демократичного і ліберального характеру, 6) розглядається, передусім, як феномен поведінковий та інституціональний; 7) не є об'єктом державного управління, претендуючи, натомість, на забезпечення державою умов його функціонування та життєдіяльності

Можна погодитися з розумінням громадянського суспільства як цілісної сфери громадського життя, відносно самостійної від державних інституцій і механізму державної влади. Громадянське суспільство – це унікальна система взаємодії суспільних індивідів, соціальних груп, верств і прошарків, що збалансовує вектори своїх складових, виявляючи рівнодіючу безлічі індивідуальних і групових прагнень та сподівань. Громадський лад своїм функціонуванням об'єктивно відтворює суспільні імперативи політичній системі, одно-

[1] Джуліан Ассанж Про майбутнє Інтернету. URL: http://interviews.com.ua/c/612-assange-internet/

[2] Вишневський А. Вплив інформатизації на розвиток громадянського суспільства. *Освіта регіону*. 2016. № 2. URL: ВПЛИВ ІНФОРМАТИЗАЦІЇ НА РОЗВИТОК ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА-> Стаття -> Український науковий журнал «ОСВІТА РЕГІОНУ» (uu.edu.ua)

часно зумовлюючи становлення таких державних форм, які були б спроможні адекватно реагувати на об'єктивні інтереси суспільства.[1]

В умовах становлення та розвитку інформаційного суспільства громадянське суспільство набуває нових рис, зумовлених тим, що важливу роль відіграють інформаційно-комунікаційні технології, які дозволяють збирати, обробляти, отримувати та передавати інформацію на локальному, загальнодержавному та міжнародному рівнях. Провідне місце серед таких технологій посідає Інтернет – глобальна телекомунікаційна мережа, яка з'явилася у 1969 р. і активно розвивається, починаючи з 80-х років XX ст. Основною метою Інтернет має поширення інформації серед користувачів, обмін такою інформацією. Він є унікальним засобом комунікації, що не знає часових і просторових меж, оскільки обмін інформацією відбувається блискавично і незалежно від відстані і кордонів. Всесвітня мережа у своєму розвитку пройшла три етапи.

Перший етап пов'язують з Web 1.0., функціонально обмеженою наданням користувачам можливостей читати інформацію і купувати речі.

Настання другого етапу (Web 2.0) припадає на початок 2000-х років, коли завдяки розвитку ІТ з'явились більш потужні веб-сайти і більш надійні веб-інфраструктури, що дозволило користувачам не лише споживати інформацію з Інтернету, але й публікувати її. На цьому етапі Мережа стала чимось більшим, ніж гігантський торговий центр і онлайн-енциклопедія, перетворившись на місце, де люди могли вчиняти різноманітні дії.[2]

З цим етапом можна пов'язувати формування інтерактивного громадянського суспільства, під яким розуміємо систему взаємодії вільних громадян та їх добровільних об'єднань за допомогою Інтернету, у якому інформація є головним чинником соціалізації, з метою формування механізму реалізації та захисту основних прав і свобод людини, задоволення індивідуальних та групових прагнень і сподівань, впливу на владні державні інституції, напрямок державного розвитку в цілому.

---

[1] Пасько І. Т., Пасько Я. І. Громадянське суспільство і національна ідея. (Україна на тлі європейських процесів. Компаративні нариси). Донецьк: ЦГО НАН України, УКЦентр, 1999. С. 46.

[2] Шмідт Е., Розенберг Дж. Як працює Google. Пер. с англ. Ю. Гордієнка. К: Видавнича група КМ-БУКС, 2016. С. 274-275.

Яскравим прикладом прояву інтерактивного громадянського суспільства, що формується у глобальних масштабах, можна вважати Avaaz – рух, котрий за допомогою Інтернету об'єднує небайдужих людей, працюючи 17 мовами у 193 країнах, вважаючи своєю демократичною місією «подолання дистанції між світом, у якому ми живемо, і світом, у якому хотілося б жити більшості людей». На його рахунку мобілізація широкої підтримки кліматичних акцій, що спонукали до Паризької кліматичної угоди; відстоювання безкоштовного і відкритого Інтернету;[1] рятування бджіл від пестицидів; акції за порятунок океану від пластика та ін.[2] Особливістю цього та інших рухів є те, що об'єднання користувачів Інтернет у цьому випадку не має постійного характеру. «Інтерактивність» є проявом мобілізації, активізації частини суспільства для вирішення певних завдань, висловлювання позиції з певного приводу, підтримки певних громадських ініціатив. Будь-хто з учасників руху Avaaz (при тому, що членства у русі, як такого, тут немає, а отже це може бути, практично, кожен, навіть, неофіт) має можливість запропонувати підтримати ініціативу стосовно вирішення важливої, на його думку, суспільної проблеми: підписати петицію, звернену до міжнародної організації, органів влади певної країни; зібрати кошти для матеріальної допомоги тощо.

Соціальні мережі

Новий етап розвитку громадянського суспільства інформаційної доби (інтерактивного громадянського суспільства) пов'язаний з появою соціальної мережі на основі платформи Facebook, завдяки якій люди отримали можливість обговорювати і ділитися інформацією про дії.[3] Завдяки Інтернету відбувається соціальна інтеграція як процес утворення взаємозв'язків між індивідами, групами, яскравим прикладом чого є створення соціальних мереж, які набувають все більшого значення і охоплюють все ширше коло учасників, стаючи невід'ємною ознакою інтерактивного громадянського суспільства.

---

1 https://www.avaaz.org/page/ru/highlights/?onb

2 https://mail.google.com/mail/u/0/#inbox/15c6cc2fd833243e

3 Шмідт Е., Розенберг Дж. Як працює Google. Пер. с англ. Ю. Гордієнка. К.: Видавнича група КМ-БУКС, 2016. С. 274-275.

Соціальні мережі (social network) – це соціальні структури, що утворюються окремими особами або організаціями з метою обміну інформацією, спілкування, комунікацій. Таким чином, стрімкий розвиток сучасних інформаційно-комунікаційних технологій створює таку ознаку диференціації суспільства, як ознака комунікативна. За допомогою комунікації суспільство може визначити себе, інформувати себе про власні інтелектуальні комунікації, піддавати інформацію сумніву, відхиляти її, нормувати комунікації як допустимі чи неприпустимі тощо.[1]

Соціальні мережі утворюються на різному підґрунті, об'єднуючи величезну кількість людей за інтересами, соціальним становищем, професійною, гендерною, віковою ознакою, навіть за національним принципом (Druzi.org.ua, Ukrainci.org – неполітична блого-соціальна мережа «Ми-Українці!». Останні з'явилися після Євромайдану 2013-2014 р.р., після анексії Криму і початку війни на Донбасі, внаслідок чого відбувся відтік україномовних користувачів з російськомовних соціальних мереж).

Цікавим і перспективним є розширення **соціальною мережею Facebook можливостей сервісу Safety Check, котрий автоматично активується у разі виникнення кризових ситуацій. Зокрема, у ньому буде доступна опція Community Help (допомога спільноти), яка сприятиме організації взаємодопомоги під час стихійного лиха.** Кожен користувач Facebook, який опинився у районі, де автоматично активується опція Safety Check (запускається у випадку, коли з одного місця надходить багато повідомлень про якесь лихо), зможе запропонувати оточуючим або замовити у них їжу, напої, дах над головою та можливість скористатися транспортним засобом. Для зручності відповідна сторінка Facebook містить категорії допомоги, а також її види (розділи «їжа», «дитячі речі», «одяг» тощо). Крім того, Community Help допоможе у пошуку людей у зоні лиха та забезпечить зв'язок з ними. Спочатку Community Help буде працювати у тестовому режимі лише в умовах природних катастроф і лише у США, Канаді, Австралії, Новій Зеландії, Індії та Саудівській Аравії. Після того, як виявлені за час тестового періоду недоліки будуть ви-

[1] Андреєв Д. Засоби масової інформації як механізм інтелектуальної комунікації в процесі розвитку інформаційного суспільства. *Теорія і практика інтелектуальної власності.* 2015. № 5. С. 56.

правлені, система стане доступною для усіх країн та для всіх кризових ситуацій.[1]

Разом із тим, поширення соціальних мереж стикається з істотними проблемами, значною мірою пов'язаними з недостатністю та вадами правового регулювання у цій сфері, на що зверталося увагу правознавцями.[2]

Зокрема, гострою є проблема долучення до соцмереж дітей, впливу таких мереж на дітей, відповідальності за завдання їм шкоди тощо.

Так, науковці з Університету Шефілда встановили, що чим більше часу діти проводять у оціальних мережах, тим більш нещасними вони почуваються майже в усіх аспектах життя. Як показали дослідження, проведені для інституту The IZA Institute of Labor Economics, перебування у соціальних мережах протягом лише однієї години на 14% знижує вірогідність того, що діти будуть повністю задоволені життям. Діти, які більше часу проводять у Facebook та Instagram, почуваються менш щасливими у тому, що їхньої успішності, зовнішності та родини. При цьому діти, які активно користуються соцмережами, більшою мірою задоволені стосунками з друзями.[3]

Зазначена проблема в Україні загострюється внаслідок недосконалості законодавства, котре не приділяє достатньої уваги регулюванню таких відносин. Так, поміж особистих немайнових прав і обов'язків батьків та дітей, передбачених ст. 13 СК України, певною мірою проблеми, про яку тут йдеться, стосуються лише положення про права батьків на виховання дитини, на представництво і захист прав та інтересів дитини, а також обов'язки батьків щодо виховання та розвитку дитини.

При цьому головною проблемою, як на наш погляд, є спірність питання стосовно того, чи є сам факт доступу до Інтернету корисним чи шкідливим для дитини. З одного боку, не викликає сумнівів, що Інтернет та соціальні мережі є цінним джерелом інформації і можуть

---

[1] Facebook вводит функцию взаимопомощи во время стихийных бедствий. URL: https://ru.slovoidilo.ua/2017/02/09/novost/obshhestvo/facebook-vvodit-funkciyu-vzaimopomoshhi-vo-vremya-stixijnyx-bedstvij

[2] Радейко Р. І. Соціальні мережі як об'єкт правового регулювання. *ІТ право: проблеми і перспективи розвитку в Україні:* зб. матер. наук.-практ. конф. (м. Львів, 18 лист. 2016 р.). Львів: НУ «Львівська політехніка», 2016. С. 133-136.

[3] Науковці: в нещасливому дитинстві – винні соцмережі. URL: http://glavnoe.ua/news/n304610

бути потужним засобом виховного впливу на дітей. Але так само не викликає сумнівів, що та сама Мережа може бути і джерелом негативної інформації та виховання негативних якостей у дитини. На сучасному рівні розвитку інформаційних технологій у батьків відсутня можливість ефективно контролювати функціонування системи «дитина – Інтернет (соціальна мережа)». Тому за наявності такого потужного конкурента було б невиправданим покладати лише на батьків відповідальність за виховання дітей у тих випадках, коли йдеться про факт існування згаданої вище системи «дитина – Інтернет (соціальна мережа)», ігноруючи при цьому факт існування іншого, «віртуального» чинника.

Варто згадати також, що у судовій практиці європейських країн вже з'явилися справи, пов'язані зі встановленням статусу користувачів соціальних мереж. Зокрема, осіб, які вважаються «друзями» у Facebook.

Так, Касаційний суд Франції у рішенні, опублікованому 5 січня 2017 р. визнав друзів у Facebook «несправжніми друзями», зазначивши, що дружба у соціальних мережах не вважається дружбою у «традиційному» розумінні. Справа розглядалася за заявою паризького адвоката у зв'язку з тим, що адвокатська колегія розглядала скаргу одного з членів проти позивача і при цьому скаржник і член цієї колегії були друзями у Facebook. На цій підставі позивач звинуватив колегію в упередженості. Суд не погодився з його доказами, вважаючи, що дружба у Facebook не вплинула на думку Колегії.

Однак у 2015 р. аналогічна справа розглядалася у Бельгії. Суд зобов'язав бельгійця платити колишній дружині аліменти. Той вимагав скасувати це рішення, оскільки адвокат його дружини був другом судді у Facebook. У цьому випадку Верховний суд погодився із заявником.[1]

Як на нашу думку, «дружба у Facebook» не є дружбою у «традиційному» розумінні, однак може бути оцінена судом як обставина, що загрожує упередженим розглядом спору, суперечки тощо.

Однією з проблем соціальних мереж є так звані «тролі», котрі діють у мережах поза межами правового поля, виконуючи за плату різ-

[1] https://meduza.io/news/2017/01/09/frantsuzskiy-sud-ob-yavil-druzey-na-feysbuke-nenastoyaschimi-druzyami?utm_source=facebook.com&utm_medium=share_fb&utm_campaign=share

номанітні функції сумнівної якості. Одна з таких функцій це створення уявлення, що потрібні меседжі підтримує велика кількість людей. Іншим завданням тролів є виводити їхніми «коментами» з себе тих, кого їм задають як супротивника. Існує думка, що реально тролі – це намагання держав повернути собі контроль за соціальними медіа. Наприклад, Facebook, що за визначенням є інструментом з індивідуального породження інформації, завдяки тролям отримує «індустріальний» потік інформації, який завжди буде набагато сильнішим, оскільки він несе єдиний меседж. Деякі країни (Китай, Ізраїль, Росія) мають свої команди тролів, які повинні допомогти їм опанувати вільний чи квазі-вільний Інтернет.[1]

Не зайве підкреслити, що згадані та інші проблеми значною мірою зумовлені недостатністю правового регулювання на тому тлі, що, функціонування складної системи інтерактивного громадянського суспільства потребує багатовекторного і багатогалузевого законодавчого забезпечення, чим, власне, і зумовлене значення розвитку «ІТ-права».

Характер співвідношення інтерактивного громадянського суспільства та «ІТ-права» залежить від того, у якому сенсі розглядається останнє: у широкому, вузькому чи спеціальному значенні.

Якщо йдеться про «ІТ-право» у широкому сенсі, під яким розуміється сукупність усіх норм і правил, що регулюють діяльність по використанню інформаційних технологій та інформаційної правомірної активності в Інтернеті, то з таких позицій цілком очевидно, що усі відносини інтерактивного громадянського суспільства є правовим полем «ІТ-права» у широкому сенсі, включаючи як приватноправові, так і публічно-правові його складові.

Але, якщо маємо на увазі «ІТ-право» у вузькому сенсі, тобто регулятивні норми (переважно цивільно-правові), що забезпечують функціонування ІТ-відносин у цивільному (торговому) обігу, то тут, фактично, йдеться про правове регулювання на засадах цивільного права з усіма завданнями, що постають перед цією галуззю у громадянському суспільстві. Разом із тим, на нього покладаються додаткові завдання впорядкування відносин за участі члена такого суспільства (так званої, модульної людини) – забезпечення можливості

[1] Бойко М., «Вголос». 9 березня 2017 р. URL: http://www.ji-magazine.lviv.ua/2017/Pocheptsov_Vijna_4_pokolinnya.htm

створення громадських організацій, їхньої діяльності та участі в них особи; гарантування здійснення права громадської активності тощо.

Що стосується «ІТ-права» у спеціальному сенсі, яким є сукупність норм та правил, що стосуються суто сфери ІТ-відносин, то у контексті буття громадянського суспільства воно виконує «службову» роль, впорядковуючи інформаційно-комунікаційні відносини; відносини створення та використання програмного забезпечення; інтернет-відносини тощо.

ІТ-сфера, ІТ-відносини та їхнє впорядкування

Розвиток інформаційних технологій, які істотно впливають на соціальні процеси, стали чинником інформаційної революції, котра, у свою чергу, зумовлює необхідність удосконалення правового регулювання діяльності суб'єктів інформаційних відносин, виробництва, використання, поширення та зберігання електронної інформаційної продукції, захисту прав на інтелектуальну власність тощо.

Разом із тим, виникає низка проблем, пов'язаних з поширенням у суспільстві інформаційно-комунікативних технологій, принаймні частина яких може бути вирішена правовими засобами шляхом впорядкування відносин, що складаються у цій сфері, та узгодженням інтересів їх суб'єктів. Цим і зумовлюється актуальність вивчення категорії «ІТ-право», про яку останнім часом усе частіше говорять не лише науковці, але й практики.

Зазначимо, що зараз до ІТ-сфери відносять широке коло різноманітних відносин, які регулюються нормами цивільного, господарського, адміністративного законодавства. Зокрема, у сферу цивільно-правового регулювання попадають «ІТ-відносини» надання послуг програмного забезпечення або його розробки; правового захисту web-сторінок і контенту; юридичної допомоги у відкритті ІТ-бізнесу; юридичного аудиту ІТ-компаній; юридичного обслуговування фрілансерів; оформлення та захисту авторських прав і торгової марки в Інтернет; оформлення договорів купівлі-продажу сайту, домену, бренду тощо; правового забезпечення діяльності Інтернет-магазинів; створення і реєстрації юридичних осіб у цій галузі; ліцензійних угод; захисту прав інтелектуальної власності; захисту інформації тощо.[1]

[1] Бачинський Т. Основи ІТ-права. Львів: Апріорі, 2016. 136 с.

Звернемо увагу на те, що у контексті дослідження особливостей предмету правового регулювання у ІТ-сфері, використовуються терміни «інформаційні відносини», «інформаційно-комунікативні відносини», «Інтернет-відносини», а також абревіатура «ІТ-відносини»,[1] котру точніше розшифровувати не буквально, а за сутністю – «інформаційно-технологічні відносини».

Найбільш популярними з них, як об'єкт дослідження, є «Інтернет-відносини», котрі, водночас, є лише частиною більш загальної категорії «ІТ-відносини», під якими розуміємо усю сукупність суспільних відносин, що виникають у процесі створення і використання інформаційних технологій. «ІТ-відносини» є загальною категорією, що охоплює також і відносини, які складаються у Інтернеті. Разом із тим, останні можуть і не бути «інформаційними», у точному значенні цього слова. Наприклад, у процесі електронної торгівлі може застосовуватися низка категорій, котрі не несуть інформаційного навантаження, а мають «технологічне» значення при оформленні договору, його засвідченні тощо (електронний підпис, електронні реєстри і т.п.).

Таким чином, категорія «ІТ-сфера є ширшою, ніж «Інтернет», оскільки стосується також відносин, що складаються поза Мережею.

З'ясовуючи співвідношення ІТ-відносин та відносин інформаційних, згадаємо про існування у вітчизняній правовій доктрині широкого спектру поглядів стосовно природи, об'єкту, особливостей тощо останніх.[2] Тому тут лише зазначимо, що, хоча вони мають багато спільного, але не є тотожними. Співвідношення між ними виглядає як часткове накладення кіл, оскільки не всі інформаційні відносини є «технологічними», так само, як не всі «технологічні» – є інформаційними.

Отже, маємо загальну категорію «ІТ- відносин», котра охоплює усю сукупність стосунків між людьми, де мають місце (значення, використовуються) інформаційні (інформаційно-комунікативні) технології. (Припускається, що у перспективі учасником таких відносин може бути і штучний інтелект, але до цього ще маємо трохи часу).

Оскільки маємо справу зі складною системою, котра включає низку підсистем, які у цілому та кожна окремо природно ґрунтуються на систематизації і тяжіють до впорядкування, гостро постає про-

[1] ІТ-право: проблеми і перспективи розвитку в Україні: збірник матеріалів науково-практичної конференції. Львів: НУ «Львівська політехніка», 2016. 396 с.

[2] Кодинець О. А. Цивільно-правове регулювання зобов'язальних інформаційних відносин: методологія, теорія, практика: дис…. докт. юрид. наук: 12.00.03. К., 2016. С. 18-24.

блема впорядкування та обрання засобів впорядкування, визначення пріоритетів тощо.

Зазначимо, поки, що порядкування відносин у ІТ-сфері можливе двома шляхами:

1) за допомогою правового регулювання;

2) за допомогою ІТ-засобів (використання можливостей інформаційних технологій).

Із врахуванням існування зазначених шляхів далі детальніше розглянемо проблеми, які тут виникають і мають бути вирішені.

Юридичне забезпечення прав та регулювання «ІТ-сфери»

Відправним моментом при розгляді цього питання є розуміння права як концепту, що поєднує два його бачення: як категорії об'єктивної та як категорії суб'єктивної.

Аналізуючи природу суб'єктивних прав, слід зазначити, що остання залежить від того, яким є підхід до правового регулювання відповідних суспільних відносин: приватноправовим чи публічно-правовим. Приватноправовий підхід ґрунтується на визнанні природних, невідчужуваних прав особи, які не створюються, а лише визнаються і підтверджуються нормами законодавства. Публічно-правовий підхід має основою твердження, що держава не визнає, а створює права особи, наділяючи ними окремих громадян і визначаючи тим самим обсяг правоздатності, а отже й обсяг потенційних суб'єктивних прав кожного з них, який може бути збільшений або зменшений на розсуд самої держави.

З урахуванням викладеного можна зробити висновок, що при характеристиці суб'єктивних прав, засобів їхнього юридичного забезпечення тощо, необхідно, передусім, встановити, чи належать вони до сфери приватного, чи публічного права, тобто чи є елементом зв'язків «горизонтального», чи «вертикального» типу. Відповідно до цього вся система суб'єктивних прав може поділятися на публічні та приватні суб'єктивні права, від чого й залежать засади їхнього юридичного забезпечення.

Зауважимо, що при розгляді цього питання не завжди розрізняються «юридичне (правове) забезпечення» і «правове регулювання».

Зустрічаються, щоправда, праці, у яких поняття «правове забезпечення» розглядається як складна категорія, котра не зводиться до правого регулювання якогось виду суспільних відносин. Так, О. К. Вишняков, розглядаючи напрями правового забезпечення зовнішньоекономічної інтеграції України, поділяв їх на загальні та окремі, визначаючи перший як зняття існуючих взаємних претензій між Україною і ЄС і перехід на новий ступінь стосунків, і, відносячи до другого – імплементацію міжнародних договорів України та інших міжнародно-правових документів, регулювання підприємницьких відносин, інвестиційне регулювання та правову охорону іноземної власності, реформу судової системи та захист приватного бізнесу.[1] Отже, під «правовим (юридичним) забезпеченням» тут мається на увазі не лише правове регулювання суспільних відносин, але й організаційно-правові заходи, що вживаються для досягнення певної мети.

Далі виходимо з того, що «юридичне забезпечення» – це створення юридичними засобами надійних умов для здійснення чогось, вирішення якихось завдань, що являють інтерес для індивіда, суспільства (держави).

Відтак маємо враховувати, що для забезпечення впровадження цивілізаційних феноменів (яким, зокрема, є право) у певне суспільство, держава, як механізм організації життя цього суспільства, має здійснювати в межах правового поля низку заходів. Таким чином відбувається «об'єктивізація» згаданих феноменів (зокрема, права), перехід їх з абстрактного цивілізаційного рівня на рівень цінностей суспільства, правових конструктів та категорій, інституцій відповідної держави.

Держави має докласти значних зусиль, аби впровадити певні цивілізаційні феномени, ідеологію, концепти тощо в життя суспільства. Зокрема, йдеться про створення «ІТ-права», котре формується як симбіоз віртуальної та дійсної реальності, що відображає спроби ввести у звичне правове поле ІТ-відносини, віртуальні за своєю сутністю.

Згаданих зусиль має докладати не лише держава, а й суспільство, оскільки без цього процес уповільнюється, а іноді взагалі стає неможливим. Така умова не є обов'язковою. Проте, у випадках, коли держава проголошує, а іноді – нав'язує суспільству цінності, які суперечать його ментальності і природному шляху еволюції, існує вірогідність

[1] Вишняков О. К. Правове забезпечення зовнішньоекономічної інтеграції України: моногр. Одеса: Юридична література, 2007. С. 66-132.

зворотності процесу. Отже юридичне забезпечення ІТ-сфери не може зводитись лише до видання нормативних актів, а потребує вжиття низки організаційних заходів.

При цьому, оскільки діяльність держави є лише одним із засобів юридичного забезпечення, маємо розрізняти державне та недержавне (громадське) юридичне забезпечення.

У свою чергу, діяльність держави по юридичному забезпеченню ІТ-сфери здійснюється за наступними напрямками:

1) методологічне та доктринальне забезпечення. Розробка концепції, визначення засад юридичного забезпечення тощо; підтримка певної доктрини права. Сюди слід віднести також ідеологічне забезпечення, як форму державних зусиль по створенню світоглядного підґрунтя впровадження нових правових конструктів і концептів у ІТ-сфері;

2) законодавче забезпечення. Сюди можна віднести видання актів законодавства, санкціонування правових звичаїв та норм моралі, що стосуються об'єкта законодавчого забезпечення (ІТ-відносин);

3) забезпечення належної реалізації норм законодавства, які стосуються об'єкта забезпечення (ІТ-відносин), за допомогою відповідних державних інституцій, судової системи;

4) інформаційно-пропагандистське (виховне) забезпечення. Роз'яснення сутності положень, що впроваджуються, мети впровадження тощо. Правова освіта, яка здійснюється у певному напрямку юридичного забезпечення ІТ-сфери;

5) організаційне забезпечення. Визначаються органи, що відповідають за конкретні напрями впровадження, їх компетенція, взаємодія тощо.

Що стосується недержавного (громадського) юридичного забезпечення, то до його форм (видів), передусім, належать:

1) світоглядне забезпечення підґрунтя, яке охоплює й правоментальність суспільства. Цінності, інституції, категорії, поняття, які впроваджуються, мають або бути такими, що не суперечать світогляду більшості суспільства, або адаптованими до визнаних у ньому світоглядних засад;

2) доктринальне забезпечення – у тій його частині, що виникає незалежно від завдань держави щодо наукових розробок (і навіть, попри не зацікавленості держави у таких розробках). Впровадження

правових цінностей, системи права, правових інститутів, державних інституцій має відбуватися за умови готовності до такого впровадження з боку правознавців – фахівців у цих та суміжних галузях;

3) правосвідомість суспільства (населення). Правосвідомість може слугувати як стимулюючим, так і гальмуючим чинником. Цінності можуть впроваджуватися на вже існуюче підґрунтя, але, частіше, така основа формується у процесі їхнього впровадження.

При цьому недержавне (громадське) юридичне забезпечення слід відрізняти від «недержавної системи безпеки», під якою мається на увазі об'єднання зусиль держави та недержавних без пекових структур і організацій тощо з метою організації ефективного захисту національної економіки (підприємництва).[1]

Отже, юридичне забезпечення ІТ-сфери здійснюється шляхом використання правових засобів (формування «ІТ-права», «ІТ-законодавства» тощо), а також організаційних зусиль державних органів управління та громадських інституцій (інтерактивного громадянського суспільства).

«ІТ-право» як феномен правового регулювання

Попри те, що останнім часом термін «ІТ-право» широко використовується як науковцями, так і практиками для позначення норм, що стосуються сфери ІТ-відносин, загально визнане бачення сутності цього явища у вітчизняній юриспруденції ще не сформувалося.

Зокрема, «ІТ-право» розуміють як сукупність норм, що регулюють діяльність по забезпеченню інформаційної активності в Інтернет та безпеки інформаційних технологій (тобто, інформаційної безпеки). Водночас, ІТ-право характеризують як мультидисциплінарну науку, як міжгалузевий інститут права [2] тощо.

Звідси випливає, що значення надається двом ознакам «ІТ-права»: 1) цей феномен пов'язаний зі сферою ІТ-відносин; 2) він є сукупністю норм (тобто, визначати це «право» пропонується з «нормативістських» позицій).

---

[1] Крутов В. В., Пилипчук В. Г. Недержавна система безпеки (проблеми становлення і розвитку): монографія. Ужгород: ТОВ «ІВА», 2013. С. 12.

[2] Бачинський Т. Основи ІТ-права: посібн. Львів: Апріорі, 2016. С. 3.

Розглянемо їх детальніше.

Відразу відмовимось від характеристики «ІТ-права» як комплексної галузі права, оскільки такий підхід, за своєю сутністю, є не вирішенням завдання, а, швидше, ухиляннням від з'ясування його сутності. Власне, нічого не додає до усвідомлення сутності «ІТ-права» і визнання його міжгалузевим інститутом права.

Постає питання, чи можна вважати феномен «ІТ-права» галуззю права (законодавства) у традиційному значенні.

Аналізуючи «інформаційні відносини», «інформаційно-комунікативні відносини», «Інтернет-відносини», а також терміно-поняття «ІТ-відносини»,[1] котрий точніше «розшифровувати» не буквально, а за сутністю – «інформаційно-технологічні відносини», і враховуючи викладене раніше стосовно розмаїття буття ІТ-сфери, можна зробити висновок про відсутність підстав розглядати «ІТ-відносини» як цілісний предмет правового регулювання.

Натомість, має йтися про сукупність відносин, пов'язаних зі сферою інформаційних технологій та суміжними сферами. Ці відносини можуть бути цивільними, адміністративними, фінансовими, корпоративними тощо.

До них застосовуються різні методи правового регулювання, (тобто, сукупності специфічних прийомів юридичного впливу на учасників суспільних відносин): як імперативний, так і диспозитивний. Імперативний метод (метод субординації) характеризується тим, що регулювання здійснюється згори вниз і ґрунтується на владно-імперативних засадах. Диспозитивний метод (метод координації) характерний для регулювання на засадах формальної рівності, ініціативності та вільного розсуду учасників відповідних відносин. На процес такого регулювання впливає активність учасників суспільних відносин, які регулюються за його допомогою. У характерних рисах диспозитивного методу проявляються особливості приватного права як наднаціонального феномену, що складається, передусім, із сукупності гуманітарних ідей, правових принципів, правил і норм, що стосуються визначення статусу і захисту інтересів окремої особи (людини).

«Диспозитивний» та «імперативний» методи у різному співвідношенні присутні у галузях права (законодавства), дотичних до ІТ-сфе-

[1] ІТ-право: проблеми і перспективи розвитку в Україні: збірник матеріалів науково-практичної конференції. Львів: НУ «Львівська політехніка», 2016. 396 с.

ри. Так, для цивільних норм, якими регулюються майнові та немайнові відносини між приватними особами у реальному та віртуальному світі (реалізація права власності, договори про надання послуг, виконання роботи, передачу прав тощо) властивим є диспозитивний метод правового регулювання. Для норм, спрямованих на асекуризацію інформаційної безпеки у цій сфері, захист немайнових прав, інтелектуальної власності, здійснення митного, фінансового, податкового контролю тощо, властивим є застосування методу імперативного.

Ця обставина дає підстави для висновку, що, так само як єдиний предмет, відсутній і спеціальний метод правового регулювання відносин у ІТ-сфери. Натомість, залежно від типу відносин, що регулюються і конкретних завдань можуть застосовуватися цивільно-правовий, адміністративно-правовий та інші методи.

(Тут варто згадати про існування позиції, згідно якій ознакою інформаційного законодавства є «метод правового регулювання – системне комплексне застосування методів цивільного, адміністративного і кримінального права (що визначає міжгалузеву сутність публічно-правового регулювання) з урахуванням методів приватноправового регулювання (на рівні угод, добрих звичаїв, традицій, норм суспільної моралі, ділової етики. Але залишається нез'ясованим питання, чим відрізняється застосування усього того, що входить до цього «комплексу» методів, від звичайного застосування цивільно-правового, адміністративно-правового тощо методів у багатьох інститутах чи підгалузях права, скажімо, у праві інтелектуальної власності, спадковому праві, транспортному праві тощо)».[1]

Об'єднуючим чинником норм, що діють стосовно ІТ-сфери, здавалося б, могли б слугувати функції «ІТ-права», тобто головні напрями впливу правових норм на суспільні відносини з метою впорядкування останніх. Тому тут варто коротко згадати основні риси цієї категорії.

Передусім зауважимо, що розрізняють функції, які є спільними для права взагалі, і функції, що є специфічними для певної галузі (специфічні галузеві функції).

Загально-правовими функціями, що проявляються на рівні галузі права, є: 1) функція інформування про правила поведінки; 2) функція

[1] Пилипчук В. Г., Дзьобань О. П. Інформаційне суспільство:філософсько-правовий вимір: моногр. Ужгород: ТОВ «ІВА», 2014. С. 225.

виховання учасників відносин (превентивна); 3) функція регулювання відносин, яка полягає у наданні їх учасникам прав та обов'язків, встановленні правил їхньої поведінки; 4) функція захисту (відшкодування шкоди тощо). Ці функції властиві кожній галузі права, але набувають специфічних властивостей за рахунок предмету (сфера відповідних відносин), методу правового регулювання та засад, на яких здійснюється досягнення мети.

Крім того, галузь права виконує специфічні функції, властиві лише їй, оскільки в інших галузях така мета, як правило, не ставиться).

Але, якщо «ІТ-відносини» не можуть розглядатися як цілісний предмет правового регулювання, тобто, як суспільні відносини, що знаходяться у правовому полі і можуть бути піддані впливу юридичних норм за допомогою певних правових засобів (методів), то і спеціальних галузевих функцій правового регулювання тут не існує.

Отже «ІТ-право» не може розглядатися як самостійна (чи комплексна чи ще якась галузь права), оскільки не відповідає таким критеріям, як наявність самостійних предмету та методу правового регулювання.

Таким чином, оскільки стосовно «ІТ-права», фактично, має місце спроба комплексного підходу до правового регулювання різноманітних відносин інформаційного суспільства, не коректно оцінювати сутність та співвідношення відповідних нормативних масивів з позицій «нормативістського» підходу.

Тому слід визнати, що «ІТ-права», так само, як «Інтернет-права», «інформаційного права» тощо, як галузей права, не існує.

Натомість, з певними застереженнями, може йтися про «ІТ-законодавство», яке застосовується до відносин, що виникають при використанні інформаційно-комунікаційних технологій, хоча часом цей термін не має змістовного наповнення. Втім, слід зазначити, що й у цьому разі йдеться не про «ІТ-законодавство», як галузь, а лише про «віртуальну» сукупність норм, що регулюють різноманітні відносини тим чи іншим чином поєднані зі створенням та використанням інформаційних технологій.[1]

[1] Пестова К. В., Кравчук В. В. ІТ-законодавство: проблеми, пріоритети та напрями розвитку. *ІТ-право: проблеми і перспективи розвитку в Україні:* збірник матеріалів науково-практичної конференції. Л.: НУ «Львівська політехніка», 2016. С.126-127.

Звісно, це не означає неможливості використання терміну «ІТ-право», так само, як не викликає сумнівів можливість визнання існування феномену «ІТ-права». Однак останнє має характеризуватися з позицій не «нормативізму (позитивізму)», а «цивілізаційного» підходу, коли право розглядається як цивілізаційний феномен, котрий одночасно виступає як елемент соціально-політичного устрою та елемент суспільної свідомості.

Отже «ІТ-право» можемо розглядати як концепт (conceptus – думка, уявлення, поняття), тобто як сукупність уявлень, понять, знань, асоціацій, емоцій, що виникають у зв'язку з використанням терміну «ІТ-право», супроводжують і характеризують його.

Однак лише констатація цієї обставини не відповідала б потребам правового регулювання ІТ-відносин в інформаційному суспільстві. Можна, навіть, вважати таке рішення ухиляннням від відповіді на виклик часу. Тому маємо дати характеристику «ІТ-права», як концепту.

Отже, виходимо з того, що «ІТ-право» («ІТ-законодавство») є позірною (уявною) сукупністю норм, що регулюють відносини, тим чи іншим чином поєднані зі створенням та використанням інформаційних технологій.

Сфера «ІТ-права» охоплює норми цивільного, господарського, адміністративного, карного, митного, податкового права тощо, котрі складають його як мозаїка певне цілісне полотно. Особливо багато різноманітних ІТ-відносин виникає у сфері цивільно-правового регулювання.

Оскільки розмаїття ІТ-відносин створює на практиці істотні незручності при пошуку та застосуванні актів законодавства, які стосуються таких відносин, виникає необхідність визначення орієнтирів для встановлення кола норм, які можуть бути віднесені до сфери «ІТ-права».

При цьому враховуємо наступні засади визначення правового масиву у ІТ-сфері:

1) до сфери «ІТ-права» доцільно відносити лише регулятивні відносини, і відповідно, норми законодавства, що їх регулюють;

2) при систематизації та структуруванні «ІТ-права» має бути розрізнення цього поняття у широкому та вузькому сенсі;

3) під «ІТ-правом» у широкому сенсі розуміємо сукупність усіх норм і правил, що регулюють діяльність по використанню інфор-

маційних технологій та інформаційної правомірної активності в Інтернеті;

4) структура «ІТ-права» у широкому сенсі виглядає як відносно інтегрована система багаторівневого порядку, котра містить приватноправові та публічно-правові елементи, питома вага яких визначається пріоритетністю інтересів (приватні чи публічні). На цьому підґрунті визначаються особливості методів правого регулювання, що застосовуються у тих та інших випадках;

5) переважання публічних інтересів (забезпечення інформаційної безпеки тощо) означає, що відповідні відносини регулюються лише нормами актів законодавства і не можуть бути змінені або припинені за домовленістю;

6) ІТ-відносини, що належать до приватноправової сфери правового регулювання, переважно є регулятивними, але у деяких випадках можуть також супроводжуватися організаційними відносинами (створення юридичних осіб). Оскільки йдеться про сферу приватного права, де діє принцип «Дозволено все, що не заборонено законом», існування якого забезпечує надання договору значення норми цивільного законодавства, саме за його допомогою складається основний масив норм ІТ-права.

Таким чином, «ІТ-право» у вузькому сенсі може розглядатися як регулятивні норми (переважно цивільно-правові), що забезпечують функціонування ІТ-відносин;

7) можливе також виокремлення «ІТ-права у спеціальному сенсі». При цьому до відповідного нормативного масиву мають бути віднесені вже лише ті норми, що стосуються суто сфери ІТ-відносин: інформаційних відносин; створення та використання програмного забезпечення; інтернет-відносин тощо.

У підсумку можемо зазначити, що фактично йдеться про створення та визнання парадигми: «ІТ-право» – концепт», яка є альтернативою позиціям, котрі зараз набули певної популярності у вітчизняній юриспруденції, але не забезпеченні відповідним науково-теоретичним підґрунтям. Такий підхід дає можливість зняти проблеми методологічного характеру, котрі неминуче виникають при спробах визначення «ІТ-права» на основі традиційного «нормативістського» розуміння права.

Структура «ІТ-права»

Ґрунтуючись на такому розумінні «ІТ-права», можна визначити його структуру (точніше кажучи, основні напрями правового регулювання у ІТ-сфері).

Як згадувалося, наразі до сфери «ІТ-права» включають норми цивільного, господарського, адміністративного, карного, митного, податкового права тощо, котрі складають його як мозаїка певне цілісне полотно.

Але особливо багато різноманітних ІТ-відносин виникає у сфері цивільно-правового регулювання.

Зокрема, сюди відносять: 1) ІТ-договори надання послуг програмного забезпечення або його розробки; 2) ІТ-договори роботи із фізичною особою підприємцем або програмістами; 3) юридичний супровід фрі-лансерів; 4) юридичний аудит ІТ-компаній; 5) правовий захист web-сторінок і контенту; 6) оформлення та захист авторських прав і торгової марки в Інтернет; 7) оформлення договору купівлі-продажу сайту, домену, бренду тощо; 8) правове забезпечення діяльності інтернет-магазинів; 9) створення і реєстрація юридичних осіб у цій галузі; 10) ліцензійні угоди; 11) захист прав інтелектуальної власності; 12) захист інформації тощо.

Таке широке коло відносин (а відтак і правовідносин), які вважаються ІТ-відносинами, потребує систематизації норм, які можуть бути віднесені до сфери «ІТ-права».

Почати, вважаємо, слід з винесення за межі «ІТ-права» норм адміністративного, карного, митного, податкового тощо права, оскільки зазначені галузі, як управлінські та охоронні, стосуються (можуть стосуватися) різних видів суспільних відносин, забезпечуючи їхнє впорядкування та охорону. Рівною мірою це можуть бути, скажімо, підприємницькі, аграрні, транспортні, екологічні тощо відносини. Навряд чи, є достатні підстави для включення норм згаданих «забезпечуючих» галузей до складу кожної галузі чи підгалузі права, котру вони «обслуговують». В іншому разі, довелось би книги «Право власності та інші речові права», «Право інтелектуальної власності», «Зобов'язальне право», «Спадкове право» вилучати з Цивільного кодексу, а відповідні розділи цивільного права виводити за межі цієї галузі, оскільки відносини, які регулюються нормами, що містяться

в цих книгах, «обслуговуються також нормами адміністративного, карного, митного, податкового тощо права».

Таким чином, до сфери дії, власне, «ІТ-права» доцільно відносити лише регулятивні відносини, і відповідно, норми законодавства, що їх регулюють.

Наступним кроком систематизації та структурування «ІТ-права» має бути згадуване вище розрізнення цього поняття у широкому та вузькому сенсі.

Під «ІТ-правом» у широкому сенсі розуміємо сукупність усіх норм і правил, що регулюють діяльність по використанню інформаційних технологій та інформаційної правомірної активності в Інтернеті. Структура «ІТ-права» у широкому сенсі виглядає як відносно інтегрована система багаторівневого порядку, що містить приватноправові та публічно-правові елементи. Необхідність врахування приватноправового та публічно-правового забарвлення ІТ-відносин має враховуватися, аби визначити пріоритетність інтересів (приватні чи публічні) і на цьому підґрунті особливості методів правого регулювання, що застосовуються. Разом із тим, публічно-правові за своєю сутністю ІТ-відносини, можуть складатися і в галузі цивільного права. Наприклад, такими є відносини цивільної відповідальності, відшкодування шкоди, завданої цивільними правопорушеннями у сфері ІТ-відносин. Вони виникають не з правомірних дій; їхні суб'єкти, зміст, підстави і порядок виникнення та припинення визначаються безпосередньо нормами законодавства. Згадані вище відносини за своєю сутністю є або організаційними, або охоронними і ніколи не бувають регулятивними.

Врахування цієї обставини має прагматичне значення, оскільки на практиці потребує врахування тієї обставини, що такі відносини регулюються лише нормами актів законодавства і не можуть бути змінені або припинені за домовленістю.

ІТ-відносини, пов'язані зі створенням та припиненням юридичних осіб, відносини інтелектуальної власності, договірні відносини за участі суб'єктів ІТ-відносин, відносини спадкування тощо, належать до приватноправової сфери правового регулювання. Такі відносини переважно є регулятивними, але у деяких випадках можуть також супроводжуватися цивільними організаційними відносинами (у галузі створення та діяльності юридичних осіб). Оскільки йдеться

про сферу приватного права, де діє принцип «Дозволено все, що не заборонено законом», існування якого забезпечує надання договору значення норми цивільного законодавства, можна стверджувати, що саме за його допомогою складається основний масив норм ІТ-права.

Таким чином, «ІТ-право» у вузькому сенсі це регулятивні норми (переважно цивільно-правові), що забезпечують функціонування ІТ-відносин.

Перед тим, як визначити структуру «ІТ-права» у вузькому сенсі, слід врахувати доцільність виокремлення групи норм, присвячених загальним положенням законодавства, що стосуються ІТ-права..

Із врахуванням зазначеного, структура «ІТ-права» у вузькому сенсі виглядає наступним чином:

1) норми цивільного законодавства, що стосуються ІТ-відносин (можуть бути застосовані для регулювання ІТ-відносин). До них належать засади цивільного законодавства; положення про аналогію закону та аналогію права; підстави виникнення цивільних прав та обов'язків у сфері ІТ-відносин; самозахист та захист суб'єктивних прав; положення про об'єкти цивільних прав, зокрема, про інформацію, як такий об'єкт; положення про правочини; представництво; строки та терміни; захист особистих немайнових прав фізичної особи тощо;

2) норми, що стосуються суб'єктного складу ІТ-відносин. Сюди мають бути віднесені положення про створення та припинення юридичних осіб; визначення видів юридичних осіб і форм товариств, які можуть створюватися для забезпечення діяльності у ІТ-сфері; положення про внесення продуктів ІТ у якості частки у статутному фонді; норми, що опосередковують внутрішньо корпоративні відносини; захист прав корпорацій;

3) норми цивільного законодавства, що стосуються прав інтелектуальної власності. Зокрема, положення, що стосуються визначення інформації та об'єктів прав інтелектуальної власності; правового обслуговування програмного забезпечення; захисту інформації та прав інтелектуальної власності; оформлення та захисту авторських прав і торгової марки в Інтернет; правовий захист web-сторінок і контенту; положення про ліцензійні угоди тощо;

4) норми цивільного законодавства, що стосуються договорів у сфері ІТ-відносин. Зокрема, загальні положення про договори, їх

укладення, зміну, виконання, припинення та способи забезпечення належного виконання; договори про надання послуг програмного забезпечення або його розробки; договори роботи із фізичними особами-підприємцями або програмістами; договори про юридичний супровід фрі-лансерів; договори про юридичний аудит ІТ-компаній; договори купівлі-продажу сайту, домену, бренду тощо; договори про правове забезпечення діяльності інтернет-магазинів; концесійні договори; ліцензійні угоди; договори про сумісну діяльність у сфері ІТ-відносин тощо;

5) норми цивільного законодавства, що стосуються недоговірних відносин у сфері ІТ. Зокрема, положення про оголошення винагороди, конкурсу щодо продуктів ІТ; діяльність у сфері ІТ в інтересах іншої особи без її доручення; відшкодування шкоди, завданої у сфері ІТ; повернення безпідставно отриманого (збереженого) майна у сфері ІТ тощо;

6) норми цивільного законодавства, що стосуються спадкування у сфері ІТ. Зокрема, положення, що стосуються складання заповіту на продукти ІТ та його виконання; спадкування інтелектуальної власності на продукти ІТ, авторських прав на них тощо; поділ успадкованих прав на продукти ІТ між кількома спадкоємцями; переходу прав на продукти ІТ за спадковим договором тощо;

7) норми сімейного законодавства, що стосуються виникнення права спільної сумісної власності подружжя на продукти ІТ та права спільної часткової власності членів сім'ї на такі продукти; поділ спільної сумісної власності подружжя на продукти ІТ; встановлення права власності на продукти ІТ за шлюбним договором; захист прав неповнолітніх членів сім'ї у таких відносинах тощо.

Оскільки така структура може стосуватися не лише ІТ-права у вузькому сенсі, але й інших однотипних нормативних масивів (скажімо, підприємницького права, корпоративного права тощо.), доцільним є структурування «ІТ-права у спеціальному сенсі» у залежності від видів ІТ-відносин. При цьому до відповідного нормативного масиву мають бути віднесені вже лише ті норми, що стосуються суто сфери ІТ-відносин: інформаційних відносин; відносин створення та використання програмного забезпечення; Інтернет-відносин тощо.

Висновки

Формування інформаційно-комунікаційних технологій істотно вплинуло на розвиток суспільства, стало чинником інформаційної революції, зумовивши виникнення єдиного світового інформаційного простору. Відповідно, сформувалося середовище, яке отримало назву «інформаційне суспільство», як таке, що має безпосередній стосунок до інформації та інформаційних технологій. У вузькому значенні інформаційне суспільство – це: 1) суспільство, в якому виробництво, розподіл і споживання інформації є основною сферою діяльності; 2) суспільство нового типу, що формується внаслідок вибухового розвитку та конвергенції інформаційних та комунікаційних технологій, в якому головною умовою добробуту стає знання, здобуте завдяки безперешкодному доступу до інформації та вмінню працювати з нею; глобальне суспільство, в якому обмін інформацією не має меж; яке сприяє взаємопроникненню культур, водночас відкриваючи кожному співтовариству нові можливості для самоідентифікації; 3) вид постіндустріального суспільства, основою умовою формування якого є високотехнологічні глобальні інформаційні мережі, де інформація розглядається як товар, основна соціальна цінність. У інформаційному суспільстві виникає низка проблем, пов'язаних з поширенням у суспільстві інформаційно-комунікативних технологій, принаймні частина яких може бути вирішена правовими засобами шляхом впорядкування відносин, що складаються у цій сфері, та узгодженням інтересів їх суб'єктів. Цим і зумовлюється актуальність вивчення категорії «ІТ-право».

«ІТ-право» як концепт, іманентно властивий сучасній цивілізації, сучасному постіндустріальному (інформаційному) суспільству. При цьому слід визнати, що «ІТ-права», так само, як «Інтернет-права», «інформаційного права» тощо, як галузей права, не існує.

Натомість, з певними застереженнями, може йтися про «ІТ-законодавство», яке застосовується до відносин, що виникають при використанні інформаційно-комунікаційних технологій, хоча часом цей термін не має змістовного наповнення. Втім, слід зазначити, що й у цьому разі йдеться не про «ІТ-законодавство», як галузь, а лише про «віртуальну» сукупність норм, що регулюють різноманітні відносини тим чи іншим чином поєднані зі створенням та використанням

інформаційних технологій. Отже «ІТ-право» можемо розглядати як концепт (conceptus – думка, уявлення, поняття), тобто як сукупність уявлень, понять, знань, асоціацій, емоцій, що виникають у зв'язку з використанням терміну «ІТ-право», супроводжують і характеризують його.

Сфера «ІТ-права» охоплює норми цивільного, господарського, адміністративного, карного, митного, податкового права тощо, котрі складають його як мозаїка певне цілісне полотно. Особливо багато різноманітних ІТ-відносин виникає у сфері цивільно-правового регулювання. При цьому враховуємо наступні засади визначення правового масиву у ІТ-сфері:

1) до сфери «ІТ-права» доцільно відносити лише регулятивні відносини, і відповідно, норми законодавства, що їх регулюють;

2) при систематизації та структуруванні «ІТ-права» має бути розрізнення цього поняття у широкому та вузькому сенсі;

3) під «ІТ-правом» у широкому сенсі розуміємо сукупність усіх норм і правил, що регулюють діяльність по використанню інформаційних технологій та інформаційної правомірної активності в Інтернеті;

4) структура «ІТ-права» у широкому сенсі виглядає як відносно інтегрована система багаторівневого порядку, котра містить приватноправові та публічно-правові елементи, питома вага яких визначається пріоритетністю інтересів (приватні чи публічні). На цьому підґрунті визначаються особливості методів правого регулювання, що застосовуються у тих та інших випадках;

5) переважання публічних інтересів (забезпечення інформаційної безпеки тощо) означає, що відповідні відносини регулюються лише нормами актів законодавства і не можуть бути змінені або припинені за домовленістю;

6) ІТ-відносини, що належать до приватноправової сфери правового регулювання, переважно є регулятивними, але у деяких випадках можуть також супроводжуватися організаційними відносинами (створення юридичних осіб). Оскільки йдеться про сферу приватного права, де діє принцип «Дозволено все, що не заборонено законом», існування якого забезпечує надання договору значення норми цивільного законодавства, саме за його допомогою складається основний масив норм ІТ-права.

Таким чином, «ІТ-право» у вузькому сенсі може розглядатися як регулятивні норми (переважно цивільно-правові), що забезпечують функціонування ІТ-відносин;

7) можливе також виокремлення «ІТ-права у спеціальному сенсі». При цьому до відповідного нормативного масиву мають бути віднесені вже лише ті норми, що стосуються суто сфери ІТ-відносин: інформаційних відносин; створення та використання програмного забезпечення; інтернет-відносин тощо.

Ключові слова: ІТ-право, ІТ-відносини, інформаційне суспільство, інтерактивне громадянське суспільство, інформаційні технології, правове регулювання, концепт, соціальні мережі, приватне право, юридичне забезпечення.

Розділ 3

ГІБРИДНА ІНФОРМАЦІЙНА ВІЙНА ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

DOI

Євген Харитонов
доктор юридичних наук, професор,
член-кореспондент НАПрН України

Олена Харитонова
докторка юридичних наук, професорка,
членкиня-кореспондент НАПрН України

Попередні зауваження

Реаліями новітнього часу є поступове, але невпинне втягування усе більшої кількості країн світу у гібридні війни, котрі загрожують перетворитися у Світову війну. Ця небезпека ще дужче посилюється внаслідок «віртуалізації» суспільства, появою та зростанням потужності кіберзброї, зокрема, завдяки застосуванню у гібридній кібер війні технологій штучного інтелекту.

Розглядаючи цю проблему, передусім, маємо визначити поняття гібридної війни.

«Гібридна війна» у сучасному світі

Аналізуючи феномен гібридної війни у контексті російської агресії проти України, дослідники характеризують її, передовсім, «як новітній конфлікт і як форму глобального протистояння», і наголошують, що «поняття гібридної війни виявилося теоретично і практично найбільш придатним для визначення специфіки дій рф, яка, поєднуючи мілітарні, квазімілітарні, дипломатичні, інформаційні, економічні засоби, не гребуючи ядерним шантажем, послідовно намагається досягти в Україні та в інших точках світу

власних, не вповні зрозумілих міжнародній спільноті політичних цілей».[1]

Слід наголосити, що поняття гібридної війни охоплює не лише сучасні форми ведення бойових дій, види війн майбутнього або назви конкретних конфліктів змішаного типу, а є новим видом глобального протистояння у сучасному дестабілізованому міжнародному безпековому довкіллі.

Оскільки узагальнюючим терміном «гібридна війна» охоплюється низка різноманітних дій і поведінки, виникає необхідність структуризації відповідного концепту. Тим більше, що цей термін використовується, передусім, для позначення війни у традиційному розумінні, але війни, ускладненої, «обтяженої» додатковими елементами, компонентами, застосуванням нетрадиційних засобів, методів тощо. Наприклад, визначення гібридної війни, запропоноване у The Military Balance ще у 2015 році, охоплює (1) використання військових і невійськових засобів у комплексній кампанії, спрямованій на досягнення ефекту несподіванки, захопленні ініціативи та отриманні психологічних та фізичних переваг дипломатичними шляхами; (2) проведення складних та швидких інформаційних, електронних та технологічних операцій; (3) здійснення як прихованих, так і явних військових та розвідувальних дій; (4) здійснення економічного тиску.[2] Це визначення і пізніше визнавалося деякими авторами найбільш вдалим.[3]

Таким чином, хоча на чільне місце виступає «мілітарна війна», термін «війна» у широкому сенсі застосовується також у сферах, які не передбачають будь-якого використання військової зброї, наприклад, «інформаційна, економічна, політична війна». У кожному випадку можна говорити про певні характерні методи дій у названих

---

[1] Яворська Г. М, Їжак О. І. Феномен гібридної війни. *Світова гібридна війна: український фронт:* монографія. За заг. ред. В. П. Горбуліна. Харків: Фоліо, 2017. С.15.

[2] The Military Balance 2015: website. URL: https://archive.org/details/militarybalance-20000unse_d0k7

[3] Гуменюк В. Гібридна війна Росії проти України як загроза універсальній колективній безпеці. *Деокупація. Юридичний фронт*: матеріали Міжнародного експертного круглого столу (Київ, 18 березня 2022 р.). Державний торговельно-економічний університет, Українська асоціація порівняльного правознавства, Українська асоціація міжнародного права, Асоціація реінтеграції Криму; упоряд. і наук. ред. О. В. Кресін. Київ: Держ. торг.-екон. ун-т, 2022. С.23-25.

сферах, однак у традиційному сенсі вони, на думку деяких авторів, є тільки компонентами «мілітарної» війни.[1]

На наш погляд, головна вада такого підходу полягає в тому, що заперечуючи доцільність визнання окремих видів війни і прив'язуючи їх до ідеї (вимоги) «функціонального перетворення на зброю традиційно невійськових засобів силового впливу та об'єднання їх на цій підставі з власне військовими методами», ми втрачаємо можливість їхнього самостійного аналізу у випадках, коли агресор уникає «визнання стану війни» (і навіть «збройного конфлікту»), не використовує «власне військові методи» тощо, а досягає мети у інший спосіб (політичний, економічний, юридичний, ментальний-релігійний, дипломатичний, культурний та ін. тиск).

Власне, саме так росія і чинила протягом 1991-2013 років. Більш того, навіть після 2014 року їй удавалося, уникаючи оголошення війни, досягати своїх цілей за допомогою невійськових засобів силового впливу без об'єднання їх з власне військовими методами.

Враховуючи зазначене, з високим степенем вірогідності можна припустити, що наразі гібридні війни, скоріш за все, матимуть вигляд нерегулярної війни, де її учасники робитимуть спроби та намагатимуться підірвати легітимність та авторитет керуючого режиму. Це вимагатиме від збройних сил держави допомоги, щоб закріпити здатність держави забезпечувати соціальні, економічні та політичні потреби свого народу.[2]

Важливо відзначити, що гібридний контекст тут є продуктом глобалізації, що розмиває кордони традиційних норм та правил.

Аналізуючи твори зарубіжних авторів, В. В. Власюк і Я. В. Карман, зауважують, що у такій війні використовують три види зброї:

1) модельно – організаційна – зброя, що ґрунтується на особових базах даних політиків, державних службовців, бізнесменів…. Ці бази збирають за допомогою різних міжнародних організацій, благодійних фондів, радників, політологів та інших підготовлених служб. У цих базах даних міститься інформація про рахунки з-за кордону, а також компрометуюча інформація. Основні бази даних використову-

[1] Яворська Г. М, Їжак О. І. Феномен гібридної війни. С. 26, 28.

[2] Major Shane R. Reeves, Major Robert E. Barnsby The New Griffin of War. Hybrid International Armed Conflicts. *Academic joutnal article "Harvard International Review"* 2013. URL: https://www.questia.com/library/journal/1G1-316203914/the-new-griffin-of-war-hybrid-international-arme

ються для залякування і розкладання політичної та державної еліти для формування кола підтримки та запобіганню супротиву;

2) інформаційна зброя, яку поділяють на концептуально-методологічну (формування глобальної політики з метою створення конкретного спланованого виміру розвитку історичних подій); хронологічну (інформація хронологічного плану, послідовність фактів та явищ, що дає можливість аналізувати явища історичного процесу та прогнозувати вектори майбутньої політики); факторологічну зброю (ідеологія, релігія, технології);

3) матеріальна зброя, яку поділяють на: економічну зброю (засоби економічної боротьби, спрямовані на дезорганізацію структур противника та їх поглинання – контроль фінансово-кредитної системи країни, інших економічних систем держави, боргових зобов'язань, розподілу коштів, повернення фінансів в державу, прибутковості державного сектору в економіці тощо); зброю геноциду (етнічний геноцид, наркотичний, алкогольний, інформаційно-економічний тощо); звичайну зброю фізичного знищення.[1]

У підсумку Власюк В. В., Карман Я. В. визначають поняття «гібридна війна» як сучасний вид війни, де в конфлікті використовуються різноманітні засоби нападу та оборони держав, що виходять за рамки конвенційно-визначених варіантів та видів ведення війни. При цьому зброєю вже є не тільки матеріальні традиційні її види, а й модельно-організаційна та інформаційна види зброї. [2]

Деякі автори «виділяють принаймні сім основних видів війн, що ведуться (можуть вестись) у XXI ст. Такі війни істотно різняться між собою за багатьма ознаками, у тому числі за критерієм ефективності. До загального переліку війн пропонується віднести:

1) класичну техногенно-силову війну;

2) економічну війну;

3) неоголошений геноцид проти населення держави суперника;

4) організаційну війну (імплантацію в національно державне тіло супротивної сторони чужорідних або відкрито ворожих організацій-

[1] Власюк В. В., Карман Я. В. Деякі основи поняття «гібридна війна» в міжнародному праві. URL.: АПП – науково-практичний журнал (knu.ua)

[2] Власюк В. В., Карман Я. В. Деякі основи поняття «гібридна війна» в міжнародному праві. URL.: АПП – науково-практичний журнал (knu.ua) Право і громадянське суспільство – ДЕЯКІ ОСНОВИ ПОНЯТТЯ "ГІБРИДНА ВІЙНА" В МІЖНАРОДНОМУ ПРАВІ – Власюк В. В., Карман Я. В. (knu.ua)

них форм – від невластивих органів влади до найрізноманітніших фондів);

5) інформаційну війну;

6) хронологічну війну (довільну, проте вигідну для замовника інтерпретацію історичного минулого «незручної» країни, постійну маніпуляцію історичними фактами на власну користь);

7) духовну війну як цілеспрямоване нав'язування згубних цінностей тим народам або державам, яких потрібно підкорити».[1]

Відтак усталений наразі підхід до визначення співвідношення концептів «війна» та «гібридна віна», потребує перегляду із врахуванням наступних методологічних засад дослідження.

Як на нашу думку, враховуючи викладене, передусім, доцільно розмежувати категорії «гібридна мілітарна війна» і «гібридна війна – загальне явище».

У першому випадку йдеться про «гібридність» війни як збройного конфлікту – конструкту, що виник на традиційному підґрунті, а тепер зазнає трансформацій внаслідок використання нових методів, форм і засобів воєнних дій.

У другому випадку – маємо на увазі «гібридність» війни у широкому сенсі – як соціального конфлікту, протистояння держав, спільнот, суспільств, цивілізацій. Війна у такому сенсі охоплює також «мілітарну війну» (збройний конфлікт), але може відбуватися взагалі без застосування традиційної зброї, але із застосуванням інших засобів впливу (примусу) підпорядкування однієї сторони конфлікту іншій його стороні.

Критерієм їхнього розмежування є: мета, мотивація (очікування), середовище, засоби (методи), результат. З них найбільш важливими для прагматичних класифікацій, на нашу думку, є середовище (сфера), де йде протиборство, і засоби (інструменти, методи) протиборства (війни).

Із врахуванням цих критеріїв можуть бути виокремлені такі види гібридної війни (які можуть перетинатися і взаємно проникати. Перелік орієнтовний):

1. Мілітарна (аби уникнути слова «війна», його часто заміняють евфемізмами на кшталт «визвольний похід», «братська допо-

[1] Валіулліна З. В. Військова теорія К. Клаузевіца в теоретичному дискурсі. *Ефективна економіка.* 2017. № 11. URL: http://www.economy.nayka.com.ua/?op=1&z=5881

мога», «інтернаціональний обов'язок», «уведення обмеженого контингенту», «СВО» тощо. Ми користуємось позначенням «мілітарна аби уникнути коструватого виразу «воєнна війна»)

2. Інформаційна
3. Економічна
4. Юридична
5. Ідеологічна
6. Культурна
7. Психологічна
8. Історична
9. Дипломатична
10. Технологічна
11. Кібернетична

Характеризуючи далі гібридну війну, будемо спиратися на твердження К. фон Клаузевіца, яке зроблене ним у праці, присвяченій «війні-збройному конфлікту», але також є таким, що стосується, на нашу думку, феномену війни взагалі: це, передусім, «акт насильства, який має на меті змусити противника виконати нашу волю».[1] Додамо до цього, насильство може бути у різних формах. Але по суті, це насильство завжди психологічне, оскільки має метою зламати психіку іншої особи – об'єкту насильства – підкорити її власній волі.

Для позначення брутального впливу на духовну, емоційну, психічну тощо сферу людини використовуються терміни інформаційна, консцієнтальна, ментальна, цивілізаційна, ціннісна війна (перелік не вичерпний, і можливо, в результаті вивчення цього питання буде розширений).

Почнемо з концепту «інформаційна війна». Тут психічний вплив зазвичай здійснюється через інформацію, і вплив на духовну сферу може бути результатом суто духовного насильства. Однак психічне насильство може бути й не пов'язаним з використанням прийомів інформаційної війни, а натомість виступати як результат фізичних дій агресора. Таким випадком, на нашу думку, є геноцид, за допомогою якого досягається мета загарбника не лише привласнити чужі території, але й закріпити успіх, убезпечивши себе шляхом деформації свідомості підкорених народів від деокупації.

[1] Карл фон Клаузевіц. Природа війни. пер. Руслан Герасимов. Харків: Vivat, 2018. С. 8-11.

Отже поняття інформаційної війни і війни психічної різні за обсягом і заходами, що застосовуються.

Зауважимо також деяку некоректність вживання терміну «психічна війна», оскільки у цьому разі є перехід на інший рівень таксономії.

Подивимось, чи можна виправити цю хибу, скориставшись концептом «консцієнтальна війна», який набув популярності протягом останніх років. Зокрема, «консцієнтальною» деякі автори вважають російсько-українську війну, вказуючи, що вона «є не боротьбою різних інтересів, а передусім змаганням цінностей, що є характерним для війн міжцивілізаційних, війн, котрі вкладаються в концепцію консцієнтальної війни, війни духовної та смислової». На думку А. Шумки, така війна «спрямована на віртуальний простір та впливає на пізнавальну сферу людини. Об'єкти впливу тут є світоглядні переконання населення та цінності, сформовані у суспільствах. Мета – від тактичної цілі – зміни ставлення людей до процесів та подій до стратегічної цілі – зміни їх самоідентифікації». Походження терміну «консцієнтальність» тут виводиться від латинського constientia – «свідомість» або «совість», тлумачачи вираз «консцієнтальна війна» як «війна на ураження свідомості», і зазначаючи, що з кінця 90-х роки Москва розпочала неоголошену війну за свідомість українців., бомбардуючи їх наративами, а Україна не одразу усвідомила, що наративи формують не тільки розуміння минулого, але і програмують майбутнє. Та наративна війна, та невід'ємна частина великої стратегічної консцієнтальної війни завдала Україні найбільшої шкоди, призвела до то, що українці виявились не готовими до початку гібридної агресії Росії у 2014 році.[1]

Але, попри те, що концепція «консцієнтальної війни» приваблює спробою акцентувати увагу дослідників на значенні «світоглядних переконань населення» та «цінностей, сформованих у суспільстві», як об'єктів агресії (вони ж, очевидно, є змістом «свідомості», на ураження якої спрямована війна), ми не отримуємо відповіді на питання, чим за такого бачення «бомбардування свідомості наративами» відрізняється від інформаційної війни, яка ведеться тими самими наративами і має таку саму мету «ураження свідомості»?

[1] Шумка А. В. Російська агресія в Україні 2022 року як консцієнтальна війна. URL: https://www.polukr.net/uk/blog/2022/12/rosijska-agresija-v-ukraini-jak-konceptualna-vijna/

У кожному разі, помітної різниці, яка б давала підстави вести мову про «консцієнтальну війну», як вид, полігібридної війни, тут не вбачається.

Мабуть, тому деякі автори, використовуючи обидві згадані категорії, слушно вважаючи, що за будь-яких обставин між державами буде іти війна за вплив на людську свідомість, відносять інформаційну та консцієнтальну війни до складників гібридної війни,[1] які безпосередньо визначають роль людини у ній. [2]

У пошуках подолання вад згадуваних вище «психічних»/ «психологічних» концепцій гібридної війни політики і науковці загалом достатньо очікувано вийшли на позначення «ментальна війна», котрий нині вважається виразом, який став узагальнюючим, увібравши в себе попередні позначення («когнітивна війна», «консцієнтальна війна», «семантична війна», «дискурсивна війна» та ін., поширені у XXI ст.), котрі, хоча і не абсолютно взаємозамінні, але з різних боків описують одне й те саме явище – ураження нематеріальних складових мілітарної потуги: людської волі, духу, свідомості тощо.[3]

Позначення «ментальна війна» (іноді під назвою «мережева війна») активно використовується російськими військовиками і політиками, для яких воно є частиною «теоретичної» бази переінакшення світового порядку за російськими уявленнями та уподобаними засобами. Враховуючи це, маємо викласти суть їхніх поглядів.

Базові положення сучасного російського варіанту бачення «ментальної війни» викладені у статті Андрія Ільницького (народився у Львові) «Стратегія ментальної безпеки Росії», опублікованій у 2022 році.[4]

---

[1] Ващенко Н. М. Теоретичний вимір дослідження поняття «консцієнтальна війна» в умовах гібридної агресії Росії проти України. *Новітні тенденції в медіагалузі:* ІІ Всеукр. наук.-практ. конф. (м. Київ, 07 квітня 2020 року). Київ, 2020. С. 1–8. URL: Теоретичний вимір дослідження поняття «консцієнтальна війна» в умовах гібридної агресії Росії проти України – Наукова сторінка (univ.kiev.ua); Горбенко Ю. Л. Особистість у гібридній війні: психологічний вимір. *Психологія і особистість.* 2017. № 2 (12). С. 30–39; Сенченко М. І. Латентна світова інформаційна війна. Київ: ФОП Стебеляк, 2014. С. 14-15.

[2] Тараненко М. М., Ярош І. С. Роль людини в гібридній війні: українська революція 1917–1921 рр. та сучасність. *Юридичний науковий електронний журнал.* 2021. № 2. С. 36-39. URL: 8.pdf (lsej.org.ua)

[3] Сергій Громенко. «Ментальна війна» як складова агресії Росії проти України. 23 травня, 2022, glavcom.ua. URL: https://glavcom.ua/columns/sgromenko/mentalna-viyna-yak-skladova-agresiji-rosiji-proti-ukrajini-847665.html

[4] Ільницький А. Стратегія ментальної безпеки Росії (рос.мовою). *Военная мысль.* 2022. № 4. С. 24-35.

Спочатку трохи про особу автора, оскільки це, на нашу думку, дає можливість точніше оцінити суть його концепції.

Передусім, зауважимо метаморфози ставлення Ільніцького до США, котрим у його розмірковуваннях щодо системи загроз врешті відводиться роль головного зла. Але це було пізніше. А двадцять років тому Андрій Ільницький обожнював Америку. Свої враження від поїздки до США він описував наступним чином: «Вражаюча країна. Країна з колосальною енергетикою. Країна …створена людьми, які вірять в Бога, але передусім в себе».

Тоді Ільницький був топ-менеджером великого книжкового видавництва «Вагріус». Зараз він – головний політконсультант Сергія Шойгу, колишнього міністра оборони, а тепер секретаря Ради безпеки.

Про США Ільницький наразі відгукується зовсім інакше: Нині «вражаюча країна» обернулася на «слабнучу державу», яка «перебуває у глибокій экзистенційній кризі», але намагається знищити Росію за допомогою «технології Антихрист».[1]

Далі про «концепцію Ільницького». Точніше про інтерпретацію ним «Стратегії національної безпеки» США щодо «мереживних війн» з відповідною зміною знаків «плюс» на «мінус» і навпаки та розставлянням відповідних російських ідеологічних наголосів. Відправною тезою його статті 2022 року є твердження, що джерелом загроз є США та їхні союзники. Зумовлено це тим, що США слабшають, їхні еліти деградують, а єдиним способом подолати цю екзистенційну кризу для них є війна проти головного суперника – росії, яку вони бажають перемогти без «демографічних втрат». Вороги прагнуть поступово вивести/витравити росіян (в онтологічному розумінні) як народ, як цивілізацію зі своїм культурно-історичним кодом, усунути російську державу як перешкоду на шляху встановлення потрібного їм світового порядку.

Головні риси такої війни вбачаються у наступному: 1) агресія ведеться в «сірій зоні»; 2) війна ведеться «за світогляд окремих громадян та суспільства в цілому»; 3) поразка полягає не в окупації тери-

[1] Політтехнолог Андрій Ільницький дуже хотів змінити владу зсередини – і закликав до демократизації. Але потім «пристосувався» до системи, став радником Шойгу і заговорив про «ментальні війни» із Заходом. 1 липня 2024 року. Meduza. URL: https://meduza.io/feature/2024/07/01/polittehnolog-andrey-ilnitskiy-ochen-hotel-pomenyat-vlast-iznutri-i-prizyval-k-demokratizatsii-no-potom-prisposobilsya-k-sisteme-stal-sovetnikom-shoygu-i-zagovoril-o-mentalnyh-voynah-s-zapadom

торії, а у втраті політичної волі; 4) бліцкриг здійснюється через вплив на еліти та медіа; 5) атака на країну ведеться не лише ззовні, але й зсередини; 6) «абсолютною перемогою вважається окупація духовного простору та суспільної свідомості, коли переможений втрачає здатність відстоювати свої цінності, повністю асимілює чужі та фальшиві установки, які йому нав'язав противник-переможець».

На такому підґрунті ментальна війна визначається як «скоординована сукупність різного масштабу дій та операцій, спрямованих на «окупацію» свідомості супротивника з метою паралічу його волі, зміни індивідуальної та масової свідомості населення для деморалізації армії та суспільства, знищення духовно-моральних цінностей, традицій та культурно-історичних засад держави, «стирання» національної ідентичності народу» (с. 27-28).

У відповідь пропонується запровадження Стратегії ментальної безпеки з наступних складових: 1) консолідація держави і суспільства на базі ідеології; 2) створення центрів моніторингу, аналізу і прогнозування та розробка методів протидій ментальним загрозам; 3) посилення захисту інформаційної інфраструктури і розвиток кіберсил; 4) захист цінностей народів Росії, «запобігання фальсифікації історії, припинення атак на ментальну сферу росіян, духовну та культурну спадщину, сакральні та символічний області, історію та російську мову (с. 32).[1]

Потім ця концепція була розвинута і удосконалена з врахуванням необхідності посилення ідеологічних елементів. Зокрема, у наступних публікаціях на цю тему більш акцентується увага на злі «глобалізації», необхідності захищати «власні цивілізаційні цінності».

Зокрема, член Президії Ради із зовнішньої і оборонної політиці О. Лосєв переконаний, що «деградація» є стратегією Заходу у ментальній війні:

«Досягнення будь-якою державою геополітичних і економічних переваг дає їй можливість побудувати світовий порядок відповідно до своїх інтересів, нав'язати свою волю, а разом з нею і систему розподілу багатства і влади між усіма іншими країнами і народами. Після розпаду Радянського Союзу ці процеси підтримувалися гегемо-

[1] Громенко С. «Ментальна війна» як складова агресії Росії проти України. 23 травня, 2022, glavcom.ua. URL: https://glavcom.ua/columns/sgromenko/mentalna-viyna-yak-skladova-agresiji-rosiji-proti-ukrajini-847665.html

нією долара і домінуванням американських транснаціональних корпорацій … Західна політика просувалася також через встановлення контролю над вищою та шкільною освітою, через культурну «революцію» та створення нових культів…

…Тепер, коли... Росія відроджується, Європа слабшає, піднімається Глобальний Південь, а вплив Китаю розширюється по всьому світу, США, з метою збереження гегемонії, продовжуватимуть посилювати не лише економічний тиск на супротивників, а й переходитимуть безпосередньо до військових конфліктів, гібридних та ментальних війн, де сферами протистояння є інформаційне середовище та кіберпростір, простір сприйняття та символічні зони, історія та моральний дух націй. …

Ядерна зброя та стратегічний паритет унеможливлюють повномасштабний конфлікт між Заходом та Росією, а це означає, що, окрім ставки на київський режим та націоналістичні еліти колишніх радянських республік, посилюватиметься як економічна, так і ментальна війна. Війна на знищення Росії – це не лише розчленування території та захоплення контролю над економікою, це також війна, спрямована на зміну мислення, на розпад суспільства, на руйнування нашої багатонаціональної спільноти, зміну етичної системи тощо, ця війна почалася дуже і дуже давно.

Ментальна війна проти Росії почалася після нашої перемоги в наполеонівських війнах і не припинялася протягом двох століть, вона велася і під час Кримської війни, і під час Великої Вітчизняної війни, і під час холодної війни. Вона інтенсивно тривала і після розпаду Радянського Союзу на всій його території. Ми бачимо, як під керівництвом Заходу жахливо переформатували нашу сусідню країну і колишню братню Україну, щоб створити з неї антиРосію, і там жили наші співвітчизники – люди з радянським вихованням і з таким же розумінням, що є добро, а що таке зло, як і наше.

Інформаційний простір, культура і система загальнолюдських норм і соціальних цінностей є театром військових дій ментальної війни. І головна стратегія цієї війни – деградація культури і мистецтва, науки і освіти і суспільства в цілому. Почалося СВО, і ми побачили, як Захід перейшов до тотальної війни проти Росії, а антиросійські «комбатанти» ментальної війни Заходу втекли з нашої країни до ЄС, США, Ізраїлю, Туреччини та Еміратів».

«Треба говорити про наших героїв … адже герої, люди, які здійснюють подвиги і виконують бойову роботу зараз на фронті, це ті, хто буде прикладом для майбутніх поколінь. Потрібно пояснити суспільству, хто наші вороги і які їхні цілі. У жодному разіразі не повинно бути сліпої віри в те, що Захід – кращий світ, а ми – периферія. Ми ті, хто зберігає людську цивілізацію»,[1] – пафосно завершує автор свої екзерциції.

Для тих, хто не осягнув краси останніх, головні положення російської «концепції ментальної війни» буквально за два тижні в тій самій «Парламентській газеті» були викладені більш детально обома її «провідниками» – А. Ільніцьким та О. Лсєвим.

При цьому залишається незмінною голівна ідея. На тлі констатації того, що глобальні еліти зробили свою справу і США як держава входить в період занепаду, а Захід переживає екзистенційну кризу внаслідок деградації ліберальної мрії, висловлюється твердження, що Росія отримує шанс повернути собі статус особливої цивілізації. Відтак оголошується, що «головним завданням є формування власної російської ідеології та стратегії з протидії тотальній деградації світу, спричиненій західними глобалістами».

Характерна деталь: автори статті висловлюють впевненість, що «головною рушійною силою розвитку науки буде військово-промисловий комплекс…. Мобілізація нашої економіки для потреб перемоги на полях СВО, де відбувається битва цивілізаційної війни між Росією та Заходом, сприяє вирішенню цих проблем, ламаючи тенденцію до деградації, індуковану глобалістами».

Вони наголошують важливість розуміння того, що росія має перемогти Захід насамперед ментально. Для цього потрібна потужна ідеологія, шо збирає волю народу, яка є не «продуктом розуму» політологів, не конструктом, принесеним ззовні, а «прожитою історією, накопиченою мудрістю і усвідомленим сенсом існування народу».

Російська ідеологія, вважають вони, «має пронизувати все – від правлячих еліт до глибин суспільства, спонукаючи всіх діяти солідарно. Військові та силовики, депутати та чиновники, керівники державних корпорацій, дипломати, медійні та освітньо-культурні діячі

[1] Лосев А. Деградация как стратегия Запада в ментальной войне. Парламентская газета. URL: https://www.pnp.ru/person/aleksandr--losev/. 08.08.2023. URL: https://www.pnp.ru/politics/degradaciya-kak-strategiya-zapada-v-mentalnoy-voyne.html

мають внутрішньо мобілізуватися та чітко визначити своє місце на фронті цивілізаційної війни із Заходом».[1]

Загалом викладений матеріал – радше сукупність ідеологізованого наративу, ідеологічних закликів та гасел, ніж «концепція». Але це є досить типовим для сучасного російського політикуму: відсутність чіткого поняття, аналізу ознак явища, його структуралізації тощо.

У цьому сенсі більш аналітичними виглядають погляди Андрія Фурсова, який вважає, що ментальна війна має три рівні: 1) «війна фактів» – їхнє заперечення, викривлення, віддзеркалення чи знецінення; 2) «війна концепцій» – боротьба за інтерпретацію фактів; 3) «війна сенсів» – за право давати феноменам оцінки (Що важливіше – право України обирати рух до НАТО чи право Росії протистояти глобалізації?)». – «Для більшості жителів планети відповіді на всі три питання не є аж так очевидними, – слушно зазначає, коментуючи ці положення, Сергій Громенко.[2]

При ознайомлені зі згаданими та іншими текстами російських авторів на цю тему привертає увагу властива практично усім їм спільна риса. Попри те, що ці та інші публікації такого штибу густо наповнені емоційними інвективами та закликами, вони, водночас, не містять визначення понять, якими їх автори оперують, зокрема, таких принципово важливих у цій сфері як «ментальність» і «цінності».

На нашу думку, для сучасних російських «концепцій» історичного розвитку, «теоретиків» міжцивілізаційних конфліктів термінологічна недбалість, так само як і відсутність методології дослідження, є природною, попри усі їхні претензії на «глобальні відкриття». До того спонукають традиція – сотні літ викривлення перебігу історичного процесу, упереджене тлумачення соціальних подій, а також запозичення і цілеспрямоване зловмисне перекручення концепцій суспільного розвитку, запропонованих зарубіжними науковцями тощо.

Усі ці засоби активно використовуються у гібридній інформаційній війні з широким застосуванням інформаційних технологій та

---

[1] https://www.pnp.ru/politics/inducirovannaya-degradaciya-mira.html

[2] «Ментальна війна» як складова гібридної. До чого готується Росія і до чого слід готуватися Україні? 20.05.2022 від UIFuture. URL: https://uifuture.org/publications/mentalna-vijna-yak-skladova-gibrydnoyi-do-chogo-gotuyetsya-rosiya-i-do-chogo-slid-gotuvatysya-ukrayini/. Громенко С. «Ментальна війна» як складова агресії Росії проти України. 23 травня, 2022, glavcom.ua. URL: https://glavcom.ua/columns/sgromenko/mentalna-viyna-yak-skladova-agresiji-rosiji-proti-ukrajini-847665.html

можливостей останніх при підготовці та подачі симулякрів, фейків, діпфейків у соціальних мережах на телебаченні, електронних медіа тощо.

Спираючись на таке загальне розуміння сутності війни, розглянемо далі особливості сучасного бачення цього концепту та гібридної війни, попередньо зауваживши, що в нашій країні дослідження цієї категорії були особливо популярними у перші роки після початку російської збройної агресії в Україні,[1] зі зниженням інтересу протягом часу АТО і ООС.[2]

Наразі завдання врахування позицій фахівців у цій галузі полегшується появою низки праць оглядового характеру. Зокрема, такою працею є розвідка Ж. Павленко та А. Антонова 2023 року «Гібридна війна»: аналіз визначень поняття».[3] Її автори слушно зазначають, що наукові доробки щодо проблематики здійснюються здебільшого в

[1] Даник Ю., Малярчук Т., Бриггс Ч. Гибридная Война: Хай-Тек, Информационные и Кибер Конфликты. Connections: QI. 2017. № 16. С. 5–27. URL: http://connections-qj.org/ru/article/gibridnaya-voyna-hay-tek-informacionnye-i-kiberkonflikty; Магда Є. Гібридна війна: вижити і перемогти. Харків: Віват, 2015. 304 с.; Магда Є. Гібридна війна: сутність та структура феномену. International relations, part «Political sciences». 2014. № 4. URL: http://journals.iir.kiev.ua/index.php/pol_n/ article/view/2489/2220; Почепцов Г. Гібридна війна: інформаційна складова. Media Sapiens. 2015. URL: http://osvita.mediasapiens.ua/trends/1411978127/gibridna_viyna_informatsiyna skladova/; https://www.nato.int/docu/review/ru/articles/2015/05/07/gibridnaya-vojnasushchestvuet-li-ona-voobshche/index.html; Світова гібридна війна: український фронт: моногр. За заг. ред. В. П. Горбуліна. Харків: Фоліо, 2017. 496 с.; Тараненко М. Гібридна війна в Україні: історія та сучасність. *Вісник НТУУ «КПІ»*. Політологія. Соціологія. Право. 2016. Вип. 3/4 (31/32). С. 190-200. URL: https:// ela.kpi.ua/bitstream/123456789/25058/1/VPSP2016-3-4_190–200.pdf; Яворська Г. Гібридна війна як дискурсивний конструкт. *Strategic priorities*. 2016. № 4 (41). С. 41–48. URL: http://ippi.org.ua/sites/default/files/yavorskaya.pdf

[2] Воєнні аспекти протидії «гібридній» агресії: досвід України: моногр. За заг. ред. А. М. Сиротенка. Київ: НУОУ ім. Івана Черняховського, 2020. 176 с.; Соколов Б. Гібридна війна в дії. День. 11 листопада 2021. URL: https://day.kyiv.ua/ uk/article/den-planety/gibrydna-viyna-v-diyi; Bratko A., Zaharchuk D., Zolka V. Hybrid warfare – a threat to the national security of the state. Revista de Estudios en Seguridad Internacional. 2021. Vol. 7, № 1. P. 147–160. URL: http://www.seguridadinternacional.es/revista/; Osiichuk M., Shepotylo O. Conflict and well-being of civilians: The case of the Russian-Ukrainian hybrid war. *Economic Systems*. 2020. Vol. 44(1). С. 1–31. URL: https://www.sciencedirect.com/science/article/pii/S0939362518303960; Tkachuk I., Shynkarenko R., Tokovenko O., Svorak S, Lavoryk A. Hybrid threats and the transformation of the state political institute: a neo-institutional approach. Journal of interdisciplinary research. *Special Issue*. 2021. № 11/01-XVI. URL: http://www.magnanimitas.cz/ADALTA/110116/papers/A_05.pdf

[3] Павленко Ж., Антонов А. «Гібридна війна»: аналіз визначень поняття. *Вісник Національного юридичного університету імені Ярослава Мудрого*. 2022. № 2 (53). С. 106-119.

межах воєнних та політичних наук, хоча ці дослідження вимагають у першу чергу глибокого й ретельного філософського, зокрема логіко-методологічного, осмислення з метою конструювання поняття «гібридна війна».

Погоджуючись з цією тезою, разом із тим зауважимо, що автори послуговуються популярними, але хибними, як на наш погляд, уявленнями про співвідношення роду та виду при характеристиці цих понять, коли пишуть: «Неможливо зрозуміти поняття «гібридна війна» без його родового поняття – «війна». При цьому остання розглядається ними як феномен «суттєвими ознаками якого вважається організована збройна боротьба між державами, суспільними класами тощо; конфлікт, що здійснюється силою зброї, як між країнами, так і між сторонами всередині країни; період збройної ворожнечі або активних військових операцій, що здійснюються наземним, морським або повітряним шляхом». До того ж вони трактують війну як насамперед фізичний, матеріальний феномен.[1]

Насправді, «гібридна війна» тут є родовим поняттям щодо поняття «війна – збройний конфлікт». Як зазначає Є. Магда, «війна – це не лише безпосередньо бойові дії, але і конкуренція економік, способів життя і мислення правителів, змагання систем державного управління, сутичка потенціалів і протистояння ідеологій».[2] Головною ознакою такої війни є її «гібридність: вона є одночасно війною інформаційною, економічною, репутаційною, смисловою. На неї повинні працювати всі, хто має вплив на населення: актори, співаки, письменники, режисери. Військові дії задають лише фон для більш масштабної війни в людському розумі».[3]

РВНП (російська війна нового покоління) – запозичена версія концепції гібридної війни.

Існує думка, що концепція гібридної війни належить російському генералу Герасимову.[4]

---

[1] Павленко Ж., Антонов А. «Гібридна війна»: аналіз визначень поняття. С. 110.

[2] Магда Є. В. Гібридна війна: вижити і перемогти, Х.: Віват, 2015. С. 12.

[3] Гібридна війна: інформаційна складова. Георгій Почепцов. 25 жовтня 2015. URL: //https://ms.detector.media/mediaanalitika/post/14501/2015-10-25-gibrydna-viyna-informatsiyna-skladova/

[4] Хорунжий Г. Війна Росії проти України російська пропаганда як складова «гібридної війни». URL: ВІЙНА РОСІЇ ПРОТИ УКРАЇНИ РОСІЙСЬКА ПРОПАГАНДА ЯК СКЛАДОВА «ГІБРИДНОЇ ВІЙНИ»-> Стаття -> Український науковий журнал «ОСВІТА РЕГІОНУ» (uu.edu.ua);

Але це не так, хоча слід визнати, що саме в Україні росія звела гібридну війну в абсолют.[1] Насправді пріоритети у сфері створення сучасної концепції гібридної війни належать США. Натомість російський доробок, фактично полягає у модернізації В. Герасимовим давньої російської теорії нетрадиційних воєн (а фактично – «війн без правил»). Засновник цієї теорії Іссерсон у книзі «Нові форми боротьби», ще у 1940 році, писав: «*Війна взагалі не оголошується. Вона просто починається наперед розгорнутими збройними силами*». Важливу роль відіграли також положення творів Месснера (воєнний теоретик з білої еміграції, якого аналітики називають улюбленим стратегом путіна) стосовно війн майбутнього: «*У минулих війнах важливим вважалося захоплення території. Надалі найважливішим буде розглядатися захоплення душ у державі, з якою ворогують*». Вважаючи, що традиційні методи ведення війни вже вичерпані, він обґрунтовував низку важливих висновків: «*Колись війни йшли у двомірному просторі – на поверхні моря й суходолу. Потім з'явився третій вимір – війна в повітрі. Тепер найважливішим став четвертий вимір – психіка сторін, що воюють*». Американці програли війну у В'єтнамі саме в головах. *«Політика є мистецтвом об'єднання людей. Найважливішим завданням у бунтовійні є об'єднання власного народу і залучення на свій бік частини народу держави, з якою ведеться війна*», – зазначав він.[2]

Посилаючись на те, що нині змінилися «правила війни», оскільки невійськовий інструментарій починає бути ефективнішим за військовий, Герасимов обґрунтовував тезу про те, що наразі набувають ваги політичні, економічні, інформаційні, гуманітарні методи, що активізують протестний потенціал населення. До них додаються приховані військові засоби. (Принагідно зауважимо, що «Росія ніколи не використовувала в своїх стратегічних документах і доктринах термін «гібридний». Більше того, у росії просувалася думка, що не вона, а проти неї Захід веде гібридну війну, і це саме західна концепція. У викладі на початку 2013 року В. Герасимовим російського бачення гібридності йшлося не про дії росії, а містилася конспірологічна російська версія «арабської весни» і ставилось завдання знайти методи

[1] Магда Є. В. Гібридна війна: вижити і перемогти», Х.: Віват, 2015. С. 3.

[2] Гібридна війна: інформаційна складова. Георгій Почепцов. 25 жовтня 2015. URL: https://ms.detector.media/mediaanalitika/post/14501/2015-10-25-gibrydna-viyna-informatsiyna-skladova/

протидії. Відтак росія розробляла власні методи гібридної війни, які незабаром були застосовані проти України».[1]

Як зазначив Герберт Макмастер: «Щоб захиститися від внутрішньої опозиції та повернути Росії велич, Путін воскресив націоналістичну місію країни, він зображує свій народ як безстрашний і розробляє зовнішню політику, яка має залякати сусідів і похитнути західні демократії».[2]

Путінські амбіції штовхали його і очолювану ним країну до війни за «втрачену велич», заради якої варто було битися з численними супротивниками – за його оцінками, з усім вільним світом. Водночас битва «за велич» для росії була пов'язана з проблемою виживання, оскільки вона, як зауважує Г. Макмастер, «була недостатньо сильна, щоб безпосередньо змагатися зі США та їхніми союзниками в Європі й Азії, поступаючись їм за усіма основними економічними показниками. Вразливими місцями росії були також корупція (за «Індексом сприйняття корупції» – 135 місце в світі), несприятливі демографічні тенденції. Але відповідно до своїх кадебістських звичок Путін і Патрушев цікавляться не розбудовою Росії, а підривом інших держав. …він розробляє складні стратегії, спрямовані на досягнення цілей, розташованих майже на межі, переступання якої здатне викликати узгоджену відповідь або держави-мішені, або, скажімо, її союзників по НАТО».[3]

На таких ідейних засадах ґрунтуються положення статті В. Герасимова 2013 року з її акцентами: «змінилися самі «правила війни», «зросла роль невоєнних способів досягнення політичних і стратегічних цілей, які в окремих випадках значно перевищують силу зброї за своєю ефективністю».

Аби не спрощувати картину, маємо зауважити, що «концепція Герасимова» мала джерелом також здобутки американців, котрі у пошуках засобів боротьби з міжнародним тероризмом звернули увагу на доцільність акценту «невоєнних операцій» (Operations Other Than War) за тісної взаємодії з недержавними акторами та медіа-середовищем. Це радикально змінювало підходи до військової

[1] Долженко О. О. Концептуальні засади та понятійно-категоріальне визначення «гібридної війни» в контексті загроз національній безпеці України. *Гілея.* 2018. Вип. 128. С. 315-317.

[2] Макмастер Герберт. Поля битв. Боротьба за захист вільного світу. Пер. з англ. Надія Коваль К.: Наш формат, 2023. С. 46.

[3] Макмастер Герберт. Поля битв. Боротьба за захист вільного світу. С. 46-47.

стратегії – щонайменше, першочергові цілі ударів обиралися тепер виходячи із подальшого «потрібного» інформаційного «резонансу» таких дій.

Ці стратегії пройшли перевірку під час операції «Буря в пустелі» (1991 р.), яка засвідчила ефективність використання інформаційно-психологічного інструментарію Збройних сил США, а потім використовувалися їхніми європейськими союзниками практично в усіх наступних військових операціях кінця XX – початку XXI ст.

Першою жертвою війни ставала інформаційна інфраструктура противника: вороже суспільство отримувало вже спеціально підготовану інформацію. Новий етап розвитку ця концепція отримала після трагічних подій 11 вересня 2001 року, коли головним противником стали розосереджені, горизонтальні мережі терористичних груп з автономними «комірками», без жорсткої вертикалі управління «країна-спонсор – лідер угруповання – польові командири – бойовики». Для боротьби з таким противником був потрібен цілком новий інструмент, який би обов'язково враховував і нову інформаційну реальність світу «Інтернету 2.0».

Так з'явилася нова концепція інформаційно-психологічного протиборства, яка дістала назву Мережно-центричне протиборство (Network-Centric Warfare – NCW).

Хиби застосування NCW полягали в тому, що США використовували в операціях, побудованих за «мережним» принципом, підрозділи регулярних збройних сил. Це знижувало ефективність інформаційного «резонансу», який є центральною метою усіх дій, оскільки при інформаційному повідомленні з поля бою головною ставала не подія сама по собі, а прив'язка усіх обставин до їх учасників – військовослужбовців США, фокусуючи на американських військових усі негативні контексти, пов'язані із їхнім образом.

Російське воєнно-політичне керівництво було в захваті від ідеї, а для усунення проблем з її практичним втіленням знайшли просте рішення: замість традиційних військових підрозділів використовувати «гібридні», неідентифіковані війська. Поки противник намагається зрозуміти, що є джерелом загрози, поки прийде до тями, операція завершується з тим інформаційним «ефектом», який формується агресором. Запозичену ідею «перехрестили» у «мережеві війни». Начальник російського генштабу генерал В. Герасимов прочитав лекції

перед складом Академії воєнних наук, які отримали назву «доктрина Герасимова 1.0 і 2.0».

Перша лекція, прочитана в січні 2013 року, спиралася на досвід «мережевого» протиборства в контексті подій «Арабської весни» – масових протестів і внутрішніх конфліктів на Близькому Сході в період 2010–2012 років (були трохи змінені акценти, а гібридний інструментарій отримав назву «асиметричні дії»). Ця ідея лягла в основу військової операції з анексії українського Криму і окупації частини українського Донбасу на початку 2014 року.

Водночас практика застосування гібридного підходу показала, що він є критично залежним від двох параметрів: 1) ефекту несподіванки, 2) часу. Якщо під час анексії Криму у лютому 2014 році російські гібридні підрозділи виконали практично усі поставлені завдання до того, як політичні й безпекові інституції України змогли подолати цей штучно створений «інформаційний хаос», то під час спроби окупації Донбасу, коли Україна знала, чого можна очікувати від росіян, у липні–серпні 2014 року росія була змушена відмовитися від «чистої» гібридної тактики і перейти до масованого використання регулярних збройних сил, які відкрито переходили російсько-український кордон на Сході для підтримки гібридних збройних формувань, що діяли на Донбасі.

Росії знадобилося кілька років, щоб проаналізувати отриманий досвід і виправити помилки. 2 березня 2019 року генерал Герасимов подав продовження свого попереднього виступу перед членами АВН, в якому були враховані практичні уроки і зроблені відповідні висновки.

Новий варіант гібридних методик РФ більшою мірою спирався на масштабне застосування конвенційних сил у масштабному збройному протистоянні, головною метою якого було «досягти переваги над рештою людства». Положення оновленої концепції щодо бачення гібридного інструментарію торувало шлях до повномасштабного вторгнення рф на територію України 24 лютого 2022 року, втілюючи концепт «стратегії активної оборони», фундаментальною частиною якого був «комплекс запобіжних заходів з нейтралізації загроз безпеці держави».

Як вважає Т. Жовтенко, повномасштабне вторгнення російських військ в Україну також засвідчило загальну обмеженість гібридної

стратегії кремля: перші дні вторгнення продемонстрували, що зс рф діють за тим самим шаблоном, як вони діяли в Криму 8 років до того, масштабувавши «кримську операцію» на територію усієї української держави і спираючись цього разу на більшу чисельність власних сил.[1]

За оцінками Макмастера, сукупність тверджень, що поєднують дезінформацію та заперечення власної відповідальності з використанням руйнівних технологій, за допомогою яких росія атакує сильні сторони цільових держав і грає на їхніх слабкостях, планування використання економічної залежності від енергоносіїв, які постачає росія, браваду, визнання доцільності використання удосконалених, неконвенційних, конвенційних і ядерних воєнних засобів, і склали «доктрину Герасимова», відому також під назвами «методичка Путіна», «російська війна нового покоління» – (РВНП), а також «гібридна війна».[2] (Останнє найменування вірне формально, але за суттю це не так, оскільки поняття «гібридна війна» придумали не герасимов і не путін, котрі у черговий раз привласнили чуже, аби надати якоїсь подібності «традиційності» людиноненависницьким «новаціям». Згадаємо, що Гітлер також фактично вів гібридну війну.)

Створення «власної російської» доктрини гібридної війни було пошуком та апробацією засобів досягнення бажаного глобального результату. «Спрощено геополітична мета Росії при розв'язанні глобального гібридного конфлікту усвідомлювалася таким чином: методами гібридної війни зруйнувати існуючий світопорядок, щоб відновити світопорядок періоду холодної війни і в ньому посісти звичне місце … слід зрозуміти і прийняти, що новий гібридний світо(без) порядок, який вибудовується на наших очах, – це не якийсь «транзитний стан», це і є нова реальність, котру аж ніяк не можна екстраполювати на реалії минулого. … у цій новій гібридній реальності може просто не виявитися гідного місця для Росії», бо вона «й сама стає дуже вразливою до інструментів і механізмів, методів і методологій гібридної війни якщо вони будуть використані проти неї».[3]

[1] Жовтенко Т. Гібридна війна: анатомія інструментарію й перемоги. 3 листопада 2022.. URL: https://dif.org.ua/article/gibridna-viyna-anatomiya-instrumentariyu-y-peremogi

[2] Макмастер Герберт. Поля битв. Боротьба за захист вільного світу. С. 47.

[3] Світова гібридна війна: український фронт: моногр. За заг. ред. В. П. Горбуліна. Харків: Фоліо, 2017. С.9-10.

Інформаційний та інформаційно-технологічний компоненти гібридної війни

Констатувавши привласнення російськими політиками і військовими концепції гібридної війни (принагідно зауваживши, що такі дії за їх сутністю також є елементом інформаційної війни), погодимось з позицією Г. Почепцова, що насправді поняття гібридної війни у сучасному (військовому) його розумінні увів Ф. Гоффман,[1] котрий сформулював кілька важливих постулатів: 1) «*Гібридні війни не є новими, але вони [щоразу] різні*». 2) «*Гібридні війни об'єднують у собі летальний характер державних конфліктів із фанатичним та затяжним запалом нерегулярної війни*». 3) у таких війнах має враховуватися взаємодія когнітивного та віртуального просторів.[2]

Гібридна війна надає перевагу тому, хто вміє працювати з масовою свідомістю. Сторона, що атакує, повинна доводити справедливість своїх дій як власному народові, так народу, на який націлена атака. А для атакованої сторони досить важко давати відповідь такій неоголошеній війні.[3]

Цікаво порівняти цей «перелік основних характеристик гібридної війни» зі «складовими стратегій гібридної війни», до яких С. Полумієнко зараховує: 1. Визначення і пропаганду власних «природних коренів» та інтересів у обраній для агресії країні. 2. Інформаційна обробка власного населення, заміна критеріїв добробуту політичними цілями, перенесення наголосу з внутрішніх проблем на зовнішні тощо. 3. Інформаційна обробка населення інших країн та регіонів для забезпечення підтримки агресії. 4. Встановлення контролю над ключовими підприємствами «супротивника», зокрема через ринкові механізми. 5. Створення військових баз, угруповань, максимально наближених до території обраного супротивника. 6. Визначення ворогів та конфронтація з країнами світу, які «стримують рух до світлого майбутнього і загрожують або шкодять країні». 7. Порушення міжна-

[1] Гібридна та складна війна. Вибір Януса: визначення сьогоднішнього багатогранного конфлікту. URL: Журнал Збройних Сил – Гібридна vs. складна війна (armedforcesjournal.com)

[2] Hoffman F. G. Hybrid warfare and challenges. *Joint Force Quarterly*. 2009. I. 52.

[3] З історії поняття гібридної війни в США і Росії. Георгій Почепцов. 1 листопада 2015. URL: https://ms.detector.media/mediaanalitika/post/14619/2015-11-01-z-istorii-ponyattya-gibrydnoi-viyny-v-ssha-i-rosii/

родних угод і договорів, їх інтерпретація та прикриття невиконання «власним розумінням». 8. Нехтування інтересами населення (у тому числі власного), одночасно з показовим наданням «гуманітарної допомоги». 9. Створення та підтримка національних, регіональних і міжнародних об'єднань, угруповань тощо з метою їх використання для переорієнтації суспільства, провокація конфліктів у суспільстві, порушення його нормальної життєдіяльності з метою викликання незадоволення та спротиву чинній владі. 10. Розмивання меж миру і війни, порядку і хаосу, створення зони ризику, у якій можна стати «гарантом» порядку у сфері впливу. 11. Встановлення та підтримка маріонеткових урядів. 12. Використання для своїх цілей економіки, територій країн-маріонеток, створення мережевої структури таких країн як точок дезорганізації нормальної життєдіяльності. 13. Використання силових стратегій під прикриттям. 14. Знищення економіки та інфраструктури країни, обраної супротивником. 15. Стратегічне планування агресії здійснюється за кількома напрямами й передбачає гнучке реагування на зовнішні обставини: контрдії країни – об'єкта нападу, реакції міжнародної спільноти тощо.[1]

Попри відмінності у назві та формулюваннях, у тому, й іншому випадку фактично йдеться про визначальні риси феномену гібридної війни, При цьому, незалежно від обсягу характеристик, визначальним є те, що власне війна (мілітарна війна) не займає чільного місця у протистоянні.

Відтак постає питання щодо чинників зростання популярності терміно-поняття «гібридна війна» і, значною мірою, витіснення ним традиційного поняття «війна».

Дехто вважає, що гібридна війна стала здобутком нового часу саме тому, що багато потрібних для неї завдань можна виконати за рахунок інформаційного компоненту. Чим сильнішим стає розвиток інформаційного компоненту, тим легшим буде виконання цих завдань.[2]

Натомість, інші автори зростання інтересу до категорії «гібридна війна» пов'язують з вадами існуючого розуміння поняття. При цьому зауважується, що «згідно з міжнародним правом, «війна» –

[1] Полумієнко С. К. Гібридна війна, її окремі передумови, стратегії та наслідки. *Вісник Національної академії наук України.* 2017. № 8. С. 78.

[2] Гібридна війна: інформаційна складова. Георгій Почепцов. 25 жовтня 2015. URL: https://ms.detector.media/mediaanalitika/post/14501/2015-10-25-gibrydna-viyna-informatsiyna-skladova/

це стан справ між двома державами, або між двома групами держав, або між державою і групою держав, який супроводжується здебільшого розірванням дипломатичних відносин, подальшим призупиненням застосування загальних норм міжнародного права мирного періоду і загальною рішучістю вчинити насильницькі дії, навіть якщо такі дії насправді не мають місця. Процеси глобалізації, необхідність ведення війн за ресурси та у вирішенні геополітичних конфліктів неминуче призводять до настання юридичних наслідків для країн-учасниць війни у вигляді міжнародних санкцій». На таких тезах ґрунтується висновок, що у XXI столітті постає гостра необхідність заміни класичного розуміння «війни» на модерне поняття «гібридна війна», яке *у* законодавстві країн учасників «війни» не визначене».[1]

Як на наш погляд, слушними є і одна, й інша точка зору, відображаючи обставини залежні (бажання обійти правила міжнародних угод та пов'язані з цим санкції тощо) та менш залежні (формування інформаційного суспільства, розвиток інформаційних технологій тощо) від волі людей.

В Україні першим монографічним дослідженням гібридної війни, що з'явилося після Майдану та російської агресії 2014 року стала вже згадувана книга Євгена Магди «Гібридна війна: вижити і перемогти», опублікована у 2015 році.[2]

Головним фронтом гібридної війни є фронт інформаційний, де росія інтенсивно використовує «приватно-державне партнерство» різноманітних медіа, реалізуючи три взаємопов'язані завдання: створює сприятливий інформаційний фон усередині Росії, здійснює килимові бомбардування дезінформацією українських громадян, формує сприятливе для себе інформаційне середовище на Заході. Не менш важливим є енергетичний фронт, оскільки кремль використовує енергоресурси як інструмент політичного впливу в Європі. Крім того, у випадку з Україною використовується проросійське лобі та представники радикальних політичних сил Старого Світу, переписування історії та інтенсивний вплив російської православної церкви на події на пострадянському просторі.

---

[1] Долженко О. О. Концептуальні засади та понятійно-категоріальне визначення «гібридної війни» в контексті загроз національній безпеці України. *Гілея.* 2018. Вип. 128. С. 315–317.

[2] Магда Є. В. Гібридна війна: вижити і перемогти», Х.: Віват, 2015. 304 с.

Слід погодитися з думкою, що гібридна війна стала здобутком нового часу саме тому, що багато потрібних для неї завдань можна виконати за рахунок інформаційного компоненту. Чим сильнішим стає розвиток інформаційного компоненту, тим легшим буде виконання цих завдань.[1]

При цьому істотне значення мають такі чинники як формування інформаційного суспільства, розвиток інформаційних технологій, що зумовлює «буденність» кібервійни (тут мається на увазі інформаційна війна, яка ведеться із застосуванням інформаційних – кібернетичних – технологій). Як зазначає Девід Сенгер, «хотілось би думати, наче кібервійна якось відрізняється від інших конфліктів, наче вона розгортається собі десь у хмарах окремо від того, що відбувається на землі. Коли держави створювали військово-повітряні сили, то міркували так само: повітряні бої – це одне, а перестрілка в окопах – інше. Аж під час Другої світової війни утвердилася концепція «єдиного бойового простору», що охоплює повітря, землю та море. У деяких країнах світу до цього вже додають і кіберпростір. Просто це важче помітити».[2]

Наразі практично не залишилось країн, котрі так чи інакше не переконались би у слушності цього зауваження. Особливо це стало відчутним після російської агресії проти України. Тим більше, що «у битві за територію України та душі її мешканців традиційна війна й кібервійна не просто доповнювали одна одну. Вони, немов стрічка Мебіуса, відображають конфлікт XXI століття, гладко раз у раз перетікаючи з поверхні на поверхню. Путін продемонстрував світові, наскільки ефективна така стратегія «гібридної війни…».[3]

Правові проблеми інформаційної гібридної війни ми вже розглядали у 2016-2018 рр.[4], але відтоді минуло чимало часу і багато що змінилося.

---

[1] Гібридна війна: інформаційна складова. Георгій Почепцов. 25 жовтня 2015. URL: https://ms.detector.media/mediaanalitika/post/14501/2015-10-25-gibrydna-viyna-informatsiyna-skladova/

[2] Сенгер, Девід Е. Досконала зброя. Війна, саботаж і страх у кіберепоху. Пер. з англ. Вікторія Дєдик: фах.ред.укр.вид Олександр Дєдик і Олег Фешовець. Львів: Астролябія, 2022. С. 227.

[3] Сенгер, Девід Е. Досконала зброя. С. 227.

[4] Information security and IT law in conditions of integration processes: [Collective monograph]. Edited by O. Kharytonova, E. Kharytonov. Riga: Izdevnieciba Baltija Publishing, 2017. 213 p.; Kharytonov E., Kharytonova O., Tolmachevska Y., Fasii B., Tkalych M. Information Security

Передусім, слід наголосити ще раз, що наразі «інформаційна війна» є родовим поняття щодо усіх видів протиборства у інформаційній сфері – як традиційних, так і сучасних , що відбуваються у кіберпросторі.

Завдяки цим якостям термін «інформаційна війна» має близько десяти значень. Обмежимось тут згадкою лише про розуміння її як форми протиборства між суб'єктами … що передбачає інформаційний вплив на населення з використанням ЗМІ, комп'ютерних мереж тощо з метою формування відповідної суспільної думки, підриву морального духу як усього суспільства, так і окремих його інституцій.[1]

На такому тлі поняття «кібервійна» визначається стисло: це – різновид інформаційної війни у кіберпросторі. Складовою частиною кібервійни є «кіберзагроза» – «дестабілізуючий чинник негативного впливу на об'єкт інформаційної безпеки шляхом використання технологічних можливостей кіберпростору, спрямованих на порушення конфіденційності, цілісності, авторства, спостережності та доступності інформації; загроза застосування деструктивних інформаційно-психологічних впливів на свідомість та психічний стан населення».[2] (Найбільш поширеною загрозою є кібератака – або ж – атака інформаційно-телекомунікаційної системи – цілеспрямований вплив на уразливі елементи такої системи з метою порушення доступності, цілісності та конфіденційності інформації, блокування роботи та виведення з ладу системи або її елементів; форма боротьби в телекомунікаційних системах[3]).

Як випливає з такого розуміння кіберзагроз, невід'ємною частиною їхньої характеристики є категорії «кіберзброя» і «кіберпростір».

---

and Means of Its Legal Support. Amazonia Investiga, 8(19). P.255-265; Харитонов Є. О., Харитонова О. І. Проблеми правового регулювання в ІТ-сфері в умовах інформаційної війни. *Проблеми відновлення конституційного ладу в Україні:* Матеріали міжнародної науково-практичної конференції. м. Київ. 19-20 травня 2017 р. Київ: Таврійський національний університет ім..В. І. Вернадського. 2017. С.159-163; Харитонов Є. О., Харитонова О. І. Проблеми відшкодування майнової шкоди у сфері використання інформаційних технологій. Спогади про Людину, Вченого, Цивіліста (до 90-річчя від Дня народження професора Діни Василівни Боброової); за заг. ред. Р. О. Стефанчука. К.: АртЕк, 2019. С.275-287.

1 Попова Т. В., Ліпкан В. А. Стратегічні комунікації. Словник. За заг. ред. В. А. Ліпкана. К.: ФОП О. С. Ліпкан. 2016. 416 с.

2 Попова Т. В., Ліпкан В. А. Стратегічні комунікації. С. 189-190.

3 Попова Т. В., Ліпкан В. А. Стратегічні комунікації. С. 35.

Кіберзброя розуміється як «різновид інформаційної зброї, головними елементами якої є інформація та інформаційні технології, способи і засоби інформаційного впливу й захисту віл нього, призначені для ведення інформаційної боротьби у кіберпросторі.

Кіберпростір, навіть на рівні елементарних характеристик має кілька значень: 1. Електроне інформаційне середовище, утворене організованою сукупністю взаємопоєднаних за єдиними принципами та правилами інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем. 2. Середовище існування та розповсюдження інформації, створюване кіберінфраструктурою. 3. Середовище, створюване інформаційними системами, об'єднаними у локальні або глобальні комп'ютерні мережі або реалізованими на окремих комп'ютерах та інших пристроях. 4. Уявне середовище, в якому за допомогою комп'ютерних мереж циркулює цифрова інформація».[1]

Як на наш погляд, поняття «інформаційна війна з використанням інформаційних технологій» пов'язане з поняттям «кібервійна», однак не є тотожним йому, оскільки останнє невід'ємно пов'язане з концептом «кіберпростір», котрий виступає і тлом, і кваліфікуючою ознакою кібервійни, кіберзагроз тощо. Враховуючи це, вважаємо за доцільне проблеми застосування кіберзброї, забезпечення кіберзахисту тощо розглянути в окремому розділі.

Висновки

Аналізуючи феномен гібридної війни у контексті російської агресії проти України, зроблено висновок, що поняття гібридної війни охоплює не лише сучасні форми ведення бойових дій, види війн майбутнього або назви конкретних конфліктів змішаного типу, а є новим видом глобального протистояння у сучасному дестабілізованому міжнародному безпековому довкіллі. Оскільки узагальнюючим терміном «гібридна війна» охоплюється низка різноманітних дій і поведінки, виникає необхідність структуризації відповідного концепту. Враховуючи викладене, передусім, доцільно розмежувати категорії «гібридна мілітарна війна» і «гібридна війна – загальне явище».

[1] Попова Т. В., Ліпкан В. А. Стратегічні комунікації. С. 190-191.

У першому випадку йдеться про «гібридність» війни як збройного конфлікту – конструкту, що виник на традиційному підґрунті, а тепер зазнає трансформацій внаслідок використання нових методів, форм і засобів воєнних дій.

У другому випадку – маємо на увазі «гібридність» війни у широкому сенсі – як соціального конфлікту, протистояння держав, спільнот, суспільств, цивілізацій. Війна у такому сенсі охоплює також «мілітарну війну» (збройний конфлікт), але може відбуватися взагалі без застосування традиційної зброї, але із застосуванням інших засобів впливу (примусу) підпорядкування однієї сторони конфлікту іншій його стороні.

«Гібридна війна» тут є родовим поняттям щодо поняття «війна – збройний конфлікт». Головною ознакою такої війни є її «гібридність: вона є одночасно війною інформаційною, економічною, репутаційною, смисловою. На неї повинні працювати всі, хто має вплив на населення: актори, співаки, письменники, режисери. Військові дії задають лише фон для більш масштабної війни в людському розумі. Практика застосування гібридного підходу показала, що він є критично залежним від двох параметрів: 1) ефекту несподіванки, 2) часу.

Гібридні війни не є новими, але вони [щоразу] різні. 2) «Гібридні війни об'єднують у собі летальний характер державних конфліктів із фанатичним та затяжним запалом нерегулярної війни». 3) у таких війнах має враховуватися взаємодія когнітивного та віртуального просторів.

Гібридна війна надає перевагу тому, хто вміє працювати з масовою свідомістю. Одним з різновидів такої війни є консцієнтальна війна як війна на ураження свідомості. Сторона, що атакує, повинна доводити справедливість своїх дій як власному народові, так народу, на який націлена атака. А для атакованої сторони досить важко давати відповідь такій неоголошеній війні. Гібридна війна стала здобутком нового часу саме тому, що багато потрібних для неї завдань можна виконати за рахунок інформаційного компоненту. Чим сильнішим стає розвиток інформаційного компоненту, тим легшим буде виконання цих завдань. При цьому істотне значення мають такі чинники як формування інформаційного суспільства, розвиток інформаційних технологій, що зумовлює «буденність» кібервійни.

«Кібервійна» є різновидом інформаційної війни у кіберпросторі. Складовою частиною кібервійни є «кіберзагроза» – «дестабілізуючий чинник негативного впливу на об'єкт інформаційної безпеки шляхом використання технологічних можливостей кіберпростору, спрямованих на порушення конфіденційності, цілісності, авторства, спостережності та доступності інформації; загроза застосування деструктивних інформаційно-психологічних впливів на свідомість та психічний стан населення.

Найбільш поширеною загрозою є кібератака – або ж – атака інформаційно-телекомунікаційної системи – цілеспрямований вплив на уразливі елементи такої системи з метою порушення доступності, цілісності та конфіденційності інформації, блокування роботи та виведення з ладу системи або її елементів; форма боротьби в телекомунікаційних системах.

Кіберзброя розуміється як «різновид інформаційної зброї, головними елементами якої є інформація та інформаційні технології, способи і засоби інформаційного впливу й захисту віл нього, призначені для ведення інформаційної боротьби у кіберпросторі.

Ключові слова: інформаційне суспільство, інформаційна сфера, інформаційні технології, інформаційна війна, гібридна війна, психічне насильство, консцієнтальна війна, ментальна війна, кібервійна, кіберпростір, кіберзагроза, кібератака, кіберзброя.

Розділ 4

ШІ ЯК БІНАРНА КАТЕГОРІЯ ІТ

DOI

Євген Харитонов
доктор юридичних наук, професор,
член-кореспондент НАПрН України

Олена Харитонова
докторка юридичних наук, професорка,
членкиня-кореспондент НАПрН України

Попередні зауваження

Як зазначалося у розділі 2 цієї книги, внаслідок того, що «ІТ-право», фактично, є спробою комплексного правового регулювання різноманітних відносин інформаційного суспільства, з позицій «нормативістського» підходу ні «ІТ-права», ні «Інтернет-права», як галузей права, не існує.

Натомість може йтися про «законодавство, що регулює відносини у сфері ІТ», тобто відносини, що виникають при використанні інформаційно-комунікаційних технологій. Уживаючи термін «ІТ-право», маємо характеризувати останнє не з позицій «позитивізму», а як концепт, тобто як сукупність уявлень, понять, знань, асоціацій та емоцій, що виникають у зв'язку з використанням цього терміну і характеризують його.

Оскільки Інтернет є одним із сегментів такої сфери, то відносини, що виникають у мережі, є правовими відносинами. За бажання їх можна іменувати «Інтернет-правовідносинами», хоча точніше було б говорити про «правовідносини у мережі», «мереживні правовідносини» або «правовідносини, що складаються в Інтернеті».

Отже, виходимо з того, що «ІТ-право» – це концепт, «ІТ-законодавство» – позірна сукупність норм, що регулюють відносини, поєднані з інформаційними технологіями, а «Інтернет-правовідносини» («правовідносини, що складаються в Інтернеті», «мереживні право-

відносини» тощо), – це інформаційно-комунікативні відносини, врегульовані нормами цивільного, адміністративного, податкового тощо законодавства. Більшість норм, які регулюють згадані відносин, належать до цивільного законодавства.

Усвідомлюючи неточність і приблизність такого позначення, з міркувань зручності далі рівно використовуємо терміни «Інтернет-правовідносини» («правовідносини, що складаються в Інтернеті», «мереживні правовідносини»).

Дискусійність низки положень концепту «ІТ-право», актуальність вирішення питань захисту прав та інтересів учасників відносин, що виникають при використанні інформаційних (інформаційно-комунікаційних) технологій, не визначені остаточно засади регулювання ІТ-відносин, зростання загроз у кіберпросторі в зв'язку гібридною інформаційною війною, зумовлюють необхідність з'ясування особливостей механізму правового регулювання у цій галузі. Тим більше, що досліджень цивілістичних проблем у цій галузі поки що недостатньо.

Враховуючи зазначене, розглянемо далі особливості механізму цивільно-правового регулювання цивільних відносин, враховуючи, що повномасштабна збройна агресія росії стала серйозним викликом усій системі регулювання суспільних відносин. Разом із тим, очевидно, найбільшого потрясіння зазнала система регулювання цивільних відносин, (частина 1 ст. 1 ЦК України),[1] котра вже за самою своєю сутністю призначена забезпечувати звичайне, повсякденне буття людини, зокрема, створення та використання інформаційних технологій, користування соціальними мережами тощо.

Механізм цивільно-правового регулювання під час війни: загальні засади

У цій науковій розвідці виходимо з загальнотеоретичного розуміння механізму правового регулювання як сукупності правових засобів та заходів, за допомогою яких здійснюється правовий вплив на суспільні відносини з метою їхнього впорядкування.[2]

[1] Майданик Р. Цивільні відносини: поняття та види. *Право України.* 2009. № 8. С. 20-27.

[2] Кельман М. С., Мурашин О. Г. Загальна теорія держави і права: підручник. Київ, 2008. С.372.

У загальній теорії виокремлюють наступні елементи механізму правового регулювання (іменуючи їх також «правовими засобами»: 1) норми права; 2) правовідносини; 3) акти застосування; 4) акти тлумачення норм права. (При цьому перші два елементи зараховують до головних, а останні два – до факультативних).[1]

Зазначені положення загальної теорії права стали методологічною основою розуміння механізму правового регулювання суспільних відносин різними галузями законодавства.

Деякі автори наголошують на тому, що «поняття механізму охоплює дві сторони правового регулювання: 1) забезпечення за допомогою сукупності правових засобів правового впливу на суспільні відносини і, отже, забезпечення ефективності правового впливу; 2) це внутрішня будова механізму, його окремі елементи (частини), взяті у співвідношенні».[2]

Тобто, фактично, йдеться про «функціональне» і «структуралістське» тлумачення цього феномену, і, у підсумку, – про власне механізм і про «дію механізму».

Такий варіант характеристики механізму правового регулювання ІТ-відносин видається прийнятним, оскільки дає можливість тлумачення його стосовно Мережевих відносин (із деякими застереженнями) як природно/технічно-соціального феномену, буття якого забезпечується за допомогою юридичних заходів (створення певних структур тощо).

Положення загальної теорії права є загальною методологічною основою розуміння механізму правового регулювання суспільних відносин різними галузями національного законодавства. Разом із тим, тлумачення цієї категорії має галузеві особливості. Якщо у адміністративному праві позиція з цього питання, фактично, збігається з основними ідеями у загальній теорії права, то формування цивілістичної концепції механізму правового регулювання триває.

При цьому, хоча «цивілісти в основному дотримуються тих положень вчення про механізм правового регулювання, які є базовими в осмисленні всієї проблематики та вироблені протягом тривалого часу

[1] Кривицький Ю. В. Механізм правового регулювання в сучасній теорії права. *Часопис Київського університету права.* 2009. № 4. С. 77.

[2] Андреєв А. Механізм правового регулювання суспільних відносин: окремі аспекти щодо визначення поняття та особливостей. *Підприємництво, господарство і право.* 2019. № 6. С. 126.

на рівні загальнотеоретичних досліджень», але має враховуватися «галузева специфіка механізму цивільно-правового регулювання, зумовлена особливостями цивільних відносин та їх окремих видів, як різновиду приватних відносин».[1]

З цього приводу зауважимо, що, хоча використання здобутків теоретиків права є логічним, однак у розумінні категорії «механізм правового регулювання» на загальнотеоретичному і галузевому (зокрема, на цивілістичному) рівнях існують суттєві відмінності, котрі мають бути враховані, але зазвичай, ігноруються внаслідок недооцінки різниці між «загально-соціальниим» та «легістським» розумінням права.[2]

Якщо у характеристиці механізму правового регулювання на рівні загальної теорії права переважає легістський (позитивістський) підхід, публічно-правовий за сутністю, то у цивілістиці ця категорія характеризується з позицій приватно-правових.

Відтак виходимо з того, що цивільне право України, котре є втіленням головних ідей приватного права на рівні національної правової системи,[3] визначає статус приватної особи, підстави придбання та порядок реалізації такою особою цивільних прав та обов'язків, засади захисту її прав та інтересів.

У зв'язку з цим необхідно скоригувати загальні положення концепції механізму правового регулювання з урахуванням розділення вивчення права на приватне та публічне, і відповідно.

Зауважимо, що, коли за усталеного нормативістського підходу положення загальної теорії права повністю придатні для застосування у сфері публічній, то у приватноправовій сфері такий підхід, навряд чи, можна визнати виправданим. Такий висновок випливає з

---

[1] Мазур В. В. Механізм цивільно-правового регулювання: теоретико-методологічний аспект. *Науковий вісник Ужгородського національного університету*, 2016. Серія ПРАВО. Випуск 36. Том 1. С. 108-113.

[2] Рабінович П. М. Приватне право і публічне право як загальносоціальні явища та як легалізовані терміно-поняття. *Еволюція цивільного законодавства: Проблеми теорії і практики*: Матеріали міжнарод. науково-практ. конф. 29–30 квітня 2004 року. Харків-Київ, 2004. С. 14–31.

[3] Селіванов В., Діденко Н. Діалектика приватного та публічного в правовому регулюванні. *Право України.* 2001. № 11. С. 15-22; Харитонов Є., Харитонова О. До питання про значення дихотомії «приватне право – публічне право». *Вісник Академії правових наук України.* 2000. № 2. С. 82-88; Рабінович П. Приватне й публічне у природному праві та законодавстві. *Вісник Академії правових наук України.* 2004. № 3 С. 3.

того, що приватне право не може починатися з актів законодавства йдеться про акти законодавства:, процесу законотворчості має передувати усвідомлення того, яким чином ідеї приватного права можуть втілюватися у юридичний побут.

При цьому враховуємо, що сфери дії цивільного права також стосується загальна тенденція розвитку правової системи, згідно якій «сьогодні зростає соціальна спрямованість правової системи як засобу формування і реалізації інтересів суб'єктів права шляхом закріплення певних цілей, норм, правил поведінки. Особливого значення при цьому набуває забезпечення оптимального поєднання соціального і правового принципів розвитку суспільства».[1] У зв'язку з цим наголошується також, що сьогодні до цього додаються ще й такі «загальносоціальні завдання, як гарантування національної небезпеки, ліквідація наслідків пандемії, екологічних катастроф, реалізація соціальних програм, які відображатимуть позиції «все необхідне враховане», підтримання реабілітаційних заходів».[2] Це положення, сформульоване у рік, що передував повномасштабному російському вторгненню, логічно має бути і згадкою про завдання, які постають у зв'язку з цим перед правовою системою України.

Враховуючи зазначене, не можемо ігнорувати ту обставину, що під час війни механізм правового регулювання цивільних відносин, зокрема, у сфері ІТ, має коригуватися відповідно до головної мети суспільства: подолати екзістенційні загрози.

На перетині двох названих вимог і в такому, зумовленими ними, контексті формуються особливості концепції цивільно-правового механізму регулювання в умовах гібридної війни.

При цьому одним з найважливіших питань, що має бути вирішене вже на першій стадії, яка передує власне правовому регулюванню відносин, є : 1) формування концепції правового регулювання; 2) визначення меж юридичного впливу; 3) прогнозування очікуваних результатів. Без цього неможливе визначення кола проєктів нормативних актів, які мають бути підготовлені на етапі наступному.

---

[1] Оніщенко Н. М. Цінність права: соціальний вимір. *Новий шлях до права. Колективна* монографія. Кер. авт. колективу А. О. Селіванов. К.: Алерта, 2021. С. 7-15.

[2] Копиленко О. Л., Оніщенко Н. М. забезпечення прав людини в контексті радіаційного захисту: передумови практичної реалізації. *Бюлетень Мін'юсту України.* 2020. № 1. С. 34-40.

Проблема визначення меж та засад правового регулювання

Можливості переходу від стадії «формування концепції» правового регулювання, до власне «правового регулювання» лімітуються також межами правового регулювання. Останні визначаються як сфера відносин між людьми, котра з тих чи інших міркувань не може бути врегульована правом. При цьому постає питання про взаємини, стосунки між особистістю і державою з погляду меж влади останньої.

Як зазначав Й. О. Покровський, «не підлягає сумніву, що держава може і навіть зобов'язана обмежувати, тобто вводити у певні рамки, індивідуальну свободу і у цьому сенсі жертвувати індивідуальними інтересами на користь громадських».

Відтак на підґрунті низки логічних посилань він вибудовує принципово важливий висновок, котрий з часом не втратив своєї актуальності. Суть його полягає в необхідності чітко розрізняти дві відмінні частини спірної території: з одного боку, внутрішнє, духовне життя людини (що має своїм кульмінаційним пунктом її релігійне віросповідання)… , а з іншого боку – відносини зовнішнього, головним чином економічного характеру. Перші, духовні інтереси складають зміст, саму сутність людської особистості – те, що дає їй відчуття її дійсного, правдивого «я» і від чого вона не може відмовитись, не втративши себе….

Інша річ блага зовнішні, матеріальні… Вони завжди розглядаються лише як засіб для задоволення якихось інших потреб, для досягнення якихось інших цілей».

Але, як на нашу думку, наведені вище міркування є слушними стосовно сфери публічного права («позитивної» його частини). Що ж стосується сфери приватного права, то тут (якщо виходити з того, що учасники цивільних відносин можуть врегулювати договором між ними практично будь-які питання) межі «приватного» регулювання, очевидно, визначаються лише засадами приватного права.

Власне, йдеться про реалізацію концепту приватного права, який можна також вважати «підґрунтям» механізму цивільно-правового регулювання у цій сфері.[1]

[1] Харитонов Є., Харитонова О. Приватне право як концепт. Том VI. Приватне право в умовах гібридної війни: монографія. Одеса: Фенікс, 2024. С. 104-112.

Разом із тим, ці положення є чинними щодо механізму правового регулювання цивільних відносин у звичайних умовах, коли засади і доцільності правового регулювання є принципово різними для сфери приватного і публічного права.

Однак із врахуванням тієї обставини, що формування та прийняття актів цивільного законодавства в умовах гібридної війни, значною мірою втрачає свій приватноправовий характер, особливостями відповідного елементу механізму цивільно-правового регулювання є положення, згідно якому природне право в умовах гібридної війни не є безперечним підґрунтям актів цивільного законодавства, якими регулюються інформаційно-комунікаційні відносини.

Це зауваження стосується і засад правового регулювання ІТ-відносин, котрі мають приватно-правові та публічно-правові аспекти (охоплюють приватноправовий і публічно-правовий підходи). Приватноправовий підхід ґрунтується на визнанні природних, невідчужуваних прав особи, які не створюються, а лише визнаються і підтверджуються нормами законодавства. Публічно-правовий підхід ґрунтується на твердженні, що держава не визнає, а створює права особи, наділяючи ними окремих громадян і визначаючи тим самим обсяг правоздатності, а отже й потенційних суб'єктивних прав кожного з них, який може бути збільшений або зменшений на розсуд самої держави.[1]

З урахуванням цих міркувань можна зробити висновок, що при характеристиці суб'єктивних прав, визначенні засобів їхнього правового забезпечення тощо, необхідно, передусім, визначити, чи входять вони до змісту правовідносин приватного або публічного права, тобто чи є елементом зв'язків «горизонтального» або «вертикального» типу. Вся система суб'єктивних прав може поділятися, таким чином, на публічні та приватні суб'єктивні права, що й визначає засади їхнього правового забезпечення.

У свою чергу, важливим чинником коректив правового регулювання цивільних відносин є гібридна війна. Але, враховуючи, що це поняття є складним і має більше 10 різновидів, далі коротко розглянемо як впливає на категорії «права людини» і «цивільні права» за-

[1] Харитонова О. І. До питання про класифікацію правових відносин. *Науковий вісник Чернівецького університету.* Вип. 125: Правознавство. Чернівці, 2001. С. 13-16.

провадження внаслідок повномасштабного російського вторгнення воєнного стану.[1]

Тут скористаємось простим і зручним з точки зору практичного використання визначенням «прав людини» як невідчужуваних свобод і прав особи, котрі індивід отримує в силу свого народження, основне поняття природного і будь-якого права взагалі;[2] або ж як певних можливостей людини, необхідних для її існування та розвитку в конкретно-історичних умовах, які об'єктивно визначаються досягнутим рівнем розвитку людства (економічним, духовним, соціальним) і мають бути загальними та рівними для всіх людей».[3]

Однак для цілей нашого дослідження доцільною здається характеристика цієї категорії у контексті її зв'язку з функціонуванням механізму правового регулювання та впливу на нього запровадження воєнного стану.

У зв'язку з цим варто згадати про існування двох варіантів юридичної конструкції прав людини: 1) модель, за якої існує фіксований перелік прав (найбільш поширена у сучасному світі. Її притримується й Україна); 2) модель, де такий перелік відсутній (прикладом зазначеної моделі вважається Велика Британія, згідно з положеннями внутрішнього права якої «кожен громадянин має право робити, що йому завгодно, якщо це не заборонене загальним чи правовим статутом». Далеко не повний перелік прав міститься також в конституціях Бельгії й Австрії).[4]

Для нашого дослідження розрізнення двох згаданих моделей має те значення, що функціонування механізму правового регулювання у першому випадку спрямоване на обмеження вказаних у конституціях прав людини, а відтак має супроводжуватися одночасним замінюванням (тимчасовим) призупинених норм законодавства.

---

1 Харитонов Є. О., Харитонова О. І. Права людини та цивільна правоздатність в умовах воєнного стану. *Проблеми реалізації норм Конституції України в умовах воєнного стану* (присвячена 30-ій річниці створення навчально-наукового юридичного інституту Прикарпатського національного університету імені Василя Стефаника) : матеріали міжнародної науково-практичної інтернет-конференції (м. Івано-Франківськ, 27 червня 2022 року). Івано-Франківськ : Прикарпатський національний університет імені Василя Стефаника, 2022. С. 172-179.

2 Андрусяк Т. Г. Теорія держави і права. Львів, 1997. С.62.

3 Рабінович П. М. Основи загальної теорії права та держави. К., 1995. С.7.

4 Четверте покоління прав людини: особливості правового регулювання, проблеми та перспективи розвитку в сфері охорони здоров'я: монографія. За заг.ред.: С. Б. Булєци, М. В. Менджул. Ужгород: ВидГоверла» 2020. С. 10-11. (автор підрозділу Д. М. Бєлов)

Натомість, у другому випадку такої необхідності немає, оскільки встановлення певних заборон на позитивну поведінку не впливає на дію загального принципу: «кожен громадянин має право робити, що йому завгодно, якщо це не заборонене загальним чи правовим статутом».

Враховуючи, що в Україні прийнята перша модель, розглянемо далі, як на ній відображається запровадження воєнного стану з 5:30 24 лютого 2022 року.

З цього часу в Україні на період дії правового режиму воєнного стану, можуть обмежуватися конституційні права і свободи людини і громадянина, передбачені статтями 30–34, 38, 39, 41–44, 53 Конституції України, а також вводитися тимчасові обмеження прав і законних інтересів юридичних осіб в межах та обсязі, що необхідні для забезпечення можливості запровадження та здійснення заходів правового режиму воєнного стану, які передбачені частиною першою статті 8 Закону України «Про правовий режим воєнного стану».

Згідно зі статтею 8 Закону України «Про правовий режим воєнного стану», військове командування разом із військовими адміністраціями (у разі їх утворення) може вживати низку заходів, що стосуються сфери цивільних прав. Зокрема, регулювати роботу підприємств телекомунікацій, поліграфічних підприємств, видавництв, телерадіоорганізацій, телерадіоцентрів та інших підприємств, установ, організацій і закладів культури та засобів масової інформації, а також використовувати місцеві радіостанції, телевізійні центри та друкарні для військових потреб і проведення роз'яснювальної роботи серед військ і населення; забороняти роботу приймально-передавальних радіостанцій особистого і колективного користування та передачу інформації через комп'ютерні мережі; у разі порушення вимог або невиконання заходів правового режиму воєнного стану вилучати у підприємств, установ і організацій усіх форм власності, окремих громадян телекомунікаційне обладнання, телевізійну, відео- і аудіоапаратуру, комп'ютери, а також у разі потреби інші технічні засоби зв'язку; вживати додаткових заходів щодо посилення охорони державної таємниці.[1]

[1] В Україні запроваджено воєнний стан: що це означає. 24.02.22. URL.: https://www.legalaid.gov.ua/publikatsiyi/v-ukrayini-zaprovadzheno-voyennyj-stan-shho-tse-oznachaye-2/

Варто зауважити, що в цивілістиці категорія «права людини» використовується з певними застереженнями, як не властива безпосередньо цій галузі. Натомість, йдеться про немайнові та майнові «права фізичної особи».

Однак це не означає відсутності певного кореспондування згаданих понять. Так, серед регулятивних правовідносин розрізняють загальні та конкретні правовідносини, враховуючи різницю між ними, яка полягає в тому, що перші пов'язані в основному з такими формами реалізації юридичних норм, як дотримання, виконання та використання, а другі опосередковують їхнє застосування. Відповідно конкретні правовідносини опосередковують застосування права, а загальні – охороняють та забезпечують право.

Зокрема, загальні регулятивні правовідносини пов'язані з дотриманням членами суспільства законів, правопорядку, конституційних норм, прав людини. У межах загальних правовідносин реалізуються основні (природні) права людини, зафіксовані у міжнародних актах, Загальній декларації прав людини, інших документах.

Що стосується конкретних правовідносин, то вони виникають на підставі конкретних юридичних фактів, чому й отримали таку назву. Їх завданням є обслуговування щоденних потреб, запитів та інтересів суб'єктів права: повсякденного буття людини, цивільного обігу, ринку, праці, виробництва тощо. Такі правовідносини виникають, припиняються та змінюються безперервно. Деякі з них дуже короткотермінові, швидкоплинні. Вони очевидні, суворо індивідуалізовані.[1]

Варто зауважити, що традиційно до числа цивільних правовідносин, зазвичай, відносять конкретні правовідносини. Такий підхід має під собою відповідне методологічне підґрунтя, котре відображається у базовому розумінні суб'єктивного цивільного права як міри можливої (дозволеної) поведінки однієї особи, якій відповідає міра належної поведінки іншої особи.[2]

З традиційного цивілістичного погляду, «права людини» можуть бути віднесені до загальних цивільних відносин, а «суб'єктивні права фізичної особи» – до конкретних.

---

[1] Харитонов Є. О., Харитонова О. І. Регулятивні правовідносини: приватноправовий та публічно-правовий виміри: монографія. Одеса, 2018. С. 136.

[2] Харитонов Є. О., Харитонова О. І. Цивільні правовідносини : моногр. 2-ге вид., перероб. і доп. Одеса, 2011. С.123.

Однак, тут маємо враховувати можливість характеристики категорії правовідносин на трьох рівнях: 1) як категорії загальної теорії права; 2) як категорії приватного права; 3) як категорії певної (конкретної) галузі права.[1] Відтак враховуємо й те, що права приватної особи (другий рівень розуміння) від прав фізичної особи у цивільних правовідносинах (третій рівень розуміння) відрізняються більш високим ступенем узагальнення, врахування засад і норм природного права тощо.

Під таким кутом зору права людини можемо оцінювати як права приватної особи, котрі на рівні національному регламентуються та захищаються нормами цивільного законодавства. Разом із тим, зауважимо, що йдеться саме про «права приватної особи», а не про правоздатність останньої. Правоздатність є характеристикою загального правового становища приватної особи, що найбільш точно відображається у понятті «цивільна правоздатність», яке може бути застосоване щодо кожної «абстрактної» людини. Натомість, «суб'єктивне цивільне право» має певна, конкретна людина, що, власне, відображається і у позначенні «суб'єктивне цивільне право», тобто, «право, що належить певному суб'єкту».

Звідси випливає, що стосовно визначення наслідків запровадження воєнного стану може йтися про здійснення, захист тощо цивільних прав, обмеження цивільної дієздатності та спроби обмеження цивільної правоздатності, вирішення колізії суб'єктивних прав учасників цивільних відносин тощо.

Отже можна зробити попередній висновок, що основна проблема у демократичному суспільстві полягає у виникненні колізії не лише публічних і приватних прав (інтересів), але й прав (інтересів) приватних осіб – суб'єктів цивільних прав.

При цьому доцільно вести мову не про «зіткнення» прав та інтересів учасників відповідних правовідносин, як це має місце, скажімо, при запроваджені карантину, про «колізії» прав, які загалом мають однакову спрямованість: максимальне зосередження зусиль держави, суспільства і окремих осіб на подоланні загроз збройної агресії та шкідливих наслідків після неї.

Отже, як випливає з викладеного, в умовах воєнного стану може бути обмежена низка прав людини та прав особи, пов'язаних з ви-

[1] Харитонов Є. О., Харитонова О. І. Приватне право як концепт. Т. IV: Від ідеї до реалізації : монографія. Одеса, 2021. С. 335.

користанням інформаційно-комунікаційних технологій. Очевидно, найбільші за обсягом і найбільш відчутними для приватних осіб є обмеження, що стосуються Мереж.

Механізм цивільно-правового регулювання та Інтернет

На початку третього тисячоліття інформаційні технології, пов'язані зі Всесвітньою Мережею (Інтернет) продовжували стрімко розвиватися, результатом чого стало те, що за перше десятиліття XXI ст. кількість користувачів у Мережі зросла з 350 мільйонів до більше, ніж двох мільярдів.[1] Сформувалося покоління «I-Gen» (Internet Generation), для якого визначальним є право вільного доступу до кожного інтелектуального продукту в Мережі.

Навіть, поза межами воєнного стану і війни тут існувала низка соціальних проблем, частину яких за нормальних умов почали вирішувати правовими засобами шляхом впорядкування відносин, що складаються у цій сфері, та узгодженням інтересів їх суб'єктів. Однак гібридна війна створила низку додаткових серйозних проблем у сфері правового буття Інтернет, котрих варто тут торкнутися.

Наразі існує чимало визначень «Інтернет-відносини» як частини відносин у віртуальному просторі, з характеристикою їхніх учасників, вказівками на специфіку цих відносин, таких як невизначеність місцезнаходження сторін; складнощі ідентифікації учасників відносин у Інтернет; залежність відносин між учасниками в Інтернеті від відносин з інформаційними провайдерами; електронний характері документообігу у мережі; невизначеність юридичного статусу Інтернет; існування віртуальних організацій тощо.

На нашу думку, достатньо згадки про дві визначальні ознаки: 1) специфічний об'єкт відносин (належність до ІТ-сфери або ж, «інформаційно-комунікаційної сфери»; 2) специфічний суб'єктний склад відносин.

Далі акцентуємо увагу лише на кількох аспектах, котрі, як нам здається, мають тут найбільше значення.

[1] Ерік Шмідт, Джаред Коен. Новий цифровий світ. Львів, 2015. С.10.

Ведучи мову про науковий доробок у цій галузі, необхідно зробити деякі уточнення термінологічного характеру, зокрема, стосовно вживання виразу «мережа Інтернет» (котрий іноді використовувався і в наших працях). Неточність полягає в тому, що термін «Інтернет», власне, вже означає «міжнародна мережа» (від англ. International Network), «міжмережа». Отже виходить, що «мережа Інтернет» – це щось на кшталт «мережа міжнародної мережі». Очевидно, цілком достатньо позначення «Інтернет» або ж «Мережа».

Строго кажучи, не надто коректним є й використання терміну «Інтернет-відносини». Натомість, має йтися про «відносини у Інтернет», оскільки відносини, що складаються у Мережі, існують одночасно з реальними стосунками, віртуально відображаючи останні та співпадаючи з ними за змістом. Віртуальні відносини можна класифікувати за предметним критерієм так само, як і відносини реальні. Отже у цифровому середовищі після врегулювання їх юридичними нормами виникають правові відносини різної галузевої приналежності: цивільні, адміністративні, фінансові тощо. Крім того, за їх межами залишаються правовідносини, що виникають при порушенні прав і обов'язків суб'єктами, які діють у Мережі, – правовідносини цивільної, адміністративної, карної тощо відповідальності. (Втім, з міркувань зручності викладу терміни «Інтернет-відносини» та «Інтернет-правовідносини» вживаємо й ми і у цій книзі).

Специфіка таких відносин, з погляду оцінки їх суб'єктного складу, полягає в наступному. По-перше, невизначеністю місцезнаходження сторін, що зумовлює можливі проблеми з правом, що застосовується, а також з реальним виконанням зобов'язань. По-друге, складністю ідентифікації учасників відносин у мережі Інтернет. По-третє, існуванням віртуальних організацій. По-четверте, залежністю відносин між учасниками мережі Інтернет від відносин з інформаційними провайдерами. Таким чином, існує проблема визначення суб'єктного складу правовідносин, що виникають у цифровому середовищі, вирішення якої дозволить встановити особливості правового статусу кожного з видів таких суб'єктів.

Відомим (завжди визначеним) суб'єктом правовідносин у мережі Інтернет є володілець авторських прав. Іншою (але не єдиною) стороною у зазначених відносинах є користувачі. Існує ще два види суб'єктів відносин, що виникають у мережі Інтернет: власники інтер-

нет-сайтів, що надають послуги з надання дискового простору для розміщення інформації на сервері, підключеному до Інтернету, та провайдери, що забезпечують функціонування та використання мережі.

Інтернет-сайти бувають двох видів: платні та безоплатні. Платний сайт надає послуги за плату, тому, оскільки ця діяльність є для нього підприємницькою, виявити його досить просто. Складніше з тими сайтами, які надають безкоштовні послуги у мережі, оскільки справжнє ім'я, місцезнаходження володільця можуть не відповідати заявленим реєстратору (реєстрація відбувається без присутності користувача, для реєстрації необхідні мінімальні дані).

Сьогодні інтернет-провайдери та онлайн-платформи стають ключовими учасниками цифрового середовища[1].

Інтернет-провайдери здійснюють лише технічний супровід доступу до інтернет-сайту, що належить клієнту. У залежності від послуг, які надаються, Інтернет-провайдери діляться на види: провайдери доступу, кеш-провайдери, провайдери посилань тощо. Зауважимо, що в міжнародній практиці та законодавстві не існує єдиної позиції щодо визначення правового статусу провайдера та його ролі у попередженні та припиненні порушень авторських та суміжних прав в Інтернет. У законодавстві зарубіжних країн існує три підходи до визначення правового статусу провайдера:

1. «Розширений» – на вимогу правовласника провайдер має право контролювати діяльність користувача, на якого було отримано скаргу; згідно із рішенням органу владних повноважень повинен надавати конфіденційну інформацію про користувачів; видаляти піратський контент або блокувати доступ до сайтів, на яких він міститься; на основі рішення суду припиняти доступ порушники до Інтернет (зокрема, Франція, США, КНР, Бразилія). Позитивним моментом використання цього підходу є швидкість реагування на порушення авторських і суміжних прав в мережі Інтернет, однак він іноді призводить до зловживання та порушення прав осіб на конфіденційну інформацію, а отже не може бути визнаним оптимальним з погляду забезпечення інформаційної безпеки;

[1] Зінич Л. В. Правові аспекти відповідальності інтернет-провайдерів за порушення прав інтелектуальної власності. *Юридичний науковий електронний журнал.* 2025. № 3. С. 288.

2. «Обмежений» – на вимогу правовласника провайдер має право контролювати діяльність користувача, на якого було отримано скаргу, однак розкриття конфіденційної інформації, блокування сайтів та припинення доступу до Інтернет може відбуватися лише на основі рішення суду (зокрема, Канада, Великобританія). Є найбільш дієвим та справедливим підходом до вирішення проблеми забезпечення провайдером охорони авторських і суміжних прав в Інтернет, при цьому з урахуванням права особи на конфіденційність інформації;

3. «Вузький» – провайдер має право контролювати дії користувачів лише на вимогу державних органів, при цьому розголошення конфіденційної інформації, блокування сайтів та припинення доступу до Інтернет може відбуватися лише на основі рішення суду (зокрема, Україна, Данія). Такий підхід вважається менш ефективним, оскільки не гарантує швидкості реагування на порушення в Інтернет. Попри це, необхідно зауважити, що така модель забезпечення прав авторів та правовласника цілком прийнятна, особливо в країнах, де забезпечення провайдерів засобами контролю всіх користувачів Інтернет є достатньо фінансово та технічно складною процедурою.

Проблема визначення повноважень Інтернет-провайдерів більшістю країн світу вирішується покладенням на останніх певних функцій, пов'язаних із наглядом та перевіркою діяльності користувачів у Інтернет. У деяких країнах Інтернет-провайдери виконують рішення державних органів щодо видалення піратського контенту, закриття сайтів, відключення користувача від мережі.

Провайдери цифрових платформ довго залишалися у сліпій зоні правового регулювання, користуючись своїм імунітетом від відповідальності за поширення протиправного контенту, браком міжнародних норм у цій сфері та публічним сприйняттям як блага. Після низки подій у середині 2010-х років, яким провайдери платформ не змогли запобігти, ЄС посилив вимоги щодо їхньої діяльності із забезпечення прав користувачів. Україна вже імплементувала Директиву ЄС про аудіовізуальні медіапослуги, яка закріплює низку обов'язків для платформ спільного доступу до відео. Наступним кроком на цьому шляху має стати впровадження Акта ЄС про цифрові послуги[1].

[1] Дворовий М. В. Правове регулювання провайдерів цифрових платформ в Україні: початок європейського шляху. *Захист прав та інтересів особи в умовах реформування приватного права в Україні :* збірник наукових праць учасників круглого столу (28 лютого 2025 року). Київ : НаУКМА, 2025. С. 89-95.

Цей Акт з 2020 року обговорювався у формі Проєкту Акту про цифрові послуги (*Digital Services Act, DSA*). У листопаді 2022 року він набув чинності, а повноцінно DSA запрацював вже з 17 лютого 2024 року. Цей акт є системним рішенням у сфері онлайн-безпеки в ЄС, і його основним гаслом є «*все що заборонено офлайн, має бути забороненим онлайн».*

Основні рішення, запропоновані DSA для обмеження шкідливого впливу онлайн-платформ, зосереджуються довкола модерації контенту. Так, особливу увагу європейські законотворці приділяють процедурам сповіщення про наявність протиправного контенту *(notice and action)* та можливості оскарження рішень платформ. Акт також передбачає низку зобов'язань належної обачності (*due diligence*), зокрема щодо налагодження стійкої комунікації з органами влади та громадянами, прозорості платформ та вимог до їх правил користування[1].

У сфері прав інтелектуальної власності правове регулювання діяльності інтернет-провайдерів здійснюється такими міжнародними та національними актами, як Бернська конвенція про охорону літературних і художніх творів, Договір Всесвітньої організації інтелектуальної власності про авторське право, Договір Всесвітньої організації інтелектуальної власності про виконання і фонограми, Законами України «Про авторське право і суміжні права»[2] і «Про електронні комунікації»[3]. Відповідальність інтернет-провайдерів за порушення прав інтелектуальної власності встановлена Цивільним кодексом України, Кодексом України про адміністративні правопорушення та Кримінальним кодексом України. Одним із основних законів у цій сфері є Закон «Про авторське право і суміжні права», який, у статті 58 – відповідальність провайдерів послуг обміну контентом за порушення авторського права та/або суміжних прав, – встановлює правові засади відповідальності інтернет-провайдерів.

Враховуючи викладене вище стосовно особливостей «Інтернет-відносин» та «Інтернет-правовідносин», ще раз наголосимо, що

[1] Координатор цифрових послуг: новий гравець в регулюванні онлайн-платформ та хто ним стане в Україні? URL: https://dslua.org/publications/koordynator-tsyfrovykh-posluh/

[2] Про авторське право і суміжні права. Закон України від 01.12.2022 № 2811-IX. URL: https://zakon.rada.gov.ua/laws/show/2811-20#Text

[3] Про електронні комунікації. Закон України від 16.12.2020 № 1089-IX. URL: https://zakon.rada.gov.ua/laws/show/1089-20#Tex

відсутність предметної цілісності відносин у Інтернет дає підстави для висновку про необґрунтованість визнання існування окремих категорій «Інтернет-право», «Інтернет-правовідносини», «Інтернет-відносини», а тим більше вести мову про «Інтернет-право» як про «змішаний» або «комплексний» інститут, галузь чи підгалузь права або законодавства.

Натомість, має йтися про виникнення у цій сфері регулятивних правовідносин різної галузевої приналежності: цивільно-правових, адміністративно-правових тощо. Що стосується понять «Інтернет-відносини», «Інтернет-правовідносини», «Інтернет-право», «ІТ-право» то вони, звісно, можуть використовуватися у юридичному побуті, але лише як правові концепти, тобто, як вербально виражені сукупності уявлень, понять, знань, асоціацій, емоцій, що виникають у зв'язку з використанням відповідних термінів, супроводжують і характеризують їх.[1]

У кожному разі, «Інтернет-відносини» (якщо вже з прагматичних міркувань для забезпечення стислості викладу використовувати такий термін для позначення сукупності відносин, що складаються в Інтернеті) є лише частиною більш загальної категорії «ІТ-відносини», під якими, у першому наближенні, можна розуміти усю сукупність суспільних відносин, що виникають у процесі (в результаті) створення і використання інформаційних технологій. Таким чином, «ІТ-відносини» є загальною категорією, що охоплює також і відносини, які складаються в Інтернеті.

При цьому «ІТ-відносини» включають також інші «інформаційні», «інформаційно-комунікаційні» відносини, але можуть не бути власне «інформаційними», у точному значенні цього слова, оскільки охоплюють широке коло різноманітних відносин, які регулюються нормами цивільного, господарського, адміністративного законодавства. Зокрема, до сфери цивільно-правового регулювання належать відносини надання послуг програмного забезпечення або його розробки; правового захисту web-сторінок і контенту; юридичної допомоги у відкритті ІТ-бізнесу; юридичного аудиту ІТ-компаній; юридичного обслуговування фрі-лансерів; оформлення та захисту авторських прав і торгової марки в Інтернеті; оформлення договорів купівлі-про-

[1] ІТ-право: поняття та сутність: монографія. За ред. О. І. Харитонової, Є. О. Харитонова. Одеса, 2017. С.10-27.

дажу сайту, домену, бренду тощо; правового забезпечення діяльності інтернет-магазинів; створення і реєстрації юридичних осіб у цій галузі; ліцензійних угод; захисту прав інтелектуальної власності; захисту інформації тощо.[1]

На такому підґрунті можемо визначити «Інтернет-відносини», як складову частину концепту «ІТ-відносини», сукупність суспільних відносин, що складаються у специфічному середовищі (Інтернет, Мережа, цифрове середовище), будучи одночасно «віртуальним феноменом» і проявляючись у бутті суспільства як реальні суспільні відносини. Завдяки останній особливості (своїй подвійній природі) вони можуть бути предметом правового регулювання і ставати правовідносинами.

Тут варто згадати досить поширену позицію, прихильники якої пропонують ігнорувати різницю між «Інтернет-відносинами» та «Інтернет-правовідносинами», аргументуючи виправданість такого підходу доцільністю віднесення «Інтернет-відносин» до нового типу суспільних відносин, які виникають, змінюються і припиняються у кіберпросторі. При цьому зазначається, що це не правові в чистому вигляді і не фактичні відносини, а спеціальні зв'язки особливої правової, інформаційної та технічної природи.[2]

Зазначене свідчить про важливість встановлення співвідношення категорій «ІТ-правовідносини» та «правовідносини», а також з'ясування особливостей правовідносин, що виникають у інформаційно-комунікаційній сфері.

«Інтернет-право», «Інтернет-відносини» та «Інтернет-правовідносини»

Розмаїття відносин, котрі складаються в Інтернеті, створює на практиці істотні незручності при пошуку актів законодавства, що

[1] Бачинський Т. Основи ІТ-права. Львів, 2016. 136 с.

[2] Литвинов Є. П. Правовідносини в інтернет-праві. *Часопис Київського університету права.* 2013. № 3. С.145-149; Єфремова К. В. До перспектив правового регулювання інтернет-правовідносин: господарсько-правовий аспект. *Право та інноваційне суспільство.* 2014. № 1. С.5-11; Барабаш О. О. Загальна характеристика інтернет-правовідносин. *ІТ-право: проблеми і перспективи розвитку в Україні*: збірник матеріалів науково-практичної конференції. Львів, 2016. С. 23-28.

стосуються різних видів таких відносин; пошуку та систематизації норм права, матеріалів практики; субсидіарному застосуванні норм законодавства, застосуванні аналогії закону тощо. Отже, маємо визначити орієнтири для встановлення кола правовідносин, котрі можна вважати органічно властивими Мережі.

Методологічною основою дослідження цього питання, на наш погляд, має бути розрізнення концепту «Інтернет-право» (який використовується тут нами з певними застереженнями, зробленими вище) у широкому та вузькому значенні.

Під «Інтернет-правом» у широкому значенні ми пропонуємо розуміти усю сукупність норм і правил, які стосуються інформаційно-комунікаційної активності в Інтернет. Його структура виглядає як достатньо інтегрована система багаторівневого порядку, що включає приватноправові та публічно-правові елементи. Необхідність врахування приватноправового та публічно-правового забарвлення ІТ-відносин має враховуватися, щоб визначити пріоритетність інтересів (приватні чи публічні), а відтак мати можливість встановити мотивацію застосування певних методів правого регулювання. Разом із тим, публічно-правові за своєю сутністю відносини, можуть складатися і в галузі цивільного права. До прикладу, такими є відносини цивільної відповідальності за шкоду, завдану цивільним правопорушенням у Інтернеті, наслідки чого визначаються безпосередньо нормами законодавства і не можуть бути змінені або припинені за домовленістю.

Натомість, під «Інтернет-правом» у вузькому значенні, на нашу думку, слід розуміти лише ті правові норми, що стосуються правомірної (у тому числі, «юридично-байдужої») діяльності у Мережі, передусім, регулятивні норми (переважно – цивільно-правові), що забезпечують функціонування «Інтернет-відносин».

Оскільки у публікаціях, присвячених питанням правового регулювання в Інтернеті зустрічається твердження, що правові норми, які регулюють діяльність у Мережі, мають змішаний приватно-публічний характер,[1] доцільно розглянути цю тезу з погляду коректності її застосування щодо «Інтернет-правовідносин».

[1] Енан Р. Є. Правове регулювання відносин у мережі Інтернет. ІТ-право: проблеми і перспективи розвитку в Україні: збірник матеріалів науково-практичної конференції. Львів, 2016. С.178.

Зауваживши методологічну хибність самого виразу «правові норми … мають змішаний приватно-публічний характер» (очевидно, усе ж таки, мається на увазі змішаний приватно-публічний характер актів законодавства), розглянемо, як поєднуються приватноправовий та публічно-правовий підходи при регулюванні «Інтернет-відносин».

Передусім, це має значення для встановлення первинності та вторинності таких категорій як «Інтернет-відносини» та «Інтернет-правовідносин».

У тому випадку, коли йдеться про правомірну діяльність приватних осіб (не держави та її фігурантів) в Інтернеті, суспільні відносини є первинними щодо правовідносин, оскільки можуть виникати на підставі угоди сторін, внаслідок фактичних дій суб'єктів тощо. На існування цих відносин не впливає наявність або відсутність актів законодавства, бо права та обов'язки сторін таких цивільних відносин мають основою норми природного права, що забезпечує їхнє включення у правову сферу. Отже «Інтернет-відносини» тут є первинними щодо «Інтернет-правовідносин», зумовлюючи характер і зміст останніх.

Однак, коли йдеться про суспільні відносини, пов'язані з публічними інтересами (наприклад, забезпечення інформаційної безпеки), відповідні «Інтернет-відносин» попадають у сферу дії публічного права. Оскільки публічне право є продовженням публічної влади і проявом останньої, то воно, як правило, виступає чинником встановлення не тільки правовідносин, але й самих публічних відносин, визначаючи, коли, чому і для чого вони формуються. При цьому відповідні «Інтернет-відносин» виникають та здійснюються у відповідності з приписами правової норми, і саме в цьому проявляється реалізація останньої, перетворення її у акт конкретної поведінки. Під таким кутом зору «Інтернет-правовідносини» можуть розглядатися як результат дії норми права, що за формою є індивідуально-визначеним зв'язком управоможених та зобов'язаних осіб, а за змістом – взаємодією цих осіб, які реалізують свої права та виконують обов'язки.

Таким чином, для визначення співвідношення категорій «Інтернет-відносин» та «Інтернет-правовідносин», зокрема встановлення їх первинності одне щодо одного, вирішальним критерієм є сфера права, до якої вони належать у конкретному випадку. Звідси випливає,

що відповідно до розмежування сфери приватного та публічного права слід розрізняти приватні та публічні «Інтернет-правовідносини».

Врахування приватних та публічних засад дає також можливість характеристики сутності правового регулювання «Інтернет-відносин».

Об'єктами регулятивних «Інтернет-правовідносин» є поведінка людей. а також конкретні блага, стосовно яких складаються відносини між людьми: 1) речі; 2) дії (послуги); 3) результат дій (результат робіт); 4) результати інтелектуальної, творчої діяльності та інші об'єкти права інтелектуальної власності; 5) інформація. При цьому види регулятивних «Інтернет-правовідносин», які виникають стосовно інформації, залежать від типу останньої. Так, фізичні та юридичні особи, які володіють інформацією професійного, ділового, виробничого, банківського, комерційного та іншого характеру, одержаною за власні кошти, або яка є предметом їх професійного, ділового, виробничого, банківського, комерційного та іншого інтересу, як правило, самостійно визначають режим доступу до неї, включаючи належність її до категорії конфіденційної, та встановлюють систему захисту. Тобто, тут мають місце регулятивні цивільні правовідносини, у яких права і обов'язки їх учасників щодо об'єкту (інформації) визначаються у диспозитивному порядку. Інші правила діють щодо інформації, яка відповідно до закону є державною, комерційною, службовою, професійною таємницею. Так, державна та службова таємниці взагалі вилучені з кола об'єктів цивільних відносин і регулюються нормами публічно-правового характеру, котрі найчастіше належать до сфери адміністративного права, завдяки чому тут виникають адміністративні правовідносини.

Як зазначалося, оскільки «регулювання» є концептом, що включає як публічні, так і приватні феномени, що забезпечують функціонування соціальних систем, впорядкування суспільних відносин може здійснюватися двома шляхами: 1) регулювання спеціальним суб'єктом; 2) саморегулювання. Якщо у першому випадку регулювання здійснюється спеціально уповноваженим суб'єктом (держава, органи місцевого самоврядування тощо), що має можливість владного впливу на поведінку інших осіб, то у другому – регулювання відносин учасників відносин здійснюється ними самотужки на основі домовленості.

Але через те, що регулятивні «Інтернет-відносин» можуть належати до сфери як приватного, так і публічного права, виникає необхідність розмежування регулятивних цивільних правовідносин та регулятивних адміністративно-правових відносин, з якими пов'язують виконання управлінських функцій.

Порівнюючи два згаданих види правовідносин, передусім, слід згадати таку названу вище рису, властиву публічним правовідносинам, як те, що вони є «первинними» стосовно суспільних відносин. Правовідносини у галузі публічного права взагалі, а отже і в галузі адміністративного права, виникають, змінюються та припиняються тільки на підставі правових норм, що містяться в актах законодавства, котрі безпосередньо породжують правовідносини і реалізуються через них. Між цими явищами (нормою, встановленою актом адміністративного законодавства, та адміністративно-правовими відносинами) існує причинний зв'язок. Що стосується сфери приватного права, то у ній суспільні відносини можуть опосередковуватися й іншими (не юридичними) нормами. Тому тут можлива ситуація, коли цивільні «Інтернет-відносин» сторін взагалі можуть не потребувати правового втручання.

Підсумовуючи викладене, можна зробити висновок, що правовідносини, які виникають в Інтернет, передусім мають бути розділені на: 1) відносини приватного та публічного права, 2) відносини регулятивні та охоронні.

При цьому визначальним є загальний поділ правовідносин на ті, що виникають у галузі приватного права, і ті, що виникають у галузі публічного права. У залежності від того, чи є відносини публічно-правовими чи приватноправовими, визначається їхній зв'язок з певною галуззю права, а відтак те, якими є їхні властивості. Крім того, беремо до уваги ту обставину, що «Інтернет-правовідносини» за своєю сутністю є регулятивними правовідносинами, властивими переважно цивільному праву.

Зазначені положення можуть слугувати підґрунтям аналізу сутності правовідносин у сфері Інтернет та їхнього співвідношення з концептами «ІТ-відносини», «ІТ-правовідносини» тощо, знімаючи, до речі, питання про доцільність згадуваної вище спроби характеристики відносин у цій сфері, як «не правових в чистому вигляді» і як «не суто фактичних» відносин.

Обмеження соціальних мереж в механізмі цивільно-правового регулювання

Завдання соціального регулювання вирішуються шляхом узгодження інтересів публічних (державних), колективних та приватних. У випадках неефективності соціального регулювання суперечності між цими інтересами можуть поглиблюватись (як це має місце у випадку колізій між правом громадян на інформацію та блокуванням державою шкідливих з погляду інформаційної безпеки сайтів, правами авторів та правами вільного доступу до інформації користувачів Інтернету тощо.

Прикладом такої ситуації можуть бути труднощі, що виникають у зв'язку зі спробами юридичного обмеження користування приватними особами тими чи іншими соціальними мережами, котрі під час гібридної інформаційної війни використовують сугестивні технології маніпулятивного впливу в Інтернеті.[1]

Зокрема, після повномасштабного вторгнення російських військ загострилась проблема використання соцмережі Telegram.

Її вирішення ускладнювалося тим, що певний час політика стосовно заборон чи блокування соціальних мереж виглядала досить непослідовною, у кожному разі, такою, що іноді визначалася, якщо й не меркантильними, то прагматичними міркуваннями.[2] (Власне, це є особливістю соцмереж (платформ), котрі як кожна зброя, може бути повернута у будь-який бік). Слід також зауважити популярність Telegram в Україні. За результатами опитування, проведеного 1-6 вересня 2024 року Київським міжнародним інститутом соціології, 54% українців вважають, що не варто повністю забороняти месенджер Telegram, а треба запровадити певні обмеження і контроль – блокування окремих каналів тощо./ Лише 9% українців стверджують, що

[1] Сугестивні технології маніпулятивного впливу: навчальний посібник. За заг.ред. Є. Д. Скулиша. 2-ге вид. Київ: СКІФ, 2023. С. 165-193.

[2] Telegram отримав список «проблемних» каналів від української влади – ЗМІ. Ростислав Вонс. 4 березня 2024. URL: https://glavcom.ua/techno/telecom/telegram-otrimav-spisok-problemnikh-kanaliv-vid-ukrajinskoji-vladi-zmi-989165.html; Івженко М. Які гроші обертаються в українському сегменті Telegram і чи можна його заблокувати - розбір NV. 30 квітня 2024. URL: https://biz.nv.ua/ukr/tech/blokuvannya-telegram-yak-pracyuye-biznes-kudi-ydut-groshi-chi-mozhna-blokuvati-chogo-ochikuvati-ukrajini-50414108.html?utm_medium=push&utm_source=gravitec

його треба повністю заборонити. Водночас 26% вважають, що його не варто жодним чином контролювати.[1]

При обговоренні цього питання на засіданні Ради національної безпеки і оборони України начальник ГУР МО України Кирило Буданов заявив, що у російських спецслужб є доступ до особистого листування користувачів Telegram, навіть видалених повідомлень, а також їх персональних даних. «Я завжди виступав і виступаю за свободу слова, але питання Telegram — це питання не свободи слова, це питання національної безпеки», — наголосив він.[2]

Проаналізувавши проблему, Національний координаційний центр кібербезпеки (НКЦК) 20 вересня 2024 року, прийняв рішення обмежити використання Telegram в органах державної влади, військових формуваннях, на об'єктах критичної інфраструктури. При цьому заборона використання Telegram в Україні не стосується особистих смартфонів, а поширюється лише на комп'ютери держслужбовців, військових та співробітників критичної інфраструктури.

Зауважимо, що наразі заходів кібербезпеки вживають і власники месенджерів. Зокрема, месенджер Telegram після затримання французькою поліцією його засновника Павла Дурова почав співпрацювати зі слідством. Щоб утримати зловмисників від зловживання пошуком Telegram, компанія оновила умови використання та політику конфіденційності застосунку. Про це повідомив сам Павло Дуров :«Ми чітко дали зрозуміти, що IP-адреси та номери телефонів тих, хто порушує наші правила, можуть бути розкриті відповідним органам влади у відповідь на законні запити»..

За останні кілька тижнів спеціальна команда модераторів, використовуючи штучний інтелект, зробила пошук Telegram набагато безпечнішим. За словами Дурова, весь проблемний контент, який було виявлено в пошуку, більше не доступний: «Ці заходи мають відлякати злочинців. Пошук в Telegram призначений для пошуку друзів і новин, а не для просування нелегальних товарів. Ми не дозволимо

[1] Соціологи запитали українців про заборону Telegram – результати відповідей. URL: https://gazeta.ua/articles/life/_sociologi-zapitali-ukrayinciv-pro-zaboronu-telegram-rezultati-vidpovidej/1192934?utm_source=gravitec&utm_medium=push&utm_campaign=

[2] В Україні обмежать використання Telegram у держорганах, серед військових та працівників критичних об'єктів — РНБО. 20 вересня. URL: https://nv.ua/ukr/ukraine/events/telegram-v-ukrajini-obmezhat-vikoristannya-u-derzhorganah-ta-viyskovih-formuvannya-novini-ukrajini-50452442.html

зловмисникам ставити під загрозу цілісність нашої платформи для майже мільярда користувачів».[1]

Разом із тим, навряд чи можна напевно стверджувати, що «Телеграм» став безпечним джерелом інформації та платформою для спілкування.

Висновки

За результатами дослідження можна зробити висновок, що механізм цивільно-правового регулювання ІТ-відносин (зокрема, відносин, що виникають у Мережі) під час гібридної війни має істотні особливості.

Наразі головною з них, на нашу думку, є те, що формування та прийняття актів цивільного законодавства в умовах гібридної війни, значною мірою втрачає свій приватноправовий характер особливостями відповідного елементу механізму цивільно-правового регулювання є положення, згідно якому природне право в умовах гібридної війни не є безперечним підґрунтям актів цивільного законодавства, якими регулюються інформаційно-комунікаційні відносини, і потребує видання нормативних актів «прагматичного» спрямування.

Водночас має враховуватись і та обставина, що саме по собі врегулювання актами законодавства таких відносин не забезпечить правопорядок у цій сфері, якщо не буде передбачений засіб, який забезпечуватиме перетворення норми права у правовідносини.

Насправді досягти «автоматичного» функціонування механізму, навряд чи, можливо, оскільки його елементи перебувають у «сплячому стані», доки не будуть активовані. Крім того, існує проблема тлумачення засад природного та позитивного права, поєднання цих засад. Покладення цих обов'язків лише на професійного суддю не завжди забезпечує виконання цих вимог, а відтак ефективне функціонування механізму правового регулювання.

[1] Telegram передаватиме правоохоронцям контактні дані зловмисників: деталі. Ростислав Вонс. 23.9.24. URL: https://glavcom.ua/techno/telecom/telegram-peredavatime-pravookhorontsjam-kontaktni-dani-zlovmisnikiv-detali-1022073.html?utm_source=gravitec&utm_medium=push&utm_campaign=

Тут може стати у нагоді досвід Стародавнього Риму, де в добу перетворення застарілого jus civile у нову систему норм здійснювалося шляхом надання претору (виборна посада) влади сприяти судовому захисту спірним майновим відносинам. При цьому право на позов претор виводив не з наявності правової норми, а зі свого розуміння aquitas.

Вирішуючи питання про спрямування чи не спрямування справи до суду, претор не був зв'язаний нормами jus civile і керувався тільки одним – пануючим у суспільстві уявленням про справедливість. Якщо нові суспільні відносини, на думку претора, підлягали судовому захисту, позов надавався, якщо ні – не було й позову. Такі повноваження надавали претору можливість фактично запроваджувати нові правові норми шляхом зміни системи позовів. У формулі, що видавалася судді, претор зазначав, за наявності яких обставин позов варто задовольнити, а за яких обставин – у задоволенні позову відмовити. Суддя, залежав від формули претора, і не міг від неї відступити. Отже, судова практика керувалася не нормами jus civile, а потребами цивільного обігу, які враховувалися у преторських едиктах.

Ключові слова: інформаційне суспільство, інформаційні технології, інформаційно-комунікативні відносини, Інтернет, Мережа, правовідносини, ІТ-право, суб'єкт цивільних прав, об'єкт цивільних прав, приватне право, публічне право, римське право.

Розділ 5

СИМУЛЯКР, ГІБРИДНА (ІНФОРМАЦІЙНА) ВІЙНА І ПОТЕНЦІАЛ ІТ

DOI

Євген Харитонов
доктор юридичних наук, професор,
член-кореспондент НАПрН України

Олена Харитонова
докторка юридичних наук, професорка,
членкиня-кореспондент НАПрН України

Симулякр «це зовсім не те, що приховує собою істину, –
це істина, яка приховує, що її немає. Симулякр і є істина»
Еклезіаст

Попередні зауваження

Одним з часто уживаних про дослідженні проблем інформаційної війни терміно-понять є «симулякр». Припустимість позначення цим терміном різних феноменів зумовлює необхідність невеличкого «теоретичного» вступу до викладу основного матеріалу.

Термін «симулякр» був упроваджений у науковий обіг П. Клоссовським у 40–60-х рр. XX ст. Починаючи з другої половини XX ст. цей термін знаходиться у центрі уваги філософів-постмодерністів і набуває дещо іншого значення. Якщо в класичній теорії репрезентації будь-який знак має необхідні елементи: позначаюче, означуване та референт, то в постмодерністській теорії зв'язок з референтом розривається. Розривається і прямий зв'язок між тим, що позначає, та означуваним. Позначаюче починає володарювати над означуваним. Тож симулякром постає усе те, що не має безпосереднього зв'язку з референтом, це є знак, який абсо-

лютно відірваний від реальності і не позначає того, що він мав би позначати.[1]

«Симулякр», як результат віртуалізації соціального буття людини, став одним з поширених концептів нашої доби, набувши особливої популярності після публікації у 1981 році праці Жана Бодріяра «Симулякр і симуляції» (Simulacres et Simulation),[2] де Бодріяр досліджує взаємозв'язки між реальністю, символами і суспільством, пов'язуючи саме явище симуляції з епохою постмодернізму, яка є епохою тотальної симуляції, коли реальність перетворюється на модель, а протиставлення між дійсністю і знаками зникає.

Таким чином, симулякри є сконструйованим звабливим символічним за своїм характером об'єктом, орієнтованим на задоволення бажань певного суб'єкта (суб'єктів). Це неправдива подібність, умовний знак чогось, що функціонує в суспільстві як його замінник. Як наслідок, сучасність є епохою загальної симуляції, яка створює гіперреальність і охоплює усі сфери життя особистості, котра звикла в епоху постмодернізму не відрізняти справжнє від вимислу.

Симуляція в інтерпретації Ж. Бодріяра означає набуття символами, знаками, образами самодостатньої реальності. На його думку, розвиток людської цивілізації сьогодні йде у напрямку затвердження світу симуляцій, котрі поширились практично на всі сфери суспільного життя. Незалежно від наших уподобань різноманітні симулякри стали частиною нашої дійсності.

Ось якими, на думку Жана Бодріяра, – «могли б бути послідовні фази образу: – він є відображенням глибокої реальності; – він маскує і спотворює глибоку реальність; – він маскує відсутність глибокої реальності; – він позбавлений зв'язку з будь-якою реальністю: він є чистим симулякром самого себе.

У першому випадку образ є *доброю* видимістю – репрезентація належить до порядку таїнства. У другому він є *поганою* видимістю – порядку псування. У третьому він *грає роль* видимості – і належить до порядку чаклунства. У четвертому випадку він належить аж ніяк не до порядку видимості, але до симуляції.

---

[1] Стебельська О. І. До питання про симулякризацію соціально-культурного простору. *Актуальні проблеми філософії та соціології.* 2022. С. 76. URL: https://doi.org/10.32782/apfs.v039.2022.12

[2] Бодріяр, Жан. Симулякри і симуляція. Пер. з фр. В. Ховхун. К.: Вид-во Соломії Павличко «Основи», 2004. 230 с.

Перехід від знаків, які щось приховують, до знаків, які приховують, що нічого немає, позначає рішучий поворот. Перші відсилають до теології істини і таємниці (до якої ще належить ідеологія). Другі відкривають еру симулякрів і симуляції, коли вже не існує Бога, аби розпізнати своїх, і Страшного суду, аби відділити хибне від істинного, реальне від його штучного воскресіння, бо все вже вмерло й воскресло завчасно.[1]

Як на нашу думку, названі Ж. Бодріяром фази образу тією чи іншою мірою відображені у розвитку образів, експлуатованих путінською російською пропагандою: від дійсної історії «завойовників зі Сходу» до привласнення історії Руси і створення симулякру «руського миру» з низкою супутніх симуляцій. При цьому найбільш активізуються і використовуються російські симуляції у ході гібридної війни проти України, котру росія веде протягом усього часу свого існування.

Симулякри у російській гібридній (інформаційній) війні проти України

Симулякри невід'ємно пов'язані з феноменом війни не лише тому, що збройним конфліктам передує інформаційна, психологічна тощо підготовка. І не тільки тому, що як перед початком збройного конфлікту, так і під час такого конфлікту кожна з його сторін прагне максимально гарно подати свої успіхи і так само – максимально – применшити досягнення суперника. Але навіть сама «конвенційна» війна є симулякром, створюючи ідеальну модель поведінки сторін збройного конфлікту, яку на практиці втілити неможливо.

У гібридній війні симулякри використовуються ще більшою мірою, оскільки тут вони можуть бути й основним засобом (інформаційна війна), і допоміжним (ідеологічна, психологічна, «збройна», економічна війни) засобом.

Сучасній гібридній війні властивий і у багатьох випадках стає у нагоді феномен віртуальної реальності, у площину якої в інформаційному суспільстві перенесена значна кількість соціальних процесів, зокрема конфліктів.

[1] Бодріяр, Жан. Симулякри і симуляція. Пер. з фр. В. Ховхун. К.: Вид-во Соломії Павличко «Основи», 2004. С. 12-13.

Важливу роль відіграє те, що тема симулякру стала дуже актуальною зі зростанням ролі мас медіа та Інтернету у формуванні громадської думки. Симулякри використовуються з метою маніпулювання соціумом, створення необхідного підґрунтя для різноманітних цілей. Дуже поширені вони у гібридній війни, слугуючи засобом маніпулювання свідомістю, створення необхідного інформаційного тла, далекого від реальності.

При цьому інформаційна війна може вестися окремо і незалежно від існування збройного конфлікту, маючи метою свідоме руйнування існуючого порядку, духовного світу і культури націй, проти яких застосовуються відповідні заходи. Разом із тим, інформаційні операції можуть бути також частиною моногібридної «мілітарної» війни, починатися задовго до воєнних дій і мати метою своєрідну підготовку до збройного конфлікту.

Методологічним підґрунтям сучасної інформаційної боротьби (війни) вважається згадувана теорія симулякрів Ж. Дельоза та Ж. Бодріяра, згідно з якою симулякри, щораз далі відриваючись від відтворення реального, зрештою стають повністю автономними, відірваними від реальності, яку вони спочатку репрезентували[1].

Народження симулякрів можливе при навмисному замовчуванні інформації, зміні хронологічного порядку подій, евфемістичному перифразі, навішуванні ярликів, які мають оцінне значення, маніпулюванні текстовим матеріалом, його урізанням або перестановкою окремих його частин та ін. Головний симулякр, який використовується росією на всьому пострадянському просторі, це «ідея єдності (братерства) народів на чолі зі старшим братом (росією)». Цей елемент формується завдяки насадженню викривленої історичної пам'яті – симулякру справжньої історичної пам'яті. Саме історична пам'ять є первинним плацдармом для початку агресії.[2].

Лише останнім часом почали з'являтися наукові розвідки проблем історичної пам'яті і ролі симулякрів у цьому процесі. Зазначається, що у країні немає загальносуспільної згоди щодо «чужого», антиукраїнського характеру імперської та комуністичної влади, нав'язаної

[1] Требін М. П., Чернишова Т. О. Теорія симулякрів та її реалізація в інформаційній війні. Науковий семінар ХНУ ПС ім. І. Кожедуба, 12 грудня 2019. С. 12.

[2] Дубяга А. Історична пам'ять як ключовий чинник гібридної війни в Україні. Історичні і політологічні дослідження. Спеціальний випуск: доповіді на Міжнародній науково-практичній конференції «Трансформації історичної пам'яті». Вінниця, 2018. С. 254.

ззовні. Тому відбувалися запеклі політичні дискусії щодо інтерпретації російсько-імперського і тоталітарного радянського минулого між носіями різних конфліктних моделей пам'яті – «радянської», «національно-патріотичної» та «ліберальної».

Антиукраїнські політики ділили країну масовими маніпуляціями історії, які десуверенізували свідомість, підважували основи державності. Криза ідентичності стала виявом стану невизначеності щодо усталеної загальноукраїнської системи суспільно-політичних цінностей, гострої конфронтації різновекторних політичних сил і, як наслідок, – неможливості визначення оптимального напряму розвитку суспільства. Проблема вироблення концепту історичної пам'яті та формування національної ідентичності ускладнювалася ще й тим, що в Україні тривав затяжний перехідний період, спостерігалися постійні коливання стосовно вибору напряму цивілізаційного розвитку і свого місця в міжнародному співтоваристві.

Загрозу українській державності та суспільству становить діяльність української православної церкви московського патріархату (УПЦ МП), яка фактично є філією російської православної церкви (РПЦ). Використання історико-релігійної тематики для утримання України в просторі російського впливу, нав'язливі заяви про «спільний цивілізаційний простір», «спільне історичне буття» і, врешті, твердження, що «ми – єдиний народ», а Україну нібито «вигадали в XIX ст.» – усе це складові реалізації антиукраїнських ідеологічних проектів російської влади.[1] Таким чином формується симулякр моделі історичної пам'яті, який має метою десуб'єктизацію України. Ситуація у цій галузі ускладнюється необхідністю розрізняти у проповідях священників і заявах ієрархів УПЦ МП гуманітарні мотиви і промосковську пропаганду,[2] і відповідно визначати можливі заходи правового впливу, застосовні у першому та другому випадках.

---

[1] Політика історичної пам'яті в контексті національної безпеки України: аналіт. Доповідь. За заг. ред. В. М. Яблонського. Київ: НІСД, 2019. С. 6-7.

[2] Опанасенко О. Митрополит ПЦУ заявив, що українська влада «вигадала» війну (відео). 9 серпня. URL: https://glavcom.ua/country/society/mitropolit-ptsu-zajaviv-shcho-ukrajinska-vlada-vihadala-vijnu-video-947853.html?utm_source=gravitec&utm_medium=push&utm_campaign=%D0%A2%D0%9E%D0%9F10.+%D0%A2%D0%B8%D0%B6%D0%B4%D0%B5%D0%BD%D1%8C&utm_gravitec=digest; Тараненко В. Хто працює під брендом «УПЦ»? Суд поставив крапки над «і». 7.11.23. URL: https://glavcom.ua/publications/khto-pratsjuje-pid-brendom-upts-sensatsijne-rishennja-sudu-966920.html?utm_source=gravitec&utm_medium=push&utm_campaign=

Путінська росія активно використовує політику пам'яті для легітимації своєї політики як на міжнародній арені, так і всередині країни. До реалізації політики пам'яті масштабно залучаються не тільки всі гілки російської влади, повний спектр засобів масової інформації, але й академічне середовище щодо аналітичних оглядів представників якого слушно зазначалося: «аналітика закінчується і лишається тільки політика».[1]

Завдяки зусиллям фахівців з інформаційної війни виникли такі симулякри як «бандерівець», «українські фашисти», «київська фашистська хунта», «український тероризм», «новоросія», «донецька народна республіка», «луганська народна республіка» тощо. Таким чином створюються симулякри терору, жахіття або катастроф, які лякають більше, ніж реальні вияви насилля чи стихійні лиха, що переживаються в реальності, при цьому знак «плюс», як правило, замінюється на знак «мінус». Одним з прикладів такого впливу на формування суспільної думки є, зокрема, фейкова оповідь про «розіп'ятого у Слов'янську на «глазах у матери» трирічного хлопчика», озвучена якоюсь жінкою, нібито «свідком» на першому каналі ТБ рф[2].

Для збільшення ефекту залякування також використовувались симулякри, які формувались протягом тривалого часу підготовчого етапу, зокрема, переляк перед всесвітньою змовою проти росії з боку Америки.

Власне й сама російська інтерпретація «гібридної війни» є симулякром, створеним з метою забезпечення протистояння «арабським веснам», загрозою яких страхав генерал Герасимов.[3]

З плином часу симулякри повністю замінили собою реальність у свідомості людей на тимчасово окупованих територіях Сходу України. Нова інформація сприймається крізь призму штучно створеної історії та колективної пам'яті, а правдива інформація та намагання спростувати «міфологічну» свідомість викликає когнітивний дисонанс і повністю заперечується. Виходячи з цього, фахівці припуска-

[1] Теміров Ю. Фактор «історичної пам'яті» у зовнішній політиці сучасної росії. *Історичні і політологічні дослідження.* Спеціальний випуск. С. 263.

[2] Ложь: распятие в эфире Первого канала. URL.: // http://www.stopfake.org/lozh-raspyatie-v-efire-pervogo-kanala/?PageSpeed=noscript

[3] Долженко О. О. Концептуальні засади та понятійно-категоріальне визначення «гібридної війни» в контексті загроз національній безпеці України. Гілея. 2018. Вип. 128. С. 315-317.

ють, що відновлення контролю Україною над інформаційним простором тимчасово окупованих територій окремих районів Донецької та Луганської областей уже не буде мати успіху та зможе вплинути лише на незначну частку населення.[1]

Дослідники виокремлюють наступні особливості використання симулякрів для формування необхідної свідомості людей у процесі інформаційної війни: а) застосування методу персоніфікації події; для цього подія висвітлюється в контексті долі окремої особистості (жінки, «яка втратила під час бомбардування єдину дитину», тощо); б) візуалізація інформації: якщо до 1990-х років у подачі інформації через ЗМІ переважав вербальний компонент, то поява супутникового телебачення, технологій створення віртуальної реальності відкрили нові можливості впливу на психіку людини за допомогою візуалізованих образів. Такий вплив спирається на чуттєво-емоційний досвід людини, якому вона довіряє більше, ніж словам; в) широке використання образів-метафор, як засобу перенесення сенсу з більш знайомого феномена на менш знайомий. До прикладу, якщо за допомогою програми Adobe Photoshop зобразити якогось відомого політичного лідера в одязі есесівця, що наступив чоботом на труп дитини, то у свідомості адресата виникає, як правило, негативне ставлення до цього політика; або створення образу ворога – «мерзенного Заходу» або «фашистської України» і «образу заступника народного» – в кабіні гелікоптера, на підводному човні, на полюванні, на рибалці, на лижах, в оточенні дітей, людей похилого віку, погорільців, військових, з потужним торсом, що грає м'язами, за кермом вітчизняного російського автомобіля, за штурвалом літака, дістаючи амфори з дна морського, що обдаровує, рятує, гнівається, жартує, вершить політику тощо; г) подача вербальної та візуальної інформації в контексті ціннісних орієнтацій більшості громадян цієї держави. У сучасних ЗМІ найуживанішими способами подання політичної інформації є такі фрейми, як «порушення прав людини», «захист прав національних меншин», «захист російськомовних», «національні інтереси», «тероризм», «екстремізм», «екологічна загроза» тощо; д) використання феномену «цапа-відбувайла», коли для каналізації негативної енергії людей, їхньої консолідації довкола вождя використовують образ

[1] Дубяга А. Роль симулякрів у гібридних конфліктах сучасності. *Література та культура Полісся*. 2020. № 99. Серія «Історичні науки» № 13. С. 83.

«ворога», який нібито й є відповідальним за біди, що звалилися на їхні голови. Як правило, у якості такого «цапа-відбувайла» обирають будь-який народ, політичну партію або її лідера, державу, релігійну групу тощо.[1]

«Вплив симулякрів активно використовується у сфері ЗМІ. Тут йде мова не так про суто фейкову інформацію, а про те, що ті новини, які нині транслюються в різних країнах світу, дуже часто спотворюють те, що насправді відбувається. Подається або ж часткова інформація, або ж дуже поверхнева, або ж досить однобічно інтерпретована.

ЗМІ Російської Федерації взагалі перекручують факти та подають неправдиві новини. Відповідно, людині, яка володіє досить низьким рівнем критичного мислення та не володіє достатнім рівнем пошукових навиків, надзвичайно складно розібратись в хаосі інформаційних новин та вибудувати адекватне бачення ситуації. Так само як слова/поняття втратили безпосередній зв'язок з референтами, так само і новини втратили зв'язок з реальністю. ЗМІ формує подекуди надзвичайно ілюзорний світ для глядачів/слухачів, які не маючи змоги проаналізувати дані, залишаються в його полоні.

Українські ЗМІ так само виконують подібну роботу, просто в іншому напрямку. В умовах військової агресії з боку Російської Федерації вони подають більш-менш адекватну інформацію, але багато жахів війни так само залишаються за кадром. На це є причини. По-перше, в умовах війни озвучення всієї правди може спричинити падіння духу населення. По-друге, доступ до новин мають і діти, а значить подана інформація не повинна травмувати їх психіки. І хоча такі міри державних ЗМІ є виправданими, тим не менше, багато людей просто не усвідомлюють, що насправді відбувається. Частина населення, сприймаючи картинку, яку подають ЗМІ, навіть близько не усвідомлює драматизму та жахів війни».[2]

Існує також безліч художніх симулякрів, метою яких є вплив на свідомість людини для стимуляції відповідної поглядам автора поведінки. Фахівцями робиться висновок, що в духовному житті сучасної людини та суспільства естетичний і художній компонен-

[1] Требін М. П., Чернишова Т. О. Теорія симулякрів та її реалізація в інформаційній війні. *Науковий семінар ХНУ ПС ім. І. Кожедуба*, 12 грудня 2019. С. 16-17.

[2] Стебельська О. І. Вказ. Праця. С. 67.

ти вже більше не мають родовидового підпорядкування, оскільки гармонія, вдосконалення смаків людини у «сфері чуттєвих явищ» більше не є обов'язковою вимогою з боку суспільства до художніх практик, зокрема сучасного мистецтва. І велику роль у цьому відіграли різноманітні симулякри, зокрема, із візуальною формою презентації.[1]

Переведення Масмедіа у віртуальну реальність стало новим засобом впливу на психіку людини за допомогою візуалізованих образів. Формуються і продовжують жити власним життям симулякри віртуально-онлайнової культури інформаційного суспільства. Ця проблема викликана тим, що особистість сьогодні формується у штучно створеному віртуальному світі, що спотворює особистість і формує її розірваний і нецілісний образ.

Проте не можна знімати відповідальність зі ЗМІ, які створюють певний образ подій і, бажаючи «захистити» населення від болючої правди, долучаються до його омасовленості та безвідповідальності. Таку симулякризацію ЗМІ свого часу відзначив і Ж. Бодрійяр, говорячи про війну в Перській Затоці.[2]

У редакційній політиці безлічі медіа, контрольованих кремлем, можна розгледіти єдину чітку стратегію маніпуляції, спрямовану на провокування соціокультурної невизначеності серед громадян України та нагнітання почуття страху, безладу та анархії в країні. Це досягається виконанням кількох смислових завдань.

По-перше, такі медіа системно гіперболізують масштаб і значення внутрішніх проблем України, применшуючи результати й значення загрози російської агресії, російського впливу за часи незалежності.

По-друге, штучно, маніпулятивно розширюються межі дискусії та контекст новин – до межі абсурду, за якою непрофесійний глядач втрачає будь-які раціональні орієнтири й авторитети.

По-третє, прокремлівська медіа-мережа маніпулює питаннями й героями поточного порядку денного. Теми, значущість яких не відповідає об'єктивній реальності й соціологічним даним, штучно ак-

---

[1] Поліщук О. П. Симулякр, естетичний досвід і художні практики сучасності в контексті принципу «неповного осягнення об'єкта». *Вісник Житомирського державного університету імені Івана Франка.* Філософські науки. 2019. № 1 (85). URL: (zu.edu.ua)

[2] Кириченко М. Концепція симулякрів віртуально-онлайнової культури інформаційного суспільства: концептуальні виміри постмодерністів. *Гуманітарний вісник Запорізької державної інженерної академії.* 2018. № 73. (vestnikzgia.com.ua)

туалізуються в ефірі. І навпаки. Найчастіше корупція важливіша за російську агресію.

По-четверте, реваншистська медіа-мережа штучно роздмухує теми, які поглиблюють суспільні розбіжності й радикалізують погляди громадян.[1]

У кожному разі, симулякри, які вони продукують, спрямовані на досягнення бажаного ними результату, який гарно охарактеризувала, досліджуючи етику симулякрів, О. І. Стебельська: «На політичному рівні етичні принципи теж розмились. Наш світ поділився на тих, хто на боці Добра, і тих, хто на боці Зла. Парадоксально, що цей поділ виявився досить відносним. Адже якщо аналізувати позицію агресорів, то вони щиро переконані, що це вони на боці Добра. Окрім того, свою позицію вони репрезентують, як таку, що прагне привнести мир та злагоду, що вони виступають проти брехливого уряду, проти проявів фашизму на нашій землі. Достатньо послухати виступ президента Росії під час оголошення часткової мобілізації. Перша думка, яка відвідала автора, що Зло ніколи не являє себе безпосередньо, воно прикривається лозунгами про мир, гуманність, наявну несправедливість, турботу про інших, необхідність надання захисту тощо. Зло виступає під личиною Добра».[2]

Декомунізація як десимулякризація

Революція Гідності і наступна російська агресія зумовили зростання національного патріотизму, що виявився в захисті власної землі від агресора, сплеску інтересу українців до науково обґрунтованої історії та прагненні позбутись комуністичного минулого. Сучасна політична еліта, яка прийшла до влади на революційній хвилі, значною мірою розуміє, що консолідація суспільства навколо єдиних цілей можлива лише за умови подолання дуалізму в оцінюванні історичних подій, а отже, створення нової моделі історичної пам'яті, яка сформує спільний історичний наратив народу.

[1] Політика історичної пам'яті в контексті національної безпеки України: аналіт. доповідь. За заг. ред. В. М. Яблонського. Київ: НІСД, 2019. 24-25.

[2] Стебельська О. І. Вказ. праця. С. 70.

Попри уявну спонтанність і еволюційність процесів формування історичних наративів, у сучасних умовах держава використовуючи засоби політики та управління, є впливовим суб'єктом формування національної пам'яті. Така сфера діяльності органів влади в політичному й науковому дискурсах отримала усталену назву «державна політика пам'яті», яка є сукупністю офіційних репрезентацій історичного минулого, комеморативних стратегій і практик (формату вшанування), орієнтованих на формування історичної пам'яті національної спільноти. В інституційному, тобто державному, вимірі політика пам'яті трансформується під впливом зміни ідеології, політичного режиму, а це впливає на вписування індивідуальної пам'яті в матрицю інституційну (державну).

Як зазначає А. Коник, «політика пам'яті» означає здійснення владною верхівкою чи домінуючою елітою контролю над конструюванням знань про минуле, який досягається через інтерпретацію історії, організацію масової історичної освіти (через держзамовлення на підручники, у яких викладено офіційний курс історії), організацію музейної й архівної бази, монументальну пропаганду, комеморативну практику, форми міфологізації (відзначення державних свят, символіка, меморіали), топоніміку (перейменування назв вулиць, населених пунктів), медіа тощо[1]. Очевидно, що всі ці практики активно застосовуються сьогодні в Україні. Особливу активну позицію у сфері історичної пам'яті й політики пам'яті в сучасній Україні відстоює Український інститут національної пам'яті (далі – УІНП) як центральний орган виконавчої влади, який реалізує державну політику у сфері відновлення та збереження національної пам'яті українського народу. Слід зазначити, що основними завданнями УІНП є подолання тоталітарного минулого (десовєтизація), відкриття й популяризація української історії, фіксація в національній пам'яті новітніх подій – Майдану та війни з росією.[2]

Разом із тим, констатуючи значення історичної пам'яті, як політичного феномену, дослідники практично залишають поза увагою симулякри, що були створені росією у галузі правознавства і досить успішно впроваджувалися у життя, як шляхом законодавства, так і

[1] Коник А. «Історична пам'ять» та «політика пам'яті» в епоху медіакультури. *Вісник Львівського університету.* 2009. Вип. 32. С. 158.

[2] Гурик М. І. Декомунізація як шлях побудови україноцентристської моделі історичної пам'яті. *Актуальні проблеми філософії та соціології.* 2016. Вип. 11. С. 27.

з використанням «м'якої сили» – правових концептів. Однак це тема окремого дослідження

Відтак, беручи до уваги активне та різноманітне використання симулякрів у гібридній війні та погоджуючись з думкою, що «саме історична пам'ять є первинним плацдармом для початку агресії»,[1] розглянемо далі деякі питання пошуку «асиметричної відповіді» на агресію російських симулякрів у найближчій нам галузі – цивілістиці.

Підбиваючи підсумки викладеному, зауважимо, що цифрові технології, в міру свого поступового вдосконалення і вплетіння в культурно-історичний контекст, все більшою мірою стають віртуальними, перестаючи відображати реальність і починаючи симулювати дійсність. Віртуальна реальність і симулякри не є нейтральними стосовно людини, вони змінюють психіку людей, дійсність навколо них, і, таким чином, отримують бажаний замовнику симулякру результат.

Симулякри та ІТ

Як зазначають дослідники, у сучасному світі найбільш помітним є створення і функціонування політичних симулякрів. Кількість таких симулякрів зростає в періоди політичних криз. Кризова ситуація в політичному житті багатьма дослідниками визначається як «інформаційна війна». Головним засобом маніпуляції свідомістю людей є новинний менеджмент, що включає управління інформаційними потоками за допомогою сучасних психологічних та медіа-технологій.

Переведення засобів масової інформації у віртуальну реальність стало новим засобом впливу на психіку людини за допомогою візуалізованих образів.

Формуються і продовжують жити власним життям симулякри віртуально-онлайнової культури інформаційного суспільства. Ця проблема викликана тим, що, як уже зазначалось, особистість сьогодні формується у штучно створеному віртуальному світі, що споворює особистість і формує її розірваний і нецілісний образ. Ігрова складова стала складовою домінантою сучасного віртуального віту,

[1] Дубяга А. Історична пам'ять як ключовий чинник гібридної війни в Україні. *Історичні і політологічні дослідження.* Спеціальний випуск: доповіді на Міжнародній науково-практичній конференції «Трансформації історичної пам'яті». Вінниця, 2018. С. 254.

а сама гра стала маркером постмодерністського суспільства, в центрі якого перфомативне, ігрове «Я»[1].

Україна, перебуваючи на передньому краї інформаційної війни, котру веде проти неї рф, зазнає на собі щораз потужніших нападів, програючи по декільком напрямкам. Яскравим прикладом застосування симулякрів для спроби зміни вектору цивілізаційного розвитку стала виборча кампанія 2019 року. Річ у тім, що серед великої кількості реальних і віртуальних криз існує криза розуміння суспільством влади. Конструкція політичного простору сучасності помітно відрізняється від попередніх століть, зокрема, тим, що на політичній арені кожної держави виокремились нові впливові політичні актори, елітарні страти «нового покоління», діяльність яких визначає провідні тенденції розвитку своїх країн.

На думку Р. Швиденка, стара модель працювала за принципом зривання масок. Її конструкція виглядала таким чином: влада складається зі своїх та чужих політичних сил, які перебувають у стані війни. Чужі скривають свої наміри під масками, вводячи своїх прибічників у оману. Свої, відповідно, таких масок не мають і їх словам і вчинкам можна вірити. Завданням є зривання масок з чужих і демонстрація суспільству їх реальних намірів.

Перший удар по цій моделі відбувся внаслідок відставки Ю. Тимошенко 2005 року. Другий – виходу Соцпартії з демократичного табору. Таким чином, маски виявилися у всіх.

Наразі маємо справу уже не з масками, а з симулякрами. Якщо маска створюється з метою скрити реальність, то симулякри для того, щоб замістити реальність, якої ніколи не існувало[2]. Найбільш під цю категорію підпадають популісти, які завойовують симпатії мас шляхом нереальних чи дешевих обіцянок.[3]

Найбільш помітною і гострою проблема симулякрів є у журналістиці і засобах масової інформації. Всесвітній індекс свободи преси у 2023 році демонструє дуже високу волатильність ситуацій, що

---

[1] Кириченко М. Концепція симулякрів віртуально-онлайнової культури інформаційного суспільства: концептуальні виміри постмодерністів. *Гуманітарний вісник Запорізької державної інженерної академії.* 2018. № 73. (vestnikzgia.com.ua)

[2] https://www.pravda.com.ua/rus/articles/2008/07/16/4445284/

[3] Герасіна Л. М. Модерні зміни чи симулякри в українській еліті за умов посилення соціальної нерівності? *Вісник Національного університету «Юридична академія України імені Ярослава Мудрого».* 2016. № 3 (30). С. 200. Gerasina_198-202.pdf (nlu.edu.ua)

складаються, зі значними підйомами та спадами, безпрецедентними змінами. Ця нестабільність є наслідком підвищеної в багатьох країнах агресивності влади та зростання кількості проявів ворожості до журналістів як у соціальних мережах, так і у реальному житті. Нестабільність також є наслідком зростання індустрії виробництва симулякрів, яка формує та поширює дезінформацію, а також надає інструменти її виробництва». У Індексі-2023 підкреслюється небезпека впливу індустрії фікцій у цифровій екосистемі на свободу преси. У 118 країнах – двох третинах країн, оцінюваних Індексом, – більшість респондентів, які заповнили анкети, повідомляють, що політичні діячі їхньої країни або регулярно, або систематично залучені до масштабних кампаній дезінформації чи пропаганди. Межі між істинним та хибним, реальним і штучним, фактом й артефактом стають настільки розмитими, що це ставить під загрозу саме право про інформацію. Безпрецедентні маніпулятивні можливості використовуються для ще більшого послаблення тих, хто уособлює собою якісну журналістику, одночасно з цим послаблюючи всю журналістику загалом.

Разюче швидкий розвиток генеративного штучного інтелекту струшує й без того тендітний світ ЗМІ, який уже був значною мірою підірваний Web 2.0...

Так, зокрема, П'ята версія штучного інтелекту Midjourney, яка генерує зображення дуже високої чіткості, наповнює соціальні мережі все більш правдоподібними підробками, які не відрізнити від реальності, про що свідчать напрочуд реалістичні фотографії жорсткого затримання Дональда Трампа чи портрет Джуліана Ассанжа, який перебуває у стані овоча, стягнутий гамівною сорочкою, які стали вірусними[1]. Зрозуміло, що це дуже вигідно недемократичним режимам, зокрема, рф, у її війні проти України.

Загрози, що виникають тут, можна проілюструвати за допомогою наступного прикладу. Українська студентка і блогерка Ольга Лоєк живе в Мюнхені й навчається в Університеті Пенсільванії. У 2023 році вона завела свій YouTube-канал, де розповідає про психічне здоров'я. За деякий час дівчина почала отримувати повідомлення від підписників про те, що її бачили у китайських соцмережах. І там вона зовсім не Ольга Лоєк, а росіянка, що розмовляє китайською. Її клон

[1] Всесвітній індекс свободи преси 2023 року: загроза індустрії симулякрів – Детектор медіа. (detector.media)

представляється Наташею чи Софією, Ейпріл чи Стейсі – залежно від соцмережі, де фігурує її обличчя.

Один з найбільших акаунтів «Імпортна їжа від Наташі» має понад три млн підписників. А господарка акаунту запевняє, що Росія – найкраща в світі країна, тож шкода, що інші держави відвертаються від неї. Вона стверджує, що російські жінки мріють приїхати до Китаю, після чого рекламує російські цукерки. Аватари, створені штучним інтелектом, які китайською мовою, розповідають про міцну дружбу між Пекіном і Москвою, а також рекламують російські товари.

«Я бачила своє зображення, яке вимовляє те, чого я ніколи не казала», – розповіла BBC 21-річна дівчина. Вона запевняє, що це неможливо, адже вона з України, з якою Росія веде повномасштабну війну з 2022 року: «Божевілля – використовувати українку для російської пропаганди …90% відео присвячені китайсько-російській дружбі й рекламі російської їжі. Це дуже образливо», – обурюється Ольга, сім'я якої мешкає в пошматованій російською війною Україні.

Але у ширшому сенсі її справа привертає увагу до ризиків технології, яка швидко розвивається і є справжньою проблемою. Ольга знайшла свої ШІ-клони на Xiaohongshu – китайській версії Instagram та на Bilibili – найбільшому китайському відеосайті, схожому на YouTube. «Їх [акаунтів] було дуже багато. Деякі з позначками російських прапорів»», – згадує дівчина. Наразі вона виявила близько 35 облікових записів зі своїм обличчям.

Клонів Ольги створили за допомогою сервісу HeyGen, що спеціалізується на реалістичних цифрових аватарах, генерації голосу та перекладах відео на різні мови.

Компанія відгукнулася на допис нареченого Ольги, який розповів її історію у соцмережі X. Вони з'ясували, що з обличчям українки створили понад 4900 відео і запевнили, що заблокували зловмисників. Представник HeyGen розповів BBC, що їхню систему зламали для створення «несанкціонованого контенту», але компанія негайно оновила безпекові протоколи, щоб запобігти подальшому зловживанню.

Анжела Чжан з Університету Гонконгу стверджує, що ситуація Ольги – дуже поширена в Китаї. І це попри те, що Китай є однією з перших країн, де запровадили правила щодо використання штучного інтелекту.

За офіційними даними, тільки у 2023 році місцева влада заарештувала 515 людей за фактом «підміни особи» на базі штучного інтелекту. Постає питання – як стільки відео з Ольгою потрапили в мережу? Можливо, причина криється в політиці – в просуванні дружби між Китаєм і Росією. В останні роки Пекін і Москва дуже зблизилися. А російський лідер Володимир Путін і президент Китаю Сі Цзіньпін заявляють, що дружба між їхніми державами «не має меж». Китай висвітлює війну в Україні через російські наративи, виправдовуючи їхнє вторгнення, а соцмережі цензурують обговорення війни.

«Навіть якщо такі акаунти не пов'язані з Комуністичною партією Китаю, просування через них пропагандистського контенту знижує ймовірність видалення», – каже Еммі Хайн, дослідниця права й технологій в Болонському університеті.

Справа Ольги Лоєк виходить далеко за межі Китаю і показує, як складно регулювати галузь, що розвивається з шаленою швидкістю.

Ольга Лоєк впевнена, що вона – не остання жертва ШІ, але не збирається йти з YouTube чи припиняти розміщувати матеріали. Вона виклала свою історію і каже, що деякі китайські користувачі допомагали їй виявляти підроблені зображення. За словами Ольги, після того, як вона та її підписники надіслали скарги до китайських соцмереж, близько десяти облікових записів, які імітували її, були видалені.»[1]

Підбиваючи підсумки, варто зазначити, що цифрові технології, в міру свого поступового вдосконалення і вплетіння в культурно-історичний контекст, все більшою мірою стають віртуальними, перестаючи відображати реальність і починаючи симулювати дійсність. Віртуальна реальність і симулякри не є нейтральними стосовно людини, вони змінюють психіку людей, дійсність навколо них, і, таким чином, отримують бажаний замовнику симулякра результат.

Інформаційна війна за участі ІТ – дія і протидія

Крім цього, в умовах інформаційної війни важливе значення має належним чином організована антипропаганда з використанням

[1] Як штучний інтелект перетворив українську блогерку на російську пропагандистку. Author,Фан Ван. Role,BBC News. 15 травня 2024. URL: Як штучний інтелект перетворив українську блогерку на російську пропагандистку – BBC News Україна

ІТ. При цьому має викриватися неправдива інформація з ворожої сторони і, натомість, подаватися власна інформація, яка відповідає дійсності. Так, зокрема, як відповідь на загрози в інформаційній сфері, було створено ІТ-армію. 6 лютого Міністерство цифрової трансформації запустило проєкт під назвою ІТ-армія або ж IT Army of Ukraine. Її основне завдання – боротися проти країни-агресора у цифровій площині. ІТ-армія України – це волонтерський рух. Сьогодні він об'єднує понад 310 000 українських та міжнародних ІТ-спеціалістів, кіберспеціалістів, працівників креативної індустрії тощо, які борються проти окупанта в онлайні. Долучитися до кібервійська може будь-хто. Для цього потрібно підписатися на Telegram-канал проекту IT Army of Ukraine, в якому публікуються актуальні задачі. Крім блокування російських ресурсів, до завдань ІТ-армії входить поширення серед населення країни-агресора правдивих відомостей про війну в Україні, та тиск на компанії, які не хочуть виводити свій бізнес з РФ. З останніх кейсів – німецька мережа супермаркетів METRO. Задача ІТ-армії полягала у тому, аби залишати на сторінці компанії у Facebook негативний відгук та коментар такого змісту: *Russia started war in Ukraine. Russia kills innocent people in Ukraine. You support Putin and Russian aggression. Still clear consciousness? #shameonmetro #StopFinancingRussia.* Після – переходити у Google Maps та обвалювати рейтинг сторінки METRO там[1].

Люди мають право на правду. За її відсутності довіра до влади безупинно знижується. Ми програємо, коли з запізненням даємо якісь факти, бо факти завжди входять в масову свідомість разом з інтерпретацією. А вже позбавитися цієї, навіть ворожої для нас інформації, важко, бо вона увійшла у свідомість першою. Щоб «перемогти» цю першою введену інформацію, треба докласти набагато більше зусиль. При цьому у одних випадках (як наприклад, з росією) існує агресивний конфлікт, а тому тут є специфічні завдання. В інших, просувати країну, її власну позицію треба в усьому світі. Одні завдання маємо в Європі, інші – в США. Та і в Європі розмова з країнами Балтії і Польщею буде різною. Це все принципово різні аудиторії. Так, навряд чи вірним було б стверджувати, що інформаційна війна ведеться Україною з Польщею. Скоріш за все, тут має

[1] Боротьба проти агресора на кіберфронті: як працює ІТ-армія та що їй вдалося досягти – AIN. UA

місце різна інтерпретація історії, де можна знайти порозуміння, і його рано чи пізно знайдуть. Крім того, у кожній країні є експертна спільнота, яка впливає на владу, та журналістська спільнота, що впливає на населення. І вони теж мають отримувати налаштовані саме на них повідомлення. Основне – це довіра до інформації. Тому йде пошук того, яким чином викликати довіру до власного повідомлення. Майбутня пропаганда стане набагато ефективнішою, бо вона буде базуватися на об'єктивному типі інструментарію. При цьому пропаганда ускладниться технологічно, а людина залишиться тою самою (фізіологічно, психологічно), якою була дві тисячі і більше років тому. Модерний інструментарій буде працювати проти незмінного мозку. Крім того, завдання ускладнюється тим, що, хоча проблема інформаційної безпеки існує для кожної країни (інформаційний простір багато в чому спільний, у ньому важко встановити кордони), але тут має місце асиметрія: ми дивимося американські серіали, читаємо американські книжки, а вони не дивляться наші фільми і не читають наших книжок. Отже свій продукт має стати найцікавішим для аудиторії, оскільки він відображає власну картину світу. Тому державі треба вкладати кошти у створення власних бестселерів і блокбастерів тощо.[1]

Важливим профілактичниим засобом боротьби з симулякрами є інформаційна гігієна.

Експерти зазначають, що безпечність українців в інформаційному просторі та відсутність гігієни в Мережі вбиває імунітет до кіберзагроз. На їхню думку, суспільство практично не захищене. Про безпеку люди думають дуже мало. Всі читають про кібератаки і хитрих хакерів, але водночас ставлять собі примітивні паролі просто через те, що їм так зручно, викладають про себе інформацію, яку стороннім знати не обов'язково. Низька культура безпеки є чинником більшості злочинів у Мережі: люди переходять за незнайомим посиланнями, ведуться на фейки і стають жертвами – втрачають свої гроші, дані, а їхні комп'ютери блокуються злочинцями. Збройне протистояння проти України розпочалась з інформаційної війни, яка триває паралельно бойовими діями. Серед методів, що застосовуються в інформаційній агресії, є наступні: дезінформування та маніпулювання;

[1] Георгій Почепцов. Інтерв'ю Марія Бойко, «Вголос». 9 березня 2017 р. URL: http://www.ji-magazine.lviv.ua/2017/Pocheptsov_Vijna_4_pokolinnya.htm

пропаганда; диверсифікація громадської думки; психологічний та психотропний тиск; поширення чуток.

В інформаційній війні з метою отримання переваги над супротивником часто користуються методом обману або введення об'єкта спрямувань в оману щодо справжності намірів, запрограмованих суб'єктом.[1]

Симулякри і право на інформацію

Оскільки протидія симулякрам у ході інформаційної війни припускає застосування певних обмежень та засобів державного примусу, неминуче виникає проблема колізії використання згаданих засобів здійснення та права на інформацію.

Особливо гостро постає ця проблема, коли йдеться про обмеження у сфері ІТ, котра вже за своєю сутністю є феноменом, що забезпечує вільний доступ до різноманітної інформації і, до того ж, має транскордонний характер. Не дивно тому, що після затвердження 15 травня 2017 р. Указом Президента України рішення РНБО від 28 квітня 2017 р., яким передбачалося блокування низки російських сайтів, активізувалося обговорення обґрунтованості такого обмеження, у тому числі, під кутом зору дотримання права на інформацію. Критики, вважаючи таке блокування неправомірним, доводять, що ним порушене їхнє право на інформацію, тоді як їхні опоненти наголошують на доцільності таких заходів у контексті загальної системи інформаційної безпеки.[2] Мало також місце оскарження Указу в суді, куди звернувся з позовом київський студент Нікіта Євстифєєв, який прохав визнати недійсними кілька пунктів рішення РНБО, які стосуються, зокрема, заборони сайтів групи Mail.Ru, соцмереж «Вконтакте» та «Одноклассники». Вищий адміністративний суд відмовився

[1] Фещенко І. В. Інформаційна війна як органічна складова сучасного збройно-політичного конфлікту. *Філософія та політологія в контексті сучасної культури.* 2021. Т. 13, № (1). С. 100.

[2] Барчук М. Мухи і котлети. URL:// http://viche.net.ua/index.php/blohy-2/item/post-5; Заборона російських соцмереж: не треба було просувати «русский мир». URL: https://blogs.online.ua/cibulko/post/736/zaborona-rosiyskih-sotsmerezh-ne-treba-bulo-prosuvati-russkiy-mir/; Запрет российских соцсетей в Украине: четыре аргумента «за». URL: https://blogs.online.ua/matjushin/post/739/zapret-rossiyskih-sotssetey-v-ukraine-chetyre-argumenta-za/

визнати неправомірним і скасувати заборону в Україні російських соціальних мереж. Після засідання Євстифєєв заявив, що «очікував будь-якого рішення і що для нього очевидним є, що обмежена свобода вираження поглядів та переконань.»[1] Менш з тим, це обмеження дало позитивні результати, санкції мали для російських компаній важкий економічний ефект і після введення заборон у першій десятці не залишилося жодного російського ресурсу[2].

Ситуація, яка склалася, зумовлює необхідність аналізу колізії, що склалася, з погляду реалізації права на інформацію із врахуванням вимог асекурації інформаційної небезпеки.

Передусім, зазначимо, що право на інформацію не лише проголошується Конституцією України, але й набуло практичного наповнення у Законі про інформацію, який, крім того, що встановлю таке право, ще й передбачає низку гарантій його здійснення.

Так, ст. 5 Закону про інформацію передбачає, що кожен має право на інформацію, що передбачає можливість вільного одержання, використання, поширення, зберігання та захисту інформації, необхідної для реалізації своїх прав, свобод і законних інтересів.

Разом із тим, ст. 2 цього Закону встановлює, що основними принципами інформаційних відносин є: гарантованість права на інформацію; відкритість, доступність інформації, свобода обміну інформацією; достовірність і повнота інформації; свобода вираження поглядів і переконань; правомірність одержання, використання, поширення, зберігання та захисту інформації.

Водночас, ст. 3 Закону про інформацію передбачає певні зобов'язання держави у цій галузі, визначаючи, що основними напрямами державної інформаційної політики є: забезпечення доступу кожного до інформації; забезпечення рівних можливостей щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації; створення умов для формування в Україні інформаційного суспільства тощо.

На додаток до цього ст. 7 Закону про інформацію «Охорона права на інформацію» передбачає низку гарантій такого права. Зокрема,

[1] http://news.liga.net/news/politics/14769093-sud_otkazalsya_priznat_nezakonnym_zapret_sotssetey_rf_v_ukraine.htm

[2] Казанський Д. Невіртуальний ефект. Російський Інтернет втратив близько 10 млн українських користувачів. І, здається, назавжди… *Український тиждень.* 2017. № 23 (499). С. 8-9.

встановлено, що право на інформацію охороняється законом. Держава гарантує всім суб'єктам інформаційних відносин рівні права і можливості доступу до інформації; ніхто не може обмежувати права особи у виборі форм і джерел одержання інформації, за винятком випадків, передбачених законом; суб'єкт інформаційних відносин може вимагати усунення будь-яких порушень його права на інформацію.[1]

Разом із тим, до основних напрямків державної інформаційної політики Закон про інформацію відносить забезпечення інформаційної безпеки України.

У свою чергу, вимогою до реалізації права на інформацію є те, що вона не повинна порушувати громадські, політичні, економічні, соціальні, духовні, екологічні та інші права, свободи і законні інтереси інших громадян, права та інтереси юридичних осіб.

Із врахуванням цих вимог право на інформацію може бути обмежене законом в інтересах національної безпеки, територіальної цілісності або громадського порядку, з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя.

Крім того, відповідно до ст. 28 Закону про інформацію неприпустимим є зловживання правом на інформацію[2]. Ця заборона має практичним результатом те, що інформація не може бути використана для закликів до повалення конституційного ладу, порушення територіальної цілісності України, пропаганди війни, насильства, жорстокості, розпалювання міжетнічної, расової, релігійної ворожнечі, вчинення терористичних актів, посягання на права і свободи людини.

Недотримання цієї вимоги має наслідком відмову у захисті права на інформацію, а у випадках, передбачених законом, тягне настання юридичної відповідальності.

Обмеження публічної інформації має місце під час війни. Тут важливо не допустити маніпуляцій стосовно того, яка інформація може бути обмежена. Є інформація, вільний обіг якої є важливим для де-

[1] Роз'яснення Міністерства Юстиції України від 3 травня 2012 р. «Право на доступ до інформації як елемент правового статусу особи». URL: https://zakon.rada.gov.ua/laws/show/n0012323-12#Text

[2] Закон України «Про інформацію». *Відомості Верховної Ради України*. 1992. № 48. Ст. 650. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text

мократичної держави. Вважається, що в усіх випадках і незалежно від обставин суспільний інтерес в поширенні такої інформації буде переважати шкоду від її оприлюднення. Відкритість цієї інформації прямо передбачається законами.

Передовсім, це інформація про розпорядження бюджетними коштами, державним і комунальним майном (що передбачено частиною п'ятою статті 6 Закону України «Про доступ до публічної інформації» (надалі – Закон № 2939-VI))[1]. Втім, не тільки: великий перелік безумовно відкритої інформації закріплений у частині четвертій Закону України «Про інформацію»[2], також понад десять галузевих законів забороняють обмежувати доступ до окремих категорій інформації.

Але частина п'ята статті 6 Закону № 2939-VI передбачає тільки 3 випадки, коли інформація про розпорядження бюджетними коштами може бути віднесена до таємної: 1)таємні видатки відповідно до статті 31 Бюджетного кодексу України[3]; 2) окрема інформація про закупівлі товарів, робіт і послуг становить державну таємницю відповідно до Закону України «Про державну таємницю»[4]; 3) випадки, передбачені частиною другою статті 23 Закону України «Про основи національного спротиву»[5].

Винятки з правила, що передбачає відкритість інформації про розпорядження бюджетними коштами, можуть бути встановлені тільки законами України, а не підзаконними актами [6]

На особливу увагу заслуговує поводження з інсайдерською інформацією під час війни. В Україні вперше поняття «інсайдерської інформації» набуло юридичної сили у Законі «Про цінні папери та фондовий ринок» від 23.02.06 р.: інсайдерська інформація – неоприлюднена інформація про емітента, його цінні папери та похідні (деривативи),

---

1 Закон України «Про доступ до публічної інформації» від 13.01.2011 № 2939-VI. *Відомості Верховної Ради України.* 2011. № 32. Ст. 314.

2 Закон України «Про інформацію». *Відомості Верховної Ради України.* 1992. № 48. Ст. 650. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text

3 Бюджетний кодекс України від 08.07.2010 № 2456-VI. *Відомості Верховної Ради України.* 2010. № 50-51. Ст. 572.

4 Закон України «Про державну таємницю». *Відомості Верховної Ради України.* 1994. № 16. Ст. 93. URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text

5 Закон України «Про основи національного спротиву» від 16.07.2021 № 1702-IX. *Відомості Верховної Ради.* 2021. № 41. Ст. 339.

6 Ващук-Огданська О. Обмеження доступу до публічної інформації під час війни: про що говорить судова практика? (частина 3. Що таке "безумовно відкрита інформація"?) URL: HTTPS://CEDEM.ORG.UA/ANALYTICS/BEZUMOVNO-VIDKRYTA-INFORMATSIYA/

що перебувають в обігу на фондовій біржі, або правочини щодо них, у разі якщо оприлюднення такої інформації може істотно вплинути на вартість цінних паперів та похідних (деривативів), та яка підлягає оприлюдненню відповідно до вимог, встановлених цим Законом. Інформація щодо оцінки вартості цінних паперів та/або фінансово-господарського стану емітента, якщо вона отримана виключно на основі оприлюдненої інформації або інформації з інших публічних джерел, не заборонених законодавством, не є інсайдерською інформацією. Інформація не вважається інсайдерською з моменту її оприлюднення відповідно до закону. Перелік відомостей, віднесених до інсайдерської інформації визначається Державною комісією з цінних паперів та фондового ринку. Основними ознаками інсайдерської інформації є істотність (комерційна цінність), непублічність, релевантність[1].

Стаття 232-1 КК України встановлює відповідальність за незаконне використання інсайдерської інформації, стаття 11-1 Закону України «Про ринок електричної енергії»[2] говорить про обмеження поводження з інсайдерською інформацією на ринку електричної енергії. Інсайдерська інформація має велике значення, яке зросло під час війни, а її неправомірне поширення може завдати шкоди також національним інтересам в цілому.

На користь національної інформаційної безпеки вирішується колізія, яку ми тут розглядаємо, і законодавством європейських демократичних держав. Зокрема, уряд ФРН, вважаючи, що соцмережі надто мало роблять для видалення забороненого контенту (Twitter видаляє лише 1 % такого контенту, Facebook – менше половини і тільки YouTube витирає 90 % заборонених матеріалів), 5 квітня 2017 р. схвалив законопроєкт, згідно якому соціальні мережі можуть каратися штрафами у розмірі до 50 млн євро за невиконання зобов'язань по видаленню забороненого контенту (коментарів, спрямованих на розпалювання ненависті тощо). Міністр юстиції ФРН підкреслив, що держава не може далі миритися з тим, що компанії в ФРН не дотримуються закону. І хоча критики (керівництво соцмереж, галузеві спілки та правозахисники) висловили побоювання, що соцмережі під

[1] Шевченко С., Жданова Ю., Складанний П., Бойко С. Інсайдери та інсайдерська інформація: суть, загрози, діяльність та правова відповідальністЬ. *Кібербезпека: освіта, наука, техніка.* 2022. № 3 (15). С. 178.

[2] Закон України Про ринок електричної енергії від 13.04.2017 р. – № 2019-VIII (редакція 03.09.2023 р.).

загрозою штрафів будуть видаляти надто багато матеріалів, що обмежить свободу слова в Інтернеті, законопроєкт був прийнятий. Втім, як годиться у демократичній державі, критика також була врахована: на відміну від первісного варіанту, одноразові порушення не будуть вважатися злочином, а тому штрафи за них накладатися не будуть.[1] Таким чином, від суворих санкцій не відмовились, але їхнє застосування співвіднесли зі ступенем зловмисності порушників. У підсумку маємо показове вирішення колізії між свободою слова (правом на інформацією) та інформаційною безпекою.

Таким чином, правове обмеження права на інформацію з міркувань інформаційної безпеки є досить поширеним явищем, котре відповідає загальним засадам реалізації прав особи і не порушує права людини. Не суперечить таке тлумачення і позиціям з відповідної категорії справ Європейського Суду з прав людини.[2]

Висновки

Підбиваючи підсумки викладеному вище, зауважимо, що цифрові технології, в міру свого поступового вдосконалення і вплетіння в культурно-історичний контекст, все більшою мірою стають віртуальними, перестаючи відображати реальність і починаючи симулювати дійсність. Віртуальна реальність і симулякри не є нейтральними стосовно людини, вони змінюють психіку людей, дійсність навколо них, і, таким чином, отримують бажаний замовнику симулякру результат.

Ключові слова: гібридна війна, інформаційна війна, інформація, інформаційні технології, цифрові технології, штучний інтелект, симулякри, фейк, віртуальна реальність, цінності, медіа.

[1] http://glavnoe.ua/news/n304235

[2] http://cedem.org.ua/analytics/pravo-na-dostup-do-informatsiyi-evolyutsiya-pidhodiv-yevropejskogo-sudu-z-prav-lyudyny/

Розділ 6

ІНФОРМАЦІЙНЕ СЕРЕДОВИЩЕ ЯК СТРАТЕГІЧНИЙ РЕСУРС У ГІБРИДНИХ КОНФЛІКТАХ

DOI

Оксана Калітенко
кандидатка юридичних наук, доцента

Гібридні конфлікти як багатовимірне явище сучасності стали результатом трансформації класичних форм воєнного протистояння та еволюції інструментів геополітичної боротьби. Ці конфлікти на сучасному етапі розвитку людства поєднують військові, політичні, економічні, інформаційні, цифрові та кібернетичні елементи, які взаємодіють у межах єдиної стратегії для досягнення складних і багаторівневих цілей. У цифрову епоху гібридні конфлікти набули нових форм, адже стрімкий розвиток інформаційних технологій, глобальна цифровізація, а також зростання ролі кіберпростору в житті кожної людини значно розширили арсенал інструментів, доступних їхнім учасникам. Ідея гібридних конфліктів, хоча й отримала широке визнання лише у XXI столітті, має глибокі історичні корені. Елементи гібридності можна виявити у багатьох конфліктах минулого, які поєднували використання військових і невійськових засобів впливу на населення задля досягнення стратегічних цілей. Наприклад, під час Холодної війни активно використовувалися «проксі-війни», дезінформація, пропаганда конкретних ідей, економічний тиск і дипломатичні маніпуляції. Однак лише у 2000-х роках, з розвитком та активним поширенням цифрових технологій, гібридні конфлікти почали сприйматися як цілісний феномен, що вимагає окремого наукового аналізу.

Перші більш-менш грунтовні дослідження концепції гібридних конфліктів з'явилися у відповідь на події, які продемонстрували на практиці ефективність поєднання різних засобів ведення війни. Зокрема, конфлікт у Грузії у 2008 році можливо став одним із перших

яскравих прикладів гібридної війни у сучасному розумінні цього терміну. У ньому військові дії були інтегровані з активними інформаційними кампаніями, дипломатичним тиском та кібероперацією. Подальший розвиток цієї концепції активно відбувався на тлі подій в Україні у 2014 році, коли гібридні засоби стали основою стратегії агресії росії проти суверенної держави.

Цифрова епоха суттєво трансформувала природу гібридних конфліктів, шляхом значного розширення спектру доступних інструментів і підвищення їх ефективності. Всесвітня цифровізація надала змогу швидко та масштабно впливати на суспільну свідомість, політичні процеси та економічну стабільність, навіть не вдаючись до прямого військового втручання. Основними факторами, що зумовили ці зміни, без сумніву, є розвиток інформаційних технологій, зростання ролі соціальних мереж, значення кіберпростору та активне впровадження технологій штучного інтелекту у всі сфери людського життя.

Стрімкий розвиток інформаційних технологій дозволив реалізувати стратегії асиметричного впливу, коли менш потужні держави або недержавні учасники отримали можливість досягати стратегічних переваг, використовуючи новітні цифрові інструменти. Це створило умови для зміщення акценту від класичних військових операцій до інформаційних і кібернетичних, в тому числі за участі ШІ.

В той же час соціальні мережі стали важливим, або, навіть, ключовим полем для ведення гібридних конфліктів. Завдяки їхній інтерактивності, миттєвості поширення інформації та широкому охопленню аудиторії, вони перетворилися на потужний інструмент для дезінформації, пропаганди та маніпуляції суспільною думкою. Використання алгоритмів соціальних платформ для таргетованого впливу, а також організація інформаційних кампаній через ботоферми створили нові можливості для здійснення інформаційного тиску.

В свою чергу кіберпростір став одним із найважливіших елементів гібридних конфліктів. Кібератаки частішають систематично і дозволяють завдавати значної шкоди економічним системам, критичній інфраструктурі та інформаційним ресурсам будь-якої держави. Завдяки використанню технологій штучного інтелекту та великих даних агресори отримують можливість не лише поширювати інформацію, а й прогнозувати реакції суспільства, адаптувати свої стратегії та підвищувати ефективність своїх дій.

Сучасні науковці останнім часом приділяють значну увагу дослідженню загальних характеристик та особливостей гібридних конфліктів. Так, наприклад Харитонов Є. О. та Харитонова О. І. в своїй роботі, що присвячується дослідженню людського виміру в гибрідній війні, визначають гібридну війну як зіткнення багатовекторних інтересів – політичних, правових, психологічних і гуманітарних – у межах сучасного конфлікту. Особливу увагу науковці приділяють людському виміру війни, тобто тій сфері, де інформаційні, правові та ментальні впливи перетинаються і формують правосвідомість, поведінку, реакцію на агресію, відчуття справедливості й правової захищеності. У тезах наголошено, що гібридна війна – це не лише збройна агресія, а й «вплив на людську свідомість, цінності та правові орієнтири через інструменти масової комунікації, маніпуляції, дезінформації». У цьому контексті інформаційне середовище функціонує як стратегічний інструмент формування сприйняття конфлікту і правової легітимності держави. «Гібридна війна – це не лише протистояння збройних підрозділів, а й конфлікт на рівні ментальності, права, моралі, історичної пам'яті та інституційної довіри. У центрі цього конфлікту – людина, її вибір, її ставлення до подій, її здатність протистояти маніпуляції».[1]

У публікації аналізується світоглядна вразливість особистості в умовах гібридної агресії, підкреслюється, що правові механізми не можуть бути ефективними, якщо не враховують фактори інформаційного впливу, особливо в межах окупованих територій або за умови систематичного інформаційного тиску на свідомість.

«Інформаційна атака, як складова гібридної війни, формує не лише уявлення про реальність, а й підміняє правові критерії її оцінки».

Цей підхід розширює межі традиційного розуміння гібридної війни, вводячи у фокус дослідження взаємозв'язок між правовою системою та інформаційною екосистемою, в якій функціонує людина як адресат і суб'єкт впливу.

Узденова Ю. М. в своєму дослідженні "Гібридна війна: сутність, складові та ключові поняття" доходить висновку, що гібридна вій-

[1] Харитонов Є. О., Харитонова О. І. Гібридна війна як зіткнення інтересів: людський вимір. *Одеські грудневі цивілістичні читання: приватне право як концепт в умовах війни*: матеріали наук. конф. (м. Одеса, 12 груд. 2024 р.). Одеса: Фенікс, 2025. С. 13.

на – це нова форма ведення війни, війна четвертого покоління, потужний монстр, діяльність якого спрямована на досягнення політичних цілей.[1] Тут же вона зазначає: “Неабияка участь під час ведення гібридної війни приділяється інформаційній сфері, адже саме вона має неабиякий вплив на формування стабільності, довіри до влади та формування та збереження і підтримку ідеології країни.” Однак при цьому залишає дослідження інформаційної складової завданням для своїх подальших досліджень.

Кундеус О. М. пропонує чітку дефініцію гібридної війни як поєднання прямих (збройних) та непрямих (кібернетичних, інформаційних, диверсійних тощо) операцій, спрямованих на підрив суверенітету України. Політична агресія реалізується не класичним військовим шляхом, а через «комплекс інструментів» гібридного впливу, що включає: приховані операції, диверсії, підтримку незаконних збройних формувань, інформаційну та кібернетичну стратегію. Автор відзначає, що основна загроза полягає у втраті або субстанційному обмеженні суверенітету України. «Інформаційний фронт “гібридної війни” розгортається… серед населення в зоні конфлікту… проти внутрішньої держави… серед громадян країни агресора та міжнародного співтовариства» – зазначає автор.[2]

В низці інших наукових досліджень також виділяються різні характерні ознаки гібридних війн і конфліктів, більшість з яких перекликаються та є співзвучними. Однак при цьому майже відсутні дослідження гібридних конфліктів з акцентом на цифрові реалії людського суспільства. Хоча саме цифрові технології сьогодення, на нашу думку, і надають особливої специфіки сучасним гібридним війнам.

Гібридні конфлікти в цифрову епоху сучасності характеризуються низкою специфічних рис, які відрізняють їх від традиційних форм протистояння. Перш за все, вони мають глобальний характер, адже цифрові інструменти дозволяють вести операції у глобальному (планетарному) масштабі, впливаючи на різні регіони світу одночасно.

---

[1] Узденова Ю. М. Гібридна війна: сутність, складові та ключові поняття. *Вчені записки ТНУ імені В. І. Вернадського.* Серія: Публічне управління та адміністрування. 2024. № 4. С. 178. URL: https://www.pubadm.vernadskyjournals.in.ua/journals/2024/4_2024/28.pdf?utm_source=chatgpt.com

[2] Кундеус О. М. Теоретичні аспекти гібридної війни РФ проти України. *Регіональні студії.* 2020. № 20. С. 120–124.

Крім того, такі конфлікти характеризуються високим рівнем інтеграції між різними засобами впливу, включаючи військові, політичні, інформаційні, економічні, та кібернетичні. При цьому не залишається осторонь і емоційна складова кожної людини та людства в цілому. Також варто зазначити, що внаслідок використання цифрових технологій сучасні гібридні конфлікти відрізняються також асиметричністю – потенційно менш потужні у військовому аспекті учасники конфлікту можуть досягати стратегічних цілей, використовуючи сучасні технології та інструменти.

Ще однією важливою особливістю гібридних конфліктів сучасності є, на нашу думку, розмитість меж між державними та недержавними суб'єктами таких протистоянь. У гібридних конфліктах сьогодні активно використовуються недержавні структури, такі як приватні компанії, хакерські угруповання, громадські організації, окремі фахівці, які діють у взаємозв'язку з офіційними державними структурами.

Нарешті, такі конфлікти часто мають прихований характер, коли операції проводяться так, щоб уникнути прямої відповідальності агресора за завдану людству шкоду.

Еволюція концепту гібридних конфліктів у цифрову епоху свідчить про те, що ці конфлікти стали більш складними, багатокомпонентними та ефективними. Інтеграція цифрових технологій, розвиток кіберпростору та значення інформаційного середовища зумовили появу нових форм протистояння, які значно розширили арсенал інструментів впливу обох сторін конфлікту на людські маси. У таких умовах для ефективної протидії гібридним загрозам необхідне використання міждисциплінарного підходу, розвиток інноваційних технологій і вдосконалення міжнародного співробітництва у сфері забезпечення інформаційної безпеки.

Описані вище складність і багатовимірність гібридних конфліктів у цифрову епоху підкреслюють зростаюче значення інформаційного середовища як ключового ресурсу сучасного протистояння. Його інтеграція в стратегії ведення конфліктів обумовлює не лише необхідність використання новітніх технологій, але й вимагає глибокого розуміння структури, функцій і впливу інформаційних потоків на глобальному та національному рівнях. Як наслідок, інформаційне середовище стає центральним елементом як у забезпеченні безпеки,

так і в реалізації агресивних стратегій, що відкриває нові горизонти для його дослідження.

Розглянемо основні етапи формування інформаційного середовища в Україні. Зрозуміло, що розвиток концепту інформаційного середовища в Україні відбувався у взаємозв'язку з трансформаціями політичної системи, безпековими викликами та правовим оформленням державної інформаційної політики. Формування теоретичних і практичних засад цього концепту супроводжувалося поступовим становленням відповідного законодавства, зростанням усвідомлення стратегічної ваги інформації як ресурсу впливу, а також еволюцією доктрини національної безпеки в умовах зростання всебічних загроз.

На початковому етапі самостійності і суверенності України (у 1990-х роках) інформаційне середовище не розглядалося як цілісний об'єкт правового регулювання чи як елемент системи національної безпеки. Першочергову увагу законодавець в ті часи приділяв проблемам свободи слова, доступу до інформації, діяльності засобів масової інформації, тощо. Так, Закони України «Про інформацію» (1992 р.), «Про друковані засоби масової інформації (пресу) в Україні» (1992 р.), «Про телебачення і радіомовлення» (1993 р.) та інші стали основою для поступового формування інформаційного простору як системи обміну повідомленнями у межах конституційно-правової моделі демократичного суспільства. Водночас, у ці ж роки в юридичній науці зароджувалося усвідомлення того, що інформація – це не лише об'єкт цивільного обігу чи засіб масової комунікації, а й потенційно вразливий стратегічний ресурс.[1] Саме на цьому ґрунті у 2000-х роках починає формуватись уявлення про інформаційне середовище як цілісну, багатофункціональну систему, яка включає в себе не лише ЗМІ, а й канали електронного зв'язку, мережеву інфраструктуру, суб'єктів генерування і споживання інформації, алгоритмічні механізми її поширення, а також правові механізми її контролю та захисту. Цей підхід було частково зафіксовано в редакції Закону України «Про інформацію» 2011 року, в якому було вперше чітко визначено поняття інформаційних ресурсів, інформаційної інфраструктури, носіїв інформації та прав на неї.

[1] Пожуєв В. І. Інформатизація як ресурс розвитку сучасного українського суспільства. *Гуманітарний вісник ЗДІА*. 2009. Вип. 38. С. 4-12; Марущак А. І. Інформаційні ресурси держави: зміст та проблема захисту. *Правова інформатика.* 2009. № 1(21).С. 65-71. URL: https://ippi.org.ua/sites/default/files/09maizpz_0.pdf та інші.

Важливим етапом у розвитку концепту інформаційного середовища стало прийняття у 2016 році Доктрини інформаційної безпеки України (Указ Президента № 47/2017)[1], яка вперше на рівні стратегічного правового документа закріпила ідею про інформаційне середовище як фактор, що прямо впливає на національну безпеку, громадську стабільність, суверенітет держави та інтеграцію в євроатлантичний простір. Доктрина констатувала, що одним із ключових викликів для України є інформаційна агресія з боку іноземних держав, насамперед Російської Федерації, яка активно використовує пропаганду, дезінформацію, інформаційно-психологічні операції та інші інструменти для дестабілізації суспільства та делегітимації влади.

У зв'язку з анексією Криму (2014 р.) та початком збройного конфлікту на Донбасі, інформаційне середовище починає розглядатися не лише як сфера комунікацій, а і як поле ведення війни – «інформаційний фронт». Це призвело до активного розвитку теоретичних уявлень про інформаційно-психологічні операції, інформаційний суверенітет, інформаційну гігієну.[2] На законодавчому рівні з'являються положення, що прямо спрямовані на обмеження шкідливого впливу інформації, зокрема щодо блокування іноземних пропагандистських ресурсів (рішення РНБО, введені в дію указами Президента), законодавчі ініціативи щодо боротьби з дезінформацією, посилення відповідальності за поширення неправдивої інформації в умовах воєнного стану.

У 2020-х роках під впливом загальносвітових трендів цифровізації та технологій штучного інтелекту, а також в умовах повномасштабного вторгнення РФ в Україну (з 24 лютого 2022 року), концепт інформаційного середовища набуває ще більшої стратегічної значущості. Тепер його розуміють як складний соціотехнічний конструкт, в якому поєднуються технологічна інфраструктура, контент, алгоритми його розповсюдження (включно з бот-мережами та автоматизованими системами), інституційна спроможність до реагування, рівень цифрової грамотності населення, тощо. У практичній площині це виражається

[1] Про доктрину інформаційної безпеки України. Указ Президента України № 47/2017. URL: https://zakon.rada.gov.ua/laws/show/514/2009#Text

[2] Довгань О. Д. Національний інформаційний суверенітет – об'єкт інформаційної безпеки. *Інформація і право.* 2014. № 3 (12); Дубов Д. В. Проблеми нормативно-правового забезпечення інформаційного суверенітету в Україні. *Вісник Національної Академії керівних кадрів культури і мистецтв.* 2014. № 1. С. 233-238. та інші.

в тому, що інформаційні кампанії стають невід'ємною частиною воєнної стратегії: від застосування платформ Telegram, TikTok і Twitter для оперативного інформування та мобілізації, до протидії російському інформаційному впливу через СБУ, Центр протидії дезінформації при РНБО, а також на рівні громадянського суспільства.

Водночас, триває процес кодифікації інформаційного законодавства України відповідно до стандартів ЄС. Так, у 2022-2023 роках ухвалено нову редакцію Закону України «Про медіа»[1], який адаптує українське законодавство до Директиви Європейського Союзу про аудіовізуальні медіапослуги. Закон також закладає основи для саморегуляції ринку медіа, захисту прав споживачів інформації, прозорості власності та розподілу відповідальності за дезінформацію. Таким чином, українська правова система поступово переходить від фрагментарного до системного правового регулювання інформаційного середовища.

Підсумовуючи, можна констатувати, що концепт інформаційного середовища в українському праві сформувався як відповідь на нові форми загроз – від політичної дестабілізації до кібервтручань і маніпуляцій суспільною свідомістю. На сучасному етапі українське правове поле перебуває у процесі активної трансформації, в якому інформаційне середовище визнається не лише об'єктом захисту, але й активним елементом національної стратегії протидії гібридним впливам. Інформаційне середовище в сучасних умовах стало одним із ключових елементів національної та міжнародної безпеки. Його значення виходить далеко за межі традиційного людського уявлення про медіа та комунікації, охоплюючи цифрові платформи, соціальні мережі, кіберпростір і технології штучного інтелекту. В епоху глобальної цифровізації інформаційне середовище набуло статусу стратегічного ресурсу, здатного не лише впливати на соціально-економічний і політичний розвиток держав, але й визначати основні напрямки та методику перебігу збройних конфліктів, переділу світу. На сьогодні можна із впевненістю заявити, що у сучасних конфліктах інформаційне середовище відіграє вирішальну роль, адже воно слугує платформою для формування суспільної думки, дестабілізації державних інституцій та координації військових і невійськових дій. Інформаційні кампанії, засновані на пропаганді та маніпуляції, здатні змінювати

[1] Про медіа: Закон України. URL: https://zakon.rada.gov.ua/laws/show/2849-20#Text

громадське сприйняття конфліктів, впливати на настрої населення та політичні рішення. Інформаційні атаки підривають довіру до органів влади, створюють соціальний хаос та провокують громадянські протистояння. У конфліктах сучасності інформаційні платформи використовуються для комунікації між учасниками бойових дій, передачі даних та організації інформаційних операцій. Як зазначалось вище, особливістю сучасних гібридних конфліктів є активне використання інформаційного середовища для досягнення стратегічних цілей. До основних викликів інформаційному середовищу в таких умовах належать: дезінформація та пропаганда, які включають поширення фейкових новин, маніпулятивних повідомлень та спотворення реальних фактів; кіберзагрози, що полягають у кібератаках на державні установи, інфраструктуру та медіа; маніпуляції через соціальні мережі, які дозволяють таргетовано впливати на різні групи населення, поширюючи контент, що сприяє загостренню конфліктів; а також руйнування інформаційної довіри, яке інтенсивно використовується для зниження довіри населення до офіційних джерел і породження інформаційного хаосу в суспільстві і державі.

Інформаційне середовище сьогодні є складною та багатокомпонентною системою, яка включає технологічні, соціальні, політичні, економічні та культурні аспекти. Його дослідження вимагає комплексного підходу, який враховує різноманіття чинників, що впливають на його функціонування та трансформацію. У цьому контексті міждисциплінарний підхід дослідження набуває особливого значення, адже він дозволяє інтегрувати знання з різних галузей науки для глибокого аналізу інформаційного середовища, його ролі в сучасних суспільних процесах та викликів, які воно створює. Міждисциплінарний підхід передбачає об'єднання методологій, концептів і практичних інструментів різних наукових дисциплін для дослідження складних проблем, які виходять за межі окремої наукової галузі. У випадку інформаційного середовища такий підхід є особливо важливим, адже це явище охоплює різні сфери: від технічних аспектів функціонування цифрових платформ до соціокультурного впливу інформаційних потоків на суспільство. Аналіз інформаційного середовища на основі міждисциплінарного підходу дозволяє створювати цілісну картину його розвитку, виявляти основні тенденції та прогнозувати потенційні наслідки змін. Для аналізу інформаційного середовища в сучас-

ному суспільстві використовуються різні ключові дисципліни. Так, наприклад, інформатика та технології забезпечують технічну основу для аналізу інформаційного середовища. Інформатика надає інструменти для вивчення великих даних, алгоритмів штучного інтелекту, функціонування цифрових платформ, соціальних мереж і кібербезпеки. Завдяки використанню сучасних технологій, таких як машинне навчання та блокчейн, можливе ефективне виявлення дезінформації, прогнозування поведінки користувачів і забезпечення захисту даних.

Соціологія та психологія допомагають зрозуміти, як інформаційне середовище впливає на суспільну свідомість і поведінку індивідів. Соціологічний аналіз дозволяє виявляти динаміку формування громадської думки, механізми соціальної поляризації та роль інформації у створенні соціальних груп і спільнот. Психологія досліджує когнітивні механізми сприйняття інформації, впливу пропаганди та маніпулятивних повідомлень на особистість.

Політологія та міжнародні відносини також є підґрунтям для досліджень. Політологія аналізує інформаційне середовище як інструмент політичного впливу, розглядаючи його роль у виборчих кампаніях, політичних кризах та гібридних конфліктах. Міжнародні відносини зосереджуються на транснаціональному вимірі інформаційної політики, зокрема, у контексті інформаційних воєн, дипломатії та формування міжнародного порядку.

Право і правова наука України відіграють фундаментальну роль у формуванні, функціонуванні та захисті інформаційного середовища як складової національного простору в умовах демократичного устрою, глобалізації та гібридної агресії. У межах сучасної правової доктрини інформаційне середовище дедалі частіше трактується не лише як інфраструктурно-комунікаційна система, а як складний соціально-правовий феномен, що охоплює сукупність відносин, пов'язаних із створенням, збиранням, передачею, обробкою, зберіганням, використанням і захистом інформації у цифрову епоху. Саме правовий вимір визначає межі допустимого, моделі поведінки суб'єктів, баланс між приватною автономією і публічними інтересами, а також механізми реагування на інформаційні загрози.

У національному правопорядку України, що активно еволюціонує під впливом євроінтеграційного курсу та потреб протидії зовнішнім загрозам, право виконує як регулятивну, так і стратегічну функції у

сфері інформаційної політики. Починаючи з основоположних актів, як-от Закони України «Про інформацію», «Про доступ до публічної інформації», «Про захист персональних даних», «Про медіа», правова система забезпечує нормативно-правове поле для реалізації інформаційних прав і свобод громадян, прозорості діяльності органів влади, відповідальності журналістики та платформ цифрової комунікації. Водночас, у період збройного конфлікту та гібридної агресії з боку Російської Федерації, пріоритетним стає захист національного інформаційного простору від зовнішнього втручання, кіберзагроз, деструктивних наративів та дезінформаційних кампаній.

Зміна безпекової парадигми після 2014 року, а особливо з початком повномасштабної війни у 2022 році, спричинила необхідність радикального переосмислення ролі права у сфері інформаційної безпеки. Правові механізми почали застосовуватись не лише з метою регулювання обігу інформації, а й як інструмент протидії гібридним впливам. Зокрема, запровадження індивідуальних та секторальних санкцій, блокування ворожих інформаційних ресурсів, криміналізація колабораціонізму у сфері мас-медіа та введення додаткових обмежень під час воєнного стану свідчать про перехід до концепції «активного права», зорієнтованого на захист суверенітету у сфері інформації. Законодавчі ініціативи щодо боротьби з дезінформацією, медіаграмотності, цифрової етики та кібергігієни підсилюють цю трансформацію. У свою чергу, правова наука в Україні виконує важливу функцію методологічного осмислення нових форм правовідносин у межах інформаційного середовища. Сучасні наукові дослідження концентруються на розробці дефініційного апарату, зокрема категорій «інформаційна безпека», «інформаційний суверенітет», «дезінформація», «інформаційний тероризм», «гібридна інформаційна агресія» тощо. Увага приділяється також аналізу національного законодавства в порівняльно-правовій перспективі, зокрема в контексті імплементації актів Європейського Союзу – таких як Директива про аудіовізуальні медіапослуги, Резолюція Європарламенту про боротьбу з дезінформацією, рекомендації Ради Європи щодо свободи вираження у цифрову епоху. Наукові розвідки правників також охоплюють проблематику юрисдикційного суверенітету в кіберпросторі, законодавчого регулювання функціонування соціальних мереж, алгоритмічного моделювання контенту та право-

вого статусу автоматизованих агентів комунікації (наприклад, ботів або систем штучного інтелекту).

У межах міждисциплінарного підходу, що поєднує цивільне, інформаційне, адміністративне, міжнародне публічне та кримінальне право, розробляються концепції змішаного регулювання інформаційного середовища. Правова наука в цьому аспекті не лише фіксує правові прогалини чи суперечності в чинному законодавстві, а й формує нові вектори його розвитку – від інституціоналізації незалежних регуляторів у сфері цифрових комунікацій до запровадження моделей спільного управління даними та етичних стандартів цифрової поведінки.

Відтак, право в Україні не лише забезпечує нормативну основу для функціонування інформаційного середовища, а й виконує роль активного чинника стратегічного реагування, що здатен протидіяти загрозам, трансформувати інститути публічного управління, сприяти демократичному розвитку, а також формувати національну ідентичність і стійкість у межах глобального цифрового простору. Правова наука, в цьому контексті, постає не лише як аналітична система, а як фактор формування правового дискурсу майбутнього, здатного адаптуватися до постійної зміни форм, каналів та технологій комунікації.

Культурологічний підхід дозволяє дослідити вплив інформаційного середовища на культурні цінності, традиції та національну ідентичність. Комунікаційні науки зосереджуються на вивченні процесів передачі інформації, механізмів медіа-ефектів, особливостей роботи традиційних і цифрових медіа.

Міждисциплінарний підхід базується також на інтеграції кількісних та якісних методів дослідження. Кількісні методи, такі як аналіз великих даних, соціометрія та статистичне моделювання, дозволяють виявляти масштабні тенденції, визначати закономірності функціонування інформаційного середовища та прогнозувати його розвиток. Якісні методи, включаючи інтерв'ю, контент-аналіз, дискурс-аналіз і кейс-стаді, забезпечують глибоке розуміння конкретних явищ, їхнього контексту та значення для окремих груп.

Особливу роль у міждисциплінарному аналізі відіграє системний підхід, який дозволяє розглядати інформаційне середовище як цілісну систему, що взаємодіє з іншими сферами суспільного життя.

Використання системного підходу сприяє розумінню взаємозв'язків між окремими елементами інформаційного середовища, такими як технології, суспільні інститути та індивідуальні суб'єкти.

Міждисциплінарний підхід до аналізу інформаційного середовища має низку переваг. По-перше, він дозволяє подолати обмеження окремих дисциплін і отримати більш повне уявлення про складні явища. По-друге, інтеграція знань з різних галузей сприяє розробці комплексних рішень для вирішення актуальних проблем, таких як інформаційна безпека чи протидія дезінформації. По-третє, міждисциплінарний підхід стимулює розвиток інноваційних методів дослідження, які поєднують технічні, соціальні та гуманітарні аспекти.

Сьогоднішня актуальність аналізу інформаційного середовища особливо виражена в умовах гібридної агресії, яку переживає Україна. З 2014 року країна стала об'єктом масштабних інформаційних атак, спрямованих на підрив її територіальної цілісності, економічної стабільності та міжнародного авторитету. В інформаційному середовищі України реалізуються масштабні дезінформаційні кампанії через медіа та соціальні платформи, здійснюються кібератаки на державні інформаційні системи та об'єкти критичної інфраструктури, а також поширюються ідеї, спрямовані на розпалювання гендерних, міжетнічних та політичних конфліктів. У таких умовах для України важливим завданням є розробка ефективних механізмів захисту інформаційного середовища, враховуючи як міжнародний досвід, так і особливості національного контексту та всі можливості сучасного цифрового світу.

У глобальному масштабі інформаційне середовище впливає не лише на локальні конфлікти, а й на міжнародну безпеку. Приклади кібератак, поширення дезінформації та використання інформаційних кампаній у міждержавних протистояннях демонструють важливість розробки міжнародно-правових механізмів протидії цим викликам. Дослідження інформаційного середовища у контексті гібридних конфліктів дозволяє розкрити сутність та динаміку впливу інформаційних загроз, запропонувати ефективні механізми захисту, сприяти зміцненню інформаційної стійкості держави та підвищенню рівня міжнародної безпеки. Таким чином, аналіз інформаційного середовища як стратегічного ресурсу стає невід'єм-

ною складовою сучасних наукових досліджень, що забезпечує не лише теоретичну, але й практичну цінність у протидії сучасним викликам.

Інформаційне середовище є одним із основних (а можливо вже і єдиним основним) елементів, що формує не тільки повсякденне життя сучасного суспільства, але й взаємодію між державами, політичними структурами та іншими соціальними інститутами. В умовах глобалізації та інтенсивного розвитку цифрових технологій інформаційне середовище стає не просто складовою комунікаційного процесу, а й глобальним ресурсом, здатним впливати на всі соціально-політичні процеси, економічні трансформації та національну безпеку. У контексті сучасних конфліктів, зокрема гібридних, інформаційне середовище відіграє ключову роль, визначаючи напрямки і способи ведення боротьби на інформаційних фронтах. Настали часи коли поняття інформаційного середовища охоплює не лише засоби масової інформації, але й численні новітні технології, які утворюють складну мережу взаємозв'язків і процесів, що формують загальну картину сучасного світу.

На сучасному етапі розвитку людства інформаційне середовище можна визначити також як сукупність всіх інформаційних потоків, що циркулюють у суспільстві, а також інститутів, організацій і технологій, які беруть участь у виробництві, передачі, обробці та сприйнятті інформації. Це середовище складається з різноманітних елементів, які взаємодіють між собою, створюючи динамічну систему, що постійно змінюється під впливом зовнішніх і внутрішніх факторів. Інформаційне середовище охоплює не лише традиційні форми комунікації, такі як телевізійні канали, газети, радіо, а й в першу чергу новітні форми цифрових медіа, соціальні мережі, онлайн-платформи, а також технології, що використовуються для збору та обробки даних, такі як великі дані (big data), штучний інтелект (ШІ) та інші інноваційні рішення.

Таким чином, інформаційне середовище можна визнавати і інтегрованою мережею, яка складається з різних компонентів, що взаємодіють між собою через безліч каналів і платформ. Це середовище впливає на способи комунікації, формує суспільну думку та змінює політичні, соціальні і економічні реалії на глобальному та національному рівнях.

При всій глобальності концепту інформаційне середовище можна умовно розподілити на кілька основних складових, кожна з яких має свої функції та специфіку взаємодії.

Комунікаційні канали – це основні канали, через які передається інформація. До них відносяться традиційні засоби масової інформації, такі як телебачення, радіо, газети, а також нові медіа – соціальні мережі, блоги, веб-сайти, відеохостинги, месенджери, платформи для обміну контентом та інші інтернет-ресурси. З розвитком цифрових технологій роль останніх у формуванні інформаційного середовища постійно і швидко зростає, оскільки вони забезпечують миттєву комунікацію між різними учасниками глобального процесу.

Інформаційні продукти – це конкретний зміст, який передається через комунікаційні канали. Вони можуть бути різного формату: текстовими, аудіовізуальними, графічними, інтерактивними тощо. Ці продукти створюються для того, щоб впливати на аудиторії різного масштабу: від локальних до глобальних. Вони можуть включати новини, статті, доповіді, дослідження, рекламу, соціальні кампанії, меми, що поширюються через цифрові платформи, а також пропагандистські та маніпулятивні матеріали.

Зазвичай суб'єктами, що створюють інформацію є державні органи, медіа-компанії, громадські організації, політичні партії, міжнародні організації, а також інші групи та індивіди, які активно формують та поширюють інформаційний контент. Вони відіграють важливу роль у визначенні інформаційних стратегій, контролюванні інформаційних потоків і маніпулюванні суспільною думкою. Вони є основними суб'єктами, які виробляють, обробляють та впливають на інформаційні потоки в суспільстві.

Сучасні новітні технології обробки та зберігання інформації включають в себе інструменти для збору, аналізу, зберігання та передавання великих обсягів даних. Сюди входять технології обробки великих даних, системи управління базами даних, платформи для штучного інтелекту, автоматизація контенту, аналіз соціальних мереж і навіть інструменти для боротьби з кіберзагрозами.

Слід звернути увагу на той факт, що у контексті гібридних конфліктів інформаційне середовище виконує не лише інструментальну, а й структуроутворюючу роль. Його функції виходять за межі простої трансляції повідомлень: вони впливають на стратегічне плану-

вання, юридичну легітимацію, моральний стан населення, політичну стабільність, а також на міжнародну реакцію. Проаналізувавши життя України і українців в умовах воєнного конфлікту з нападником, пропонуємо виділити наступні функції (місії) які виконує інформація щодня.

Когнітивно-психологічна функція – вплив на свідомість, емоції, поведінкові установки і реакції населення або військових підрозділів. Прикладом може бути масове поширення фейків про «здачу міст», «зраду командування», «втрати» з метою деморалізації цивільного населення і військових (РФ активно застосовувала це під час наступу на південь України у 2022 р.). Як свідчить практика, ця функція найбільш активно реалізується через Telegram, TikTok, Facebook і пов'язана з «вірусним» ефектом поширення.

Мобілізаційна функція – здатність інформаційного середовища консолідувати населення навколо певних цілей, цінностей або рішень. Без сумніву прикладом цієї функції є інформаційні кампанії на підтримку ЗСУ (#паляниця, #Байрактар, #єПідтримка, волонтерський рух) у 2022–2023 рр. Ця функція працює через емоційну ідентифікацію, формується наративами «ми» проти «ворога», виховує та актуалізує патріотизм, жертовність, соціальну згуртованість.

Дестабілізаційна функція (протилежність мобілізаційній) – використання інформації для послаблення довіри до влади, інституцій, економіки, судової системи, тощо. Яскравим прикладо є випадки поширення дезінформації про «втечу урядовців», «продаж територій», «інфляційний колапс», "єврейське заселення територій", тощо. Названа функція породжує стратегію дезорієнтації та деморалізації супротивника в мирний спосіб, підрив правової ідентичності.

Маніпуляційна функція – контроль над формулюванням понять, підміна причинно-наслідкових зв'язків, створення фальшивих альтернатив. На прикладі обставин життя сьогоднішніх українців вона проявляється у трактуванні окупації як «визволення», війни – як «спецоперації», геноциду – як «захист російськомовних», тощо. Як свідчить практика, маніпуляція здійснюється за рахунок підбору лексики, візуальних образів, музичного супроводу, «фактів» без джерел.

Юридично-легітимаційна функція – нформаційне середовище використовується для створення або імітації правової легітимності

(псевдореферендуми, «угоди», «звернення громадян»). Наприклад, інформаційний супровід фіктивних «референдумів» у Херсоні та на Донеччині у 2022 р. В ході реалізації цієї функції медіапростір створює ілюзію юридичної форми, що підкріплює політичні рішення агресора.

Міжнародно-репутаційна функція – це вплив на формування міжнародного образу держави – як жертви, як агресора або як союзника. Ця функція проявляється в діяльності Ukraine.ua, UNITED24, у вигляді звернення Президента до парламентів світу, у викритті злочинів (Буча, Ізюм) для міжнародного обурення. В цих випадках інформаційне середовище є полем дипломатичної конкуренції – чия правда буде сприйнята легітимною світовою спільнотою.

Інституційно-захисна функція – це інформаційна підтримка інституційного авторитету, правопорядку, судової системи, правоохоронних органів. Прикладами реалізації такої функції в Україні є сучасні кампанії проти корупції в обороні, інформування про судові рішення щодо воєнних злочинів, робота Центру стратегічних комунікацій, тощо. Таким чином інформація виконує роль посередника між державою і громадянином, формує довіру до легітимної влади.

Навігаційна (інформаційно-орієнтуюча) функція – це надання достовірної, оперативної, життєво важливої інформації – тривоги, евакуація, загрози. Прикладами реалізації цієї функції можуть бути застосунок «Повітряна тривога», телемарафон, офіційні Telegram-канали Міноборони, ДСНС, тощо. Для пересічних громадян, туристів, іноземців ця функція є ключовою в умовах воєнного стану. Саме вона допомагає населенню приймати правильні, швидкі та чіткі рішення в умовах небезпеки.

Розвідувально-аналітична функція проявляється у зборі відкритих даних для аналізу воєнної ситуації, позицій противника, громадських настроїв. Наприклад, OSINTгрупи (Bellingcat, InformNapalm), аналіз геолокацій з соцмереж, фото з TikTok/Telegram. Сьогодня вона використовується як державними структурами, так і волонтерами; дозволяє коригувати дії в реальному часі.

Рекрутингова та мобілізаційна функція агресора полягає у вербуванні через інформаційні кампанії, створення наративу участі у «святій справі», «боротьбі з фашизмом» тощо. Наприклад, використання TikTok у РФ для вербування молоді до ПВК «Вагнер», розміщення

роликів про «героїзм добровольців». Агресор щодо України активно використовує сучасні візуальні платформи для залучення «мобілізаційного ресурсу» через образи.

Інформаційне середовище в гібридних конфліктах виконує водночас інформаційні, правові, політичні, емоційно-психологічні та стратегічні функції. Його значення не обмежується медійною сферою – воно впливає на правовий статус територій, юридичну оцінку подій, міжнародну підтримку, здатність держави до самоорганізації. Саме тому в науковому дискурсі та правовому аналізі інформаційне середовище дедалі частіше розглядається як глобально-стратегічний ресурс, що визначає хід і наслідки гібридного конфлікту.

Окремо варто зробити акцент на тому, що інформаційне середовище цифрового світу є важливим інструментом збереження та передачі культурних цінностей. З допомогою сучасних інформаційних технологій здійснюється демонстрація та поширення культурних, наукових та освітніх матеріалів, що є основою для розвитку національних культур і взаємодії між культурами різних країн та різних людських формувань. І саме в цих напрямках проявляється культурологічна функція інформаційного середовища.

У сучасному цифровому середовищі користувачі не лише споживають інформацію, але й активно її створюють і поширюють. Це веде до зміни традиційної моделі «один до багатьох», замінюючи її на «багато до багатьох». І саме цей підхід відображає інтерактивність сучасного інформаційного середовища. Як зазначалось раніше, інформаційне середовище в сучасному світі вже давно не обмежується національними кордонами. Взаємодія між країнами та культурами через цифрові платформи стає безперешкодною, що збільшує можливості для транснаціональних інформаційних кампаній і глобальних інформаційних війн та свідчить про міжнародний, а більш правильно говорити сьогодні – планетарний, характер інформаційного середовища.

Окремо слід звернути увагу на зміну призначення інформаційних ресурсів в цифровому світі. Так, якщо раніше інформація в основному виконувала функцію повідомлення один одному про життєві обставини, то в сучасних умовах вона виконує скоріше функцію **боротьби за увагу і довіру людини** тим чи іншим конкретним інформаційним ресурсам.

Водночас із життєво важливими, позитивними та особливими моментами, інформаційне середовище несе в собі й значні ризики, про які останнім часом вголос сповіщають всі навколо. Такими ризиками є – кіберзагроза, зловживання даними, маніпуляція інформацією або навіть фальсифікація фактів, що призводить до серйозних наслідків для безпеки суспільства.

З огляду на значні ризики, які несе в собі інформаційне середовище, важливо зазначити, що ці загрози стають особливо критичними в умовах гібридних конфліктів. Саме в такому контексті інформаційне середовище перетворюється на поле битви, де використання інформаційних технологій, маніпуляція даними та цілеспрямований вплив на суспільну свідомість є інструментами інформаційної війни. Це підкреслює не лише потенціал інформаційного середовища, але й його вразливість, що робить інформаційне середовище полем інформаційної війни та ключовим елементом сучасних гібридних стратегій.

Інформаційна війна є невід'ємною складовою гібридних конфліктів, які в сучасних умовах набули глобального масштабу та багатовимірного характеру. Вона може визначатися як систематичний, цілеспрямований вплив на інформаційне середовище з метою досягнення політичних, економічних або військових цілей, часто навіть без застосування прямої військової сили. Її сутність полягає в маніпулюванні інформаційними потоками, створенні та поширенні певних наративів, дезінформації та пропагандистських матеріалів, які впливають на сприйняття реальності, поведінку та рішення суспільства. У рамках гібридних конфліктів інформаційна війна набуває особливого значення, адже її інструменти дозволяють ефективно досягати стратегічних цілей, мінімізуючи фізичні втрати, а також формувати умови для посилення інших компонентів конфлікту, таких як економічний тиск чи військові дії.

Як свідчить практика життя сучасної України, інформаційна війна виконує кілька ключових завдань у гібридних конфліктах. По-перше, вона спрямована на формування стратегічних наративів, які виправдовують дії сторони-агресора та дискредитують супротивника. Такі наративи створюються з урахуванням історичних, культурних чи ідеологічних контекстів, що дозволяє зробити їх максимально переконливими для певних аудиторій. По-друге, інформаційна війна

агресора спрямована на підрив довіри до сучасних державних інституцій. Це досягається шляхом поширення компрометуючих матеріалів, викривлення офіційної позиції уряду та створення ілюзії його неспроможності забезпечувати ефективне управління. По-третє, інформаційна війна використовується для деморалізації українців. Через масове поширення негативної інформації, візуалізацію жахів війни та маніпулятивні повідомлення створюється атмосфера безвиході та зневіри. Окрім цього, інформаційна війна сприяє загостренню внутрішніх конфліктів в українському суспільстві. Вона використовує наявні суперечності – політичні, етнічні, релігійні, психологічні – для посилення соціальної напруги, що ускладнює консолідацію суспільства перед зовнішніми викликами.

Методи та інструменти інформаційної війни надзвичайно різноманітні. Вона включає дезінформацію, пропаганду, кібератаки, маніпулювання засобами масової інформації та використання соціальних мереж з такою ж метою. Дезінформація як метод передбачає поширення неправдивих чи викривлених фактів, що вводять аудиторію в оману. Вона може бути спрямована як на дискредитацію супротивника, так і на створення помилкового позитивного іміджу агресора.

Пропаганда, в свою чергу, зосереджується на нав'язуванні ідеологічних установок, які виправдовують дії ініціатора конфлікту. В умовах сучасного цифрового світу соціальні мережі стали основним інструментом інформаційної війни. Завдяки їхній інтерактивності, широкому охопленню аудиторії та можливості таргетованого впливу соціальні платформи використовуються для розповсюдження фейкових новин, маніпулятивного контенту, організації інформаційних кампаній через ботів та тролів. Ще одним важливим методом інформаційної війни є кібератаки, які спрямовані на підрив інформаційної інфраструктури супротивника, викрадення конфіденційних даних, руйнування баз даних чи саботаж у критично важливих галузях, таких як енергетика чи транспорт. Сучасні технології, включаючи штучний інтелект, дозволяють автоматизувати процеси створення та поширення інформаційних продуктів, зокрема deepfake-відео чи фейкових новин, що ускладнює їх виявлення та нейтралізацію.

Наслідки будь-якої інформаційної війни є масштабними та довготривалими. По-перше, вона призводить до деградації або, як мінімум, суттєвої трансформації інформаційного середовища та людського

суспільства в цілому, створюючи атмосферу недовіри до будь-яких джерел інформації. Це **ускладнює формування об'єктивної картини реальності та сприяє розповсюдженню інформаційного хаосу.** По-друге, інформаційна війна спричиняє соціальну поляризацію, загострюючи внутрішні конфлікти у суспільстві. Це знижує рівень соціальної єдності та послаблює здатність держави до ефективної реакції на зовнішні загрози. По-третє, вона створює ризики для міжнародної стабільності, оскільки інформаційні кампанії можуть виходити за межі локального конфлікту та провокувати ескалацію напруженості на глобальному рівні.

В наявних обставинах російсько-українського воєнного конфлікту можна із впевненістю зробити висновок, що інформаційна війна в інформаційному середовищі є одним із найефективніших інструментів протистояння, який дозволяє сторонам досягати стратегічних цілей з мінімальними матеріальними витратами та фізичними втратами. Її багатофункціональність, інтеграція в цифрове середовище та використання сучасних технологій щодня роблять цей інструмент дедалі потужнішим та небезпечнішим. У контексті глобальних викликів, спричинених інформаційною війною, держави мають удосконалювати механізми її запобігання, розробляти новітні інструменти інформаційної безпеки та забезпечувати медіаграмотність населення. Лише комплексний підхід, що охоплює технічні, правові, освітні та організаційні заходи, може стати ефективною відповіддю на виклики, які створює війна в інформаційному середовищі.

Вразливість інформаційного середовища в умовах гібридних конфліктів обумовлена низкою причин, серед яких можна виділити як технічні, так і соціальні та правові аспекти. Так однією з головних проблем є юрисдикційні обмеження на конкретних територіях і в конкретних країнах. Інформаційне середовище є глобальним (загальнопланетарним) явищем, тоді як правове регулювання інформаційного середовища здебільшого обмежується національними рамками. Це ускладнює протидію транскордонним інформаційним атакам, зокрема тим, що здійснюються недержавними авторами, такими як хакерські групи або комерційні організації, які співпрацюють з державами-агресорами. У багатьох випадках відповідальні за деструктивні дії особи залишаються поза межами досяжності національної юрисдикції.

Міжнародне право відіграє важливу роль у регулюванні інформаційного середовища, особливо в умовах гібридних конфліктів. Зокрема, міжнародні конвенції, резолюції та договори встановлюють загальні принципи, які сприяють захисту інформаційного середовища. Наприклад, Європейська конвенція про права людини гарантує свободу вираження поглядів, але допускає її обмеження з метою захисту національної безпеки. Такі інструменти створюють рамкові умови для формування національних стратегій у сфері інформаційної безпеки.

Проте міжнародно-правове регулювання інформаційного середовища так само стикається з низкою проблем. Однією з них є відсутність чітких і універсальних норм, які б регламентували поведінку всіх, або хоча б більшості держав у кіберпросторі. Спроби розробити такі правила, зокрема в рамках ООН, часто наштовхуються на політичні суперечності між країнами. Водночас регіональні ініціативи, такі як діяльність Європейського Союзу у сфері боротьби з дезінформацією, є ефективнішими, але їхній вплив обмежується територіальними рамками.

На національному рівні відповідальність за інформаційні загрози може бути передбачена в адміністративній, кримінальній чи цивільно-правовій формах. Наприклад, законодавство України передбачає кримінальну відповідальність за кібератаки на державні інформаційні ресурси, що є важливим елементом забезпечення інформаційної безпеки. Однак проблема ефективності правозастосування таких законодавчих норм залишається актуальною, оскільки багато авторів діють не на території України, а у міжнародному просторі, знаходячись у постійному русі (IT-кочевники, хакери-мандрівники, тощо).

Без сумніву сьогодні інформаційне середовище відіграє ключову роль у забезпеченні національної стійкості України, особливо в умовах тривалої гібридної агресії, яка націлена на підрив її суверенітету, територіальної цілісності та політичної стабільності. У цій ситуації інформаційне середовище виконує подвійну функцію: з одного боку, воно є полем битви, на якому розгортаються інформаційні операції агресора, а з іншого – стратегічним ресурсом для мобілізації суспільства, захисту державних інтересів та забезпечення національної безпеки. Успіх України у протистоянні інформаційним загрозам значною мірою залежить від її здатності розвивати та адаптувати інформацій-

ну політику, законодавчу базу, залучати медіа та громадські ініціативи, а також формувати довгострокову стратегію побудови стійкого інформаційного простору.

Інформаційна політика України у період гібридної агресії зазнала значних трансформацій, спрямованих на зміцнення здатності держави протистояти інформаційним загрозам. Після початку агресії у 2014 році основним викликом стало реагування на масовані дезінформаційні кампанії, спрямовані на підрив довіри до державних інституцій, дестабілізацію громадської думки та міжнародну ізоляцію України. У відповідь були запроваджені заходи, спрямовані на моніторинг інформаційного середовища, боротьбу з фейковими новинами, блокування деструктивних медіаресурсів і підвищення прозорості діяльності державних органів. Уряд України ініціював створення системи стратегічних комунікацій, яка має забезпечити ефективну координацію інформаційної діяльності державних структур. Одночасно відбувалася активна співпраця з міжнародними партнерами для адаптації передового досвіду у сфері інформаційної безпеки.

Медіа та громадські ініціативи відіграють невід'ємну роль у зміцненні інформаційного середовища України. Незалежні засоби масової інформації стали важливим інструментом для протидії пропаганді та донесення правдивої інформації до української та міжнародної аудиторії. Вони забезпечують оперативне реагування на дезінформаційні атаки, підвищують обізнаність громадян про реальні події та сприяють формуванню критичного мислення. Громадські ініціативи, такі як фактчекінгові платформи, медіаосвітні проєкти та волонтерські рухи, значно посилюють здатність суспільства протидіяти інформаційним загрозам. Ці ініціативи сприяють поширенню культури інформаційної безпеки, формуванню стійкості до маніпулятивних наративів і залученню громадян до захисту національних інтересів в інформаційному просторі.

Перспективи розбудови національної інформаційної стійкості України тісно пов'язані з необхідністю подальшого розвитку стратегічних комунікацій, інноваційних технологій та партнерства між державою, бізнесом і громадянським суспільством. Україна має адаптувати свої стратегії до швидких змін у технологічному середовищі, зокрема використовувати штучний інтелект для моніторингу та аналізу інформаційних загроз, підвищувати рівень захищеності

цифрових платформ і розвивати національні медіа для популяризації української культури та ідентичності. Важливим є також впровадження комплексних програм медіаграмотності, які спрямовані на підвищення обізнаності громадян щодо інформаційних загроз та розвиток критичного мислення.

Таким чином, роль інформаційного середовища у забезпеченні стійкості України є визначальною у протистоянні гібридній агресії. Вона вимагає інтегрованого підходу, який включає ефективну інформаційну політику, вдосконалене законодавче регулювання, активну участь медіа та громадянського суспільства, а також впровадження довгострокових стратегій для формування захищеного та стійкого інформаційного простору. Тільки спільними зусиллями можна забезпечити належний рівень національної інформаційної безпеки та протидії сучасним викликам у цифрову епоху.

Інноваційні технології відіграють вирішальну роль у сучасних стратегіях протидії інформаційним загрозам, які є одним із ключових викликів цифрової епохи. Гібридні конфлікти та ескалація інформаційних атак вимагають застосування технологічно розвинених рішень, здатних ефективно моніторити інформаційне середовище, ідентифікувати джерела загроз, нейтралізувати їхній вплив та підвищувати стійкість суспільства до маніпулятивних наративів. Серед таких технологій особливу увагу заслуговують штучний інтелект, блокчейн, інструменти для підвищення медіаграмотності та кібербезпекові рішення. Їхнє застосування дозволяє значно підвищити ефективність стратегій захисту інформаційного простору та забезпечити комплексний підхід до вирішення проблем сучасних інформаційних загроз.

Штучний інтелект (ШІ) є одним із найпотужніших інструментів у протидії дезінформації та маніпуляціям. Його використання дозволяє автоматизувати процеси моніторингу інформаційних потоків, аналізувати великі масиви даних та ідентифікувати підозрілий або маніпулятивний контент. Завдяки алгоритмам машинного навчання ШІ здатен визначати фейкові новини, оцінювати їхній вплив на аудиторію та прогнозувати реакції суспільства. Наприклад, спеціалізовані алгоритми аналізують лінгвістичні особливості текстів, виявляють невідповідності або штучно створені елементи, а також ідентифікують мережі, задіяні у поширенні дезінформації. Водночас ШІ вико-

ристовується для розробки інформаційних платформ, які надають користувачам доступ до перевіреної інформації, забезпечуючи альтернативу маніпулятивним джерелам. Такі рішення не лише нейтралізують вплив дезінформації, але й сприяють формуванню довіри до офіційних джерел інформації.

Блокчейн та інші технології захисту даних відкривають нові можливості для забезпечення прозорості інформаційних потоків і гарантування автентичності джерел інформації. Використання блокчейну дозволяє створювати незмінні реєстри даних, які можуть використовуватися для підтвердження джерел походження контенту та ідентифікації тих, хто відповідальний за його створення. Це особливо актуально в умовах поширення фейкових новин та deepfake-матеріалів, які важко відрізнити від реальної інформації. Технології розподіленого реєстру також можуть бути використані для створення захищених платформ обміну інформацією, де неможливо змінити або видалити дані без відповідного підтвердження. Це підвищує довіру до інформаційних ресурсів і знижує ризик маніпуляцій.

Підвищення медіаграмотності населення є одним із найважливіших напрямів протидії інформаційним загрозам, і в цьому процесі інноваційні технології також відіграють ключову роль. Розробка інтерактивних платформ для навчання, мобільних додатків та симуляційних ігор дозволяє навчати громадян навичкам критичного мислення, розпізнавання фейкових новин та аналізу джерел інформації. Наприклад, освітні програми можуть використовувати віртуальну реальність або гейміфікацію, щоб моделювати ситуації, у яких користувачі стикаються з дезінформацією, та вчити їх правильно реагувати. Сучасні інноваційні технології також сприяють розвитку платформ для фактчекінгу, де користувачі можуть швидко перевіряти достовірність інформації за допомогою спеціалізованих інструментів і баз даних. Фактчекінг (англ. fact-checking) – це процес перевірки достовірності фактів, тверджень, повідомлень чи публікацій, що поширюються в медіа, соціальних мережах, публічному дискурсі або політичному житті. Його мета – встановлення істинності або хибності інформації на основі доступних об'єктивних джерел, офіційних документів, наукових даних або логічного аналізу. Фактчекінг сьогодні є одним з головних інструментів протидії дезінформації, маніпуляціям та фейковим новинам у публічному просторі.

Фактчекінг в сучасних обставинах є інструментом не лише журналістики або масової комунікації, але й важливим елементом забезпечення інформаційної безпеки держави. В умовах гібридної війни, інформаційної агресії та когнітивних операцій фактчекінг виконує функцію фільтрації та нейтралізації маніпулятивного впливу. У цьому сенсі, його варто розглядати як превентивний механізм у сфері захисту інформаційного суверенітету.

У правовому аспекті, фактчекінг не є чітко кодифікованою категорією в українському законодавстві, однак він тісно пов'язаний із такими поняттями, як: право громадян на достовірну інформацію (ст. 34 Конституції України); право на доступ до публічної інформації (Закон України «Про доступ до публічної інформації»); обов'язок ЗМІ надавати перевірену інформацію (Закон України «Про медіа»).

Основні етапи роботи фактчекінга можуть виглядати наступним чином.

1. Ідентифікація твердження, що перевіряється. Фактчекери відбирають суспільно важливі заяви, які викликають сумніви, є резонансними або потенційно маніпулятивними. Це можуть бути: політичні промови, пости в соціальних мережах, журналістські матеріали, відео/фото з сумнівним контекстом, тощо.

2. Контекстуалізація. Фактчекери визначають контекст заяви: коли, ким і з якою метою вона була зроблена, на який сегмент аудиторії спрямована, і які наслідки може мати її поширення.

3. Пошук джерел. Наступний етап – ретельна перевірка твердження через: офіційні бази даних (законодавство, судові реєстри, статистика); наукові джерела (академічні публікації, звіти, експертні дослідження); першоджерела (відео, протоколи, стенограми, прямі цитати); міжнародні бази даних (Eurostat, WHO, UN, NATO тощо).

4. Аналіз доказової бази. Фактчекером здійснюється критичний аналіз знайденої інформації, виявляються розбіжності, логічні невідповідності, відсутність доказів, маніпуляції емоційним тоном чи статистикою. Особливу увагу приділяють використанню вирваних з контексту фраз, модифікації зображень, використанню бот-мереж тощо.

5. Встановлення вердикту. Після завершення аналізу, автори фактчекінгу дають висновок про істинність/хибність заяви за шкалою: «Правда» / «Факт підтверджено»; «Маніпуляція»; «Неповна правда» / «Позбавлено контексту»; «Фейк» / «Брехня».

6. Публікація та поширення результату перевірки. Результати фактчекінгу оформлюються у вигляді доступного матеріалу (текст, інфографіка, відео) й публікуються на спеціалізованих платформах.

Результати фактчекінгу часто використовуються у журналістських розслідуваннях, які мають юридичні наслідки (викриття корупції, подання до суду, ініціювання перевірок), в судових процесах як докази маніпулятивності або недостовірності тверджень, як підстави для звернення до регуляторів (Національна рада з питань телебачення і радіомовлення, Кіберполіція, Центр стратегічних комунікацій при РНБО). Таким чином, фактчекінг сприяє реалізації механізмів юридичної відповідальності – зокрема, за поширення фейкових новин, наклеп, порушення етичних стандартів медіа, сприяння інформаційній агресії.

У межах сучасної правової науки в Україні та Європейському Союзі зростає тенденція до визнання фактчекінгу частиною правових стратегій протидії дезінформації, інтеграції інструментів перевірки фактів до систем саморегулювання медіа (media co-regulation), розробки етичних кодексів, які зобов'язують журналістів і публічних осіб перевіряти інформацію перед публікацією, підтримки незалежних фактчекінгових інституцій як елементів публічного контролю за правдою. У деяких юрисдикціях (наприклад, у Франції, Німеччині) результати фактчекінгу навіть впливають на алгоритмічні рішення цифрових платформ, зокрема – на модерацію контенту, маркування повідомлень, тимчасове блокування акаунтів.

Фактчекінг у структурі демократичної правової держави корелює з такими базовими принципами, як: доступ до правдивої інформації як умова реалізації основоположних прав і свобод; публічна відповідальність політиків і інституцій; розвиток критичного мислення як частини правової культури громадян. Відтак, функціонування незалежних фактчекінгових організацій є індикатором зрілості інформаційної демократії та складовою правової інфраструктури відкритого суспільства.

Таким чином, хоча фактчекінг на сучасному етапі і не кодифіковано як окремий правовий механізм, він фактично виконує функції, тотожні превентивним, контрольним і регулятивним інструментам права. У межах сучасної правової доктрини, фактчекінг доцільно трактувати як структурний компонент механізму інформаційної без-

пеки, що працює на перетині права, етики та публічного управління. Думається, що його подальша інституціоналізація, нормативне закріплення та інтеграція в національну систему правового захисту інформаційного простору мають стати одним з актуальних завдань сучасної правової науки.

Приклади інституцій, які сьогодні здійснюють фактчекінг в Україні StopFake.org[1] – один із перших проєктів в Україні, який з 2014 року фокусується на викритті російської дезінформації; Verify (Радіо Свобода) – мультимедійна платформа перевірки фактів, зокрема візуального контенту; Львівський медіафорум[2] -здійснює моніторинг регіональної преси на предмет фейків; Центр стратегічних комунікацій та інформаційної безпеки при МКІП[3] – виконує функції державного реагування на дезінформацію.

Фактчекінг сьогодні є не просто технологією перевірки повідомлень, а одним із механізмів інформаційної гігієни суспільства, важливою складовою цифрової освіти та компонентом правової культури. Він сприяє підвищенню медійної грамотності населення, зменшенню впливу інформаційних атак і маніпуляцій, підвищенню довіри до медіа, посиленню інституційної стійкості держави в умовах гібридної війни. Таким чином, фактчекінг в сучасних умовах це не лише інструмент журналістського контролю, а й соціально-правовий механізм демократичного захисту істини в інформаційному середовищі.

Кібербезпекові технології є невід'ємною складовою стратегій захисту інформаційного середовища. Інструменти кібербезпеки забезпечують захист критичної інформаційної інфраструктури, попередження кібератак і зниження ризиків витоку даних. Сучасні рішення включають системи виявлення та запобігання вторгненням, криптографічні технології, а також платформи моніторингу та аналізу кіберзагроз у реальному часі. Інтеграція таких рішень у державну та приватну інформаційну інфраструктуру дозволяє не лише захищати інформаційне середовище від атак, але й швидко реагувати на інциденти, мінімізуючи їхні наслідки. Особливо важливою є розробка технологій прогнозування загроз, які базуються на аналізі даних та використанні алгоритмів штучного інтелекту.

---

[1] Про діяльність організації дивись за посиланням https://www.stopfake.org/ru/o-nas/

[2] Про діяльність організації дивись за посиланням https://lvivmediaforum.com/

[3] Про діяльність організації дивись за посиланням https://spravdi.gov.ua/

Отже, інноваційні технології відкривають нові можливості для протидії інформаційним загрозам у сучасному світі. Вони дозволяють ефективно моніторити та аналізувати інформаційні потоки, забезпечувати захист даних, підвищувати рівень медіаграмотності населення та зміцнювати кібербезпекову інфраструктуру. Усе це сприяє формуванню стійкого інформаційного середовища, здатного протистояти сучасним викликам та забезпечувати національну і міжнародну інформаційну безпеку. Успішна інтеграція цих технологій потребує активної співпраці між державою, бізнесом і громадянським суспільством, що стане запорукою стійкості до інформаційних загроз у майбутньому.

У сучасному світі, коли гібридні конфлікти стали однією з головних загроз міжнародній безпеці, захист інформаційного середовища набув глобального значення. Країни та міжнародні організації розробляють стратегії, спрямовані на підвищення стійкості інформаційного простору, протидію дезінформації, забезпечення кібербезпеки та створення механізмів міжнародної співпраці. Досвід країн НАТО, Європейського Союзу та інших міжнародних організацій є цінним прикладом для адаптації в умовах гібридної агресії проти України. Цей підрозділ присвячений аналізу міжнародної практики у сфері інформаційної безпеки, ефективності міждержавної співпраці та можливостям використання цього досвіду для зміцнення інформаційного середовища України.

Практика країн НАТО у забезпеченні стійкості інформаційного простору базується на комплексному підході, який поєднує політичні, військові, технічні та інформаційні заходи. Одним із ключових елементів стратегії НАТО є розробка концепції стратегічних комунікацій (StratCom), яка спрямована на координацію інформаційної діяльності членів Альянсу для захисту їхніх національних інтересів і протидії ворожим інформаційним кампаніям. Створення Центру стратегічних комунікацій НАТО у Ризі стало важливим кроком у розвитку інституційної спроможності Альянсу у сфері інформаційної безпеки. Цей центр займається дослідженням методів дезінформації, розробкою інструментів для її виявлення та аналізу, а також навчанням експертів, які працюють у цій сфері. Важливим аспектом діяльності НАТО є акцент на підвищенні кібербезпеки, адже кіберпростір розглядається як окремий домен операцій, нарівні з сушею, морем, повітрям і

космосом. Альянс активно впроваджує технології для моніторингу кіберзагроз, розробляє стандарти для захисту критичної інфраструктури та організовує спільні навчання для підвищення готовності до кіберінцидентів.

Європейський підхід до протидії інформаційним загрозам базується на принципах демократії, прав людини та верховенства права. Європейський Союз активно працює над розробкою законодавчих ініціатив та інструментів для боротьби з дезінформацією і маніпуляціями в інформаційному середовищі. Однією з ключових ініціатив ЄС є створення Плану дій з боротьби проти дезінформації, який передбачає комплекс заходів для виявлення, аналізу та нейтралізації дезінформаційних кампаній. У цьому контексті важливу роль відіграє діяльність Спеціальної групи зі стратегічних комунікацій Східного партнерства (East StratCom Task Force), яка займається моніторингом інформаційного простору, аналізом фейкових новин та розробкою стратегій для їхнього спростування. Крім того, ЄС розвиває ініціативи у сфері медіаграмотності, спрямовані на підвищення обізнаності громадян щодо інформаційних загроз і розвиток їхніх навичок критичного мислення. Важливим напрямом є також співпраця між країнами-членами у сфері кібербезпеки, зокрема через Агентство Європейського Союзу з кібербезпеки (ENISA), яке надає технічну підтримку, проводить навчання та розробляє стандарти для забезпечення безпеки цифрового простору.

Механізми співпраці у сфері інформаційної безпеки на міжнародному рівні відіграють ключову роль у протидії глобальним викликам, пов'язаним із гібридними загрозами. Одним із найважливіших інструментів є спільні навчання та симуляції, які організовуються міжнародними організаціями, такими як НАТО, ЄС та ООН. Ці заходи дозволяють країнам обмінюватися досвідом, відпрацьовувати спільні дії у випадку кіберінцидентів та удосконалювати свої механізми реагування. Важливою є також міжнародна співпраця у сфері розробки стандартів кібербезпеки, які сприяють уніфікації підходів до захисту критичної інфраструктури та мінімізації ризиків у цифровому середовищі. Окремо слід відзначити роль міжнародних партнерств у сфері розслідування дезінформаційних кампаній, адже ці кампанії часто мають транснаціональний характер і вимагають координації зусиль між державами.

Адаптація міжнародного досвіду в умовах гібридної агресії проти України є важливим завданням, адже вона дозволяє використовувати найкращі практики для зміцнення національного інформаційного середовища. Україна активно співпрацює з міжнародними організаціями та країнами-партнерами у сфері інформаційної безпеки. Одним із прикладів такої співпраці є участь у спільних навчаннях НАТО, які спрямовані на підвищення готовності до кіберзагроз і розвитку стратегічних комунікацій. Крім того, Україна адаптує законодавчі ініціативи ЄС у сфері боротьби з дезінформацією та кібербезпекою, що дозволяє підвищити ефективність національної політики. Важливим аспектом є інтеграція європейського досвіду у програми медіаграмотності, які допомагають населенню краще розуміти природу інформаційних загроз і ефективно їм протидіяти. Усе це сприяє формуванню стійкого інформаційного середовища, яке є важливим елементом національної безпеки України.

Таким чином, міжнародний досвід захисту інформаційного середовища у гібридних конфліктах є надзвичайно цінним для зміцнення національної інформаційної безпеки. Практика НАТО, ЄС та інших міжнародних організацій демонструє ефективність комплексного підходу, який поєднує розробку стратегічних комунікацій, підвищення кібербезпеки, боротьбу з дезінформацією та розвиток медіаграмотності. Адаптація цього досвіду до українського контексту є ключовим кроком на шляху до забезпечення стійкості інформаційного простору та протидії сучасним гібридним загрозам.

Проведене дослідження дозволяє виокремити наступні характерні риси інформаційного середовища як стратегічного ресурсу в гібридних конфліктах:

Глобальний характер. Інформаційне середовище виходить за межі національних кордонів, забезпечуючи миттєву комунікацію між учасниками конфліктів у різних частинах світу. Ця особливість дозволяє агресорам поширювати вплив далеко за межі регіону конфлікту.

Швидкість поширення інформації. Інформація в цифрову епоху поширюється практично миттєво, що дозволяє оперативно впливати на громадську думку, змінювати наративи і створювати паніку чи дезінформацію.

Маніпулятивний потенціал. Інформаційне середовище дає змогу створювати та поширювати маніпулятивний контент, такий як фей-

кові новини, пропагандистські матеріали та дезінформаційні кампанії, які впливають на сприйняття реальності.

Доступність для різних суб'єктів (всіх). У гібридних конфліктах інформаційне середовище використовується як державними, так і недержавними акторами, включаючи терористичні угруповання, хакерів, громадські організації та окремих осіб.

Асиметричність впливу. Інформаційне середовище дозволяє менш потужним сторонам конфлікту завдавати суттєвої шкоди більш сильним суперникам, використовуючи інноваційні технології та низькозатратні методи інформаційного впливу.

Інтерактивність. Сучасні цифрові платформи, особливо соціальні мережі, забезпечують зворотний зв'язок між творцями інформаційного контенту та його споживачами, що дозволяє оперативно коригувати стратегії впливу.

Високий рівень уразливості. Відкритість інформаційного середовища робить його вразливим до кібератак, дезінформаційних кампаній і пропаганди, що може дестабілізувати суспільство та послабити державні інституції.

Поляризація суспільства. Інформаційне середовище здатне посилювати соціальні розколи, використовуючи чутливі теми для створення конфліктів між різними групами населення.

Інтеграція з іншими сферами. Інформаційне середовище тісно пов'язане з політичними, економічними, військовими та соціальними процесами, що робить його важливим елементом комплексного впливу у гібридних конфліктах.

Технологічна залежність. Сучасне інформаційне середовище базується на цифрових технологіях, таких як штучний інтелект, великі дані та алгоритми, що підвищує ефективність його використання, але водночас створює нові виклики для захисту.

Ці риси підкреслюють багатогранність і стратегічне значення інформаційного середовища в умовах гібридних конфліктів, що робить його не лише ресурсом впливу, але й важливим об'єктом захисту.

Ключові слова: інформація, інформаційне середовище, гібридні конфлікти, інформаційна безпека, міждисциплінарний підхід, функції. інформаційного середовища, цифровізація, фактчекінг.

Розділ 7

ПРАВОВІ РАМКИ ДЛЯ ЦИФРОВИХ АКТИВІВ: ПЕРСПЕКТИВИ ЦИФРОВОЇ ВЛАСНОСТІ

DOI

Катерина Некіт
докторка юридичних наук, професорка

Вступ

Наразі наше суспільство переходить до нової ери активної цифровізації всіх видів людської діяльності. Постійний розвиток інформаційних технологій призводить до появи нових цифрових об'єктів, які неминуче стають об'єктами правовідносин. Проте юридична природа таких об'єктів залишається дискусійною. Для опису таких об'єктів був розроблений новий термін «цифрові активи», який останнім часом все частіше використовується як усталене поняття. Незважаючи на те що цей термін все ще застосовується до досить широкого кола об'єктів, які інколи мають явно різну правову природу, є тенденція до визначення ознак цифрових об'єктів, які будуть охоплюватися цим поняттям, з метою забезпечення єдності в їх правовому регулюванні. Сюди входять ті цифрові об'єкти, які мають значну економічну цінність і специфічні характеристики, які дозволяють відрізнити їх від інших нематеріальних об'єктів, таких як інформація та інтелектуальна власність. Натомість особливості, притаманні цій категорії цифрових активів, наближають їх до об'єктів матеріального світу, що спонукає дослідників до активного обговорення можливості застосування до таких об'єктів положень про права власності.

Класичний підхід до власності, що склався протягом багатьох століть, передбачає визнання права власності лише на фізичні (матеріальні) об'єкти. Незважаючи на те, що положення про право власності в деяких країнах поступово поширювалися на деякі нематеріальні об'єкти, у більшості країн і в усталеній правовій доктрині зберігається сприйняття власності як права, що виникає щодо матеріальних об'єктів.

Проте в умовах інтенсивного розвитку інформаційних технологій змінюється розуміння «приналежності» власності людині та сутності об'єктів, що сприймаються людиною як «свої», оскільки незліченна кількість видів людської діяльності реалізується у віртуальній реальності, що призводить до поступового зникнення меж між реальним і віртуальним світами. При цьому вартість цифрових об'єктів постійно зростає, часом значно перевищуючи вартість аналогічних об'єктів у реальному світі.

Незважаючи на таку зростаючу цінність цифрових активів, права власників цифрових активів залишаються в основному незахищеними, оскільки досі незрозуміло, які правові положення слід застосовувати для забезпечення їх захисту. В останні десятиліття дослідники в цій галузі схиляються до визнання доцільності застосування положень про права власності для регулювання відносин щодо таких нових цифрових об'єктів, які мають економічну цінність[1]. Ця тенденція відзначається і на рівні останніх регулятивних розробок (soft law).

Тому в цьому розділі буде розглянуто потенціал змін у теорії власності та речовому праві під впливом розвитку інформаційних технологій і появи нового об'єкта цивільних відносин – цифрових активів. Метою цього розділу є визначення доцільності та необхідності запровадження нового виду власності (цифрової власності) з метою захисту прав на цифрові активи, що визначаються особливостями його об'єктів.

Що таке «цифрові активи» і які з них можуть бути об'єктами права власності?

Поняття «цифровий актив» наразі застосовується до дуже різноманітних цифрових об'єктів, таких як: облікові записи електронної пошти, облікові записи в соціальних мережах, підписки, облікові записи на торгових майданчиках, мобільні додатки, фотографії, книги, музика, відео, фінансові облікові записи, ігрові облікові записи, блоги та веб-сайти, файли або програми, що зберігаються на телефоні,

[1] Fairfield J, "Virtual Property" (2005) 85 B Univ L Rev 1047; Sheldon D, "Claiming ownership, but getting owned: contractual limitations on asserting property interests in virtual goods" (2007) 54 UCLA L Rev 751.

планшеті чи комп'ютері, переваги програм лояльності, доменні імена, віртуальні активи в грі тощо[1]. Деякі вчені зазначають, що термін цифрові активи слід розуміти як усі цифрові файли на комп'ютері людини, а також онлайн-акаунти та програми лояльності[2].

У повсякденному житті та в більшості наукових досліджень термін «цифрові активи» використовується в широкому сенсі, як загальний термін, який охоплює різні типи об'єктів з різними характеристиками та юридичною природою. Деякі експерти пропонують виділяти серед різноманіття цифрових активів ті, що мають сентиментальну (емоційну) та грошову (економічну) цінність[3]. Наприклад, цифрові фотографії, приватні відео, електронні листи, особисті блоги (які не приносять доходу) тощо можуть бути дуже цінними для тих, хто їх створює, але в більшості випадків не мають користі чи грошової цінності для будь-кого іншого. З іншого боку, криптовалюта, внутрішньоігрові предмети, кредити для онлайн-ігор, цифрові подарункові картки, бали лояльності, доменні імена, облікові записи в соціальних мережах і блоги, які мають значну кількість підписників, цифрові твори мистецтва тощо можуть мати значну грошову цінність[4].

Очевидно, що не всі згадані різноманітні цифрові активи можна кваліфікувати як об'єкти права власності. Зокрема, більшість цифрових об'єктів, які мають переважно сентиментальну цінність, найчастіше є об'єктами права інтелектуальної власності, оскільки фотографії, відео, аудіо, текстові матеріали та документи можна копіювати та відтворювати нескінченну кількість разів (виняток становить конвертація таких файлів у NFT). Тому доцільно було б розрізняти поняття цифрових активів у широкому та вузькому розумінні. У той час як цифрові активи в широкому сенсі можуть охоплювати різні цифрові об'єкти, які мають особисту, практичну або матеріальну цінність, поняття цифрових активів у вузькому значенні має стосуватися лише

---

1 Edwards L and Harbinja E, ''What Happens to My Facebook Profile When I Die?' : Legal Issues around Transmission of Digital Assets on Death' (*SSRN*, 21 February 2013) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2222163>accessed 10 May 2025.

2 Connor J, 'Digital Life after Death: The Issue of Planning for a Person's Digital Assets after Death' (2010) SSRN El J <http://dx.doi.org/10.2139/ssrn.1811044> accessed 7 May 2025.

3 'A helpful overview of all your digital property and digital assets' (*Everplans* 2023) <https://www.everplans.com/articles/a-helpful-overview-of-all-your-digital-property-and-digital-assets> accessed 7 May 2025.

4 Roche Legal, "How Valuable Are Your Digital Assets?" (*Roche Legal* April 10, 2023) <https://www.rochelegal.co.uk/news/how-valuable-are-your-digital-assets/> accessed May 7, 2025

тих активів, які мають реальну або потенційну економічну цінність. Останні є предметом дискусії щодо можливості визнання їх видом майна та поширення на них положень про право власності[1]. Таким чином, питання про те, які цифрові активи є потенційними об'єктами права власності, є дуже важливим.

Спроби визначити характеристики цифрових об'єктів, які можна визнати видом майна простежуються як у досить тривалих наукових дослідженнях, так і в останніх розробках законодавчих комісій і робочих груп з визначення принципів регулювання відносин з цифровими активами.

Так, у 2022 році Європейський інститут права опублікував звіт «Принципи Європейського інституту права щодо використання цифрових активів як цінних паперів». Незважаючи на те, що вони наголошують на своєму намірі не кваліфікувати права на цифрові активи як договірні, майнові чи sui generis, Європейський інститут права намагається визначити особливості цифрових активів, які дозволяють імплементувати їх у правове поле. Пропонується розрізняти три основні атрибути таких цифрових активів: 1) їх нематеріальний характер, який відображається в їх зберіганні, відображенні та/або адмініструванні лише в електронному вигляді, навіть якщо певний актив є матеріальним, реальним активом; 2) вони припускають наявність права контролю, отримання доходів чи користування, lato sensu – визначається як право на доступ і використання нетрадиційної форми цінності, втіленої в цифровому активі – що, у поєднанні з їхнім цифровим форматом, робить їхню передачу та подальше використання технічно можливим і комерційно бажаним; 3) можливість передачі від однієї особи до іншої[2].

Правова комісія Великобританії також опублікувала консультаційний документ щодо цифрових активів у 2022 році. У документі чітко сформульований намір розглядати цифрові активи як різновид власності. Цифрові активи названі «третьою категорією особистої власності», також визначено критерії, які дозволяють розглядати об'єкт як такий вид власності. Відповідно до висновків Правової ко-

[1] Nekit K. "Legal nature and types of digital assets in the activities of technology-oriented startups" (2023) 13(2) Trib Jur 304.

[2] 'Eli Principles on the Use of Digital Assets as Security' (*European Law Institute* 2022) <https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Principles_on_the_Use_of_Digital_Assets_as_Security.pdf> accessed May 7, 2025.

місії Великобританії, щоб підпадати під третю категорію особистої власності, об'єкт повинен: 1) складатися з даних, представлених на електронному носії, у тому числі у формі комп'ютерного коду, електронних, цифрових або аналогових сигналів; 2) існувати незалежно від осіб і правової системи; 3) бути конкурентоздатним (rivalrous) – це означає, що використання об'єкту однією особою унеможливлює його одночасне використання іншою[1].

На початку 2023 року з'явився ще один проект рекомендацій щодо правового регулювання відносин щодо цифрових активів: Проект Принципів УНІДРУА щодо цифрових активів і приватного права. Розробники Принципів УНІДРУА зазначають, що переслідують мету визначення підходів до правового регулювання особливої категорії цифрових активів, а саме цифрових активів, які часто використовуються в торгівлі та можуть підлягати контролю. Так само, як і Принципи Європейського інституту права, Принципи УНІДРУА підкреслюють, що їх розробники не переслідують мету чіткого визначення цифрових активів як майна, залишаючи це питання на розсуд держав. Однак у Принципах визнається, що цифрові активи можуть бути об'єктом права власності, що може означати в певних юрисдикціях, що цифрові активи мають класифікуватися як «майно», «товар», «річ» або подібне поняття[2].

Аналіз вищезазначених проектів дозволяє виявити спільні наміри регуляторних комісій щодо окреслення кола цифрових об'єктів, які можуть вважатися цифровими активами та підпадають під правове регулювання, запропоноване вищезазначеними актами, оскільки вони мають певні визначені характеристики. Таким чином, цифрові активи в розумінні цих актів повинні, зокрема, бути конкурентними, відчужуваними та мати властивість бути підконтрольними певній особі протягом певного періоду часу. Це наближає їх за своїми ознаками до матеріальних речей і, відповідно, дає можливість застосувати до них положення про право власності.

Є підстави припускати, що ідеї цих розробок регуляторних комісій ґрунтувалися на попередніх численних наукових дослі-

[1] 'Digital Assets' (*Law Commission* January 6, 2023) <https://www.lawcom.gov.uk/project/digital-assets/> accessed May 7, 2025.

[2] 'Draft UNIDROIT Principles on digital assets and private law' (*UNIDROIT* 2023). <https://www.unidroit.org/wp-content/uploads/2023/01/Draft-Principles-and-Commentary-Public-Consultation.pdf> accessed May 8, 2025.

дженнях цифрових (віртуальних) активів, присвячених визначенню ознак, які б дозволили виділити групу цифрових об'єктів, які можна вважати різновидом майна через їх схожість з матеріальними об'єктами. Така ознака як конкурентоздатність (rivalrousness) вже досить давно обговорюється в наукових дослідженнях[1]. Серед інших ознак цифрових активів, які можна визнати різновидом майна, вчені також згадують стійкість, багаторазовість використання (здатність повторно використовувати цифровий об'єкт необмежену кількість разів) [2], можливість ідентифікації та повторного використання іншими, а не лише власником чи творцем цифрових активів[3].

Серед перерахованих ознак найбільш важливою видається так звана «конкурентоздатність» (rivalrousness). У своїх пізніших дослідженнях Дж. Ферфілд зазначає, що конкурентоздатність для цифрових активів замінює «фізичність» матеріальних речей[4]. У контексті дослідження NFT науковець зазначає, що ширшим розумінням конкурентоздатності є унікальність об'єкта[5]. Проте, на нашу думку, притаманна об'єкту властивість унікальності не є беззаперечною для визнання його цифровим активом як різновидом майна. Адже необхідно враховувати, що деякі цифрові активи є взаємозамінними, тобто не можуть вважатися індивідуально-визначеними з цивілістичної точки зору. Однак, з погляду на те, що формою існування цифрового активу є фрагмент коду як унікальна комбінація символів, кожен цифровий актив є унікальним.

Ще однією важливою характеристикою цифрових активів є їх здатність бути об'єктами контролю. Враховуючи цю характеристику, ми можемо виділити поняття цифрових активів у вузькому сенсі (як різновиду майна) в рамках поняття цифрових активів у широкому значенні. Зокрема, таким чином можна відмежувати об'єкти права інтелектуальної власності, такі як набори даних, малюнки, тексти,

---

1 Blazer Ch, "The five indicia of virtual property" (2006) 5 PLR 137, 143-145; Fairfield J, "Virtual Property" (2005) 85 B Univ L Rev 1047, 1053-1054.

2 Moon M, "Activity lifecycle of digital assets" (2007) 3(3) J Dig As Man 112.

3 Toygar A, Rohm C, Taipe J, Zhu J, «A New Asset Type: Digital Assets» (2013) 22(4) J Int Tech Inf Man 113.

4 Fairfield J, "Bitpropery" (2015) 88(4) SCL Rev 805.

5 Fairfield J, "Tokenized: the law of non-fungible tokens and unique digital property" (2022) 97(4) ILJ 1261.

які самі по собі не можуть бути предметом контролю, оскільки можуть копіюватися необмежену кількість разів. Таким чином, об'єкт інтелектуальної власності, який сам по собі не втілений у цифровій формі та не індивідуалізований таким чином (наприклад, шляхом перетворення на NFT), не кваліфікується як цифровий актив у вузькому сенсі. Відповідно, зазначені об'єкти залишаються об'єктами права інтелектуальної власності та не перетворюються на об'єкти права власності[1].

Згадані ознаки цифрових активів видаються необхідними та достатніми для визнання їх різновидом майна. Такі функції дозволяють цифровим об'єктам фактично «імітувати» об'єкти права власності в реальному світі. Так, дослідники Кембриджського центру альтернативних фінансів, визначаючи характеристики речей, посилаються на такі: можливість передачі, виключність та економічна цінність. Кінцева характеристика – тілесність – на думку дослідників, викликає сумніви. Тим не менш, виходячи з даного підходу, ознака фізичності є єдиною ознакою, яка не притаманна цифровим активам і не дозволяє їх ототожнювати з речами. Крім того, матеріальність даних залишається предметом дискусій. Зокрема, Правова комісія Великобританії наголошує, що при визначенні характеристик цифрових об'єктів вони не використовують критерій безтілесності, оскільки самі мережі чи системи мають тілесне, хоча й дуже розподілене існування.

Видається, що для розмежування категорій цифрових активів у широкому та вузькому значенні (як різновиду майна із застосуванням положень про право власності) доцільно використовувати категорію «цифрова річ». Концепцію цифрової речі можна застосувати до групи цифрових активів, які схожі на речі матеріального світу, мають ті самі характеристики, але є нематеріальними благами в цифровій формі. До їх ознак належать: безтілесність/нематеріальність (складаються з даних, представлених на електронних носіях); постійність/стабільність (багаторазове використання); конкурентоздатність; економічна цінність; відчужуваність; ексклюзивність; можливість передачі та знищення.

[1] Nekit K. "Legal aspects of the use of social media accounts: current state and perspectives" (2020) 10(3) TLQ 305.

Правові рамки для цифрових активів: недоліки сучасного підходу та доцільність застосування положень про право власності

1. Обґрунтування доцільності застосування положень про право власності до цифрових активів

Історично склалося так, що у якості основної парадигми для цифрових об'єктів розглядається перш за все право інтелектуальної власності. Можливо, така ситуація пояснюється тим, що спочатку під цифровими активами розумілися цифрові зображення, текстові файли, електронні книги, відео тощо, тобто об'єкти, які в реальному світі регулюються положеннями про право інтелектуальної власності. Дійсно, цифрові активи та об'єкти права інтелектуальної власності мають одну важливу спільну рису – нематеріальність, але, як зазначають дослідники, на цьому їхня схожість закінчується. Можливо, ця позиція є надто категоричною, і, безумовно, можна знайти інші спільні риси між цифровими активами та об'єктами права інтелектуальної власності, наприклад, як перші, так і другі можуть мати економічну цінність, іноді досить суттєву. Тим не менш, аналіз сутності та особливостей цифрових активів, проведений у попередньому розділі, виявляє їх суттєві відмінності від об'єктів права інтелектуальної власності.

Дж. Фейрфілд, один з найактивніших дослідників віртуальних активів, справедливо зазначає, що онлайн-ресурси не мають нічого спільного з інтелектуальною власністю. Швидше, ці ресурси були розроблені таким чином, щоб мати ті ж характеристики, що й реальні рухомі речі. Цей факт робить положення про право власності очевидним джерелом регулювання таких ресурсів.[1]

Однак пропозиція застосовувати положення про право власності до цифрових активів зустрічає багато заперечень, оскільки в цивілістиці усталеним є підхід, згідно з яким об'єктом права власності є матеріальна річ. Однак у національних законодавстві різних країн існують відмінності у підходах до визначення права власності. У деяких країнах, наприклад, у Німеччині, об'єктами права власності можуть

[1] Fairfield J. "Virtual Property" (2005) 85 B Univ L Rev.

бути лише суто фізичні речі[1]. Однак в інших країнах, наприклад, в Україні, деякі об'єкти, які не мають матеріального змісту, все ж таки вважаються об'єктами права власності, наприклад, електроенергія, бездокументарні цінні папери та безготівкові гроші. В Україні поняття майна тлумачиться широко та включає не лише матеріальні речі, а й майнові права та обов'язки (ст. 190 Цивільного кодексу України). Дослідники Кембриджського центру альтернативних фінансів зазначають, що більшість правових систем світу визнають майнові права у складі майна, які охоплюються категорією *res incorporales*[2]. Країни загального права взагалі зазвичай мають абстрактне поняття майна, яке не виключає можливості існування інших об'єктів речових прав, окрім фізичних речей.

У сучасній цивілістичній доктрині точаться дискусії щодо необхідності говорити про ширший підхід до визначення самого поняття права власності. Останнє можна розглядати як найповніше абсолютне право, яке встановлює право власності не лише на речі, а й на інше майно та проявляється у ставленні до майна як до свого[3]. Такий «широкий» підхід до права власності також характерний для практики Європейського суду з прав людини (ЄСПЛ). Аналіз справ ЄСПЛ призводить до однозначного висновку про «дематеріалізацію» права власності та поширення положень про майнові права не лише на речі, а й на широкий спектр нематеріальних об'єктів. Суд поширює поняття майна на акції компаній та інші фінансові інструменти, бізнес-ліцензії, майбутні доходи, оренду нерухомості та житлові права, навіть соціальні виплати та пенсії тощо[4].

У справі *Gasus Dosier – und Fordertechnik GmbH v. the Netherlands* Суд наголосив, що поняття «майна» у значенні Протоколу № 1 до Європейської конвенції про захист прав людини та основоположних свобод не обмежується однозначно фізичними речами. Деякі інші права та інтереси, що становлять активи, можуть бути класифіковані

[1] Bürgerliches Gesetzbuch (2002) 2 Bundesgesetzblatt 42.

[2] Allen J and others, 'Legal and Regulatory Considerations for Digital Assets – CCAF Publications' (*Cambridge Judge Business School*, 22 December 2020) accessed 9 May 2025.

[3] Майданик Р. Переосмислення поняття і класифікації речей в умовах рекодифікації. *Проблеми цивільного права та процесу.* Харків, 2021. С. 56.

[4] Посібник За Статтею 1 Протоколу № 1 Конвенції Про Захист Прав Людини Та Основоположних Свобод «Захист Власності». 2019. <https://unba.org.ua/assets/uploads/news/publikacii/Guide_Art_1_Protocol_1_UKR_-2019.pdf> accessed 9 May 2025.

як майнові права та охоплюватися терміном «майно»[1]. Тому можна стверджувати, що ЄСПЛ розробив підхід до розуміння майнових прав як ширшої категорії, яка не обмежується матеріальними речами. Таке широке тлумачення права власності в практиці ЄСПЛ свідчить про «розмивання меж у тлумаченні права власності в романо-германській та англо-американській правових системах»[2].

Останнім часом поширення набула також пропозиція розширеного тлумачення самого поняття «річ». Так, Р. Майданик зазначає, що в умовах глобалізації необхідно переосмислити поняття майна, речей та їх класифікацію. Вчений зазначає, що поняття речей визначається по-різному в різних країнах. В одних країнах речі розуміються вузько, як тілесні об'єкти матеріального світу, а в інших – широко, не лише як об'єкти матеріального світу, а й як майнові права. Водночас необхідно визначати категорію речей з огляду на розвиток науки, техніки та всіх соціально-економічних процесів, що відбуваються в суспільстві. Враховуючи, що річ як об'єкт правовідносин не визначається фізичними властивостями, оскільки вона не є явищем фізики, поняття речі може бути визначено законодавцем з урахуванням існуючих потреб. В цифрову епоху широке розуміння речі, яке охоплює будь-які матеріальні чи нематеріальні майнові об'єкти, над якими можливе юридичне панування, відповідає суспільним потребам. Тому пропонується розглядати річ як «обмежений у часі та просторі ресурс, привласнений особою на належних правових підставах». Таким чином, поняття речі у вузькому сенсі охоплює речі в матеріальній, тілесній формі, *res corporales*, тоді як речі в широкому сенсі включають як матеріальні (тілесні), так і нематеріальні (безтілесні). Відчутні (тілесні) речі сприймаються нашими органами чуття, тоді як нематеріальні речі сприймаються лише розумом. Визначальним для речей у широкому сенсі є здатність блага в тілесній чи безтілесній формі «бути привласненим, перебувати під правовою владою внаслідок підпорядкування волі особи, мати економічну цінність та служити для використання»[3].

---

[1] *Gasus Dosier – und Fordertechnik GmbH v. the Netherlands* App no 15375/89 (ECHR, 2005).

[2] Шимон С. Теорія майнових прав як об'єктів цивільних правовідносин. К.: Юрінком Інтер., 2014. С. 168.

[3] Майданик Р. Переосмислення поняття і класифікації речей в умовах рекодифікації. *Проблеми цивільного права та процесу.* Харків, 2021. С. 56.

Вищезазначені міркування підтримують і інші вчені, які вважають, що відмова від матеріалістичного розуміння речей є потребою сьогодення. Вони зазначають, що розвиток науково-технічного прогресу призвів до модернізації поняття права власності та поняття речі, а також до юридичного визнання нових видів майна, що спричинило розширення кола права власності у двох напрямках. По-перше, поняття майна було поширене на електроенергію, газ та інші речовини, які не вписуються в традиційне розуміння речей, а по-друге, відродилося поняття «безтілесних речей», яке охоплює права, що мають грошову цінність. В результаті більшість країн визнають два види права власності: матеріальні та нематеріальні, і доктрина та практика поступово відходять від традиційного розуміння права власності. Вчені вважають, що при відповіді на питання про те, що слід вважати річчю, потрібно виходити не з міркувань про фізичність, а про придатність цього явища в рамках цивільного обороту[1].

Конструкція безтілесної речі склалася в римському праві, де поступово виникло поняття речі в широкому сенсі, яке охоплювало не лише матеріальні об'єкти зовнішнього світу, а й майнові відносини та права. Поділ речей на тілесні (*corporales*), які можна відчути на дотик, і безтілесні (*incorporales*), які неможливо відчути на дотик, зустрічається в працях римського юриста Гая[2]. За Гаєм, тілесні речі – це ті, які за своєю природою можна схопити, такі як земля чи одяг; безтілесні речі – це ті, яких неможливо доторкнутися, але вони існують за законом, такі як спадщина, користування чи зобов'язання[3]. Таким чином, поняття безтілесних речей виникло в римському праві для вирішення питань цивільного обороту, коли все частіше поряд з матеріальними речами об'єктами відносин почали ставати нематеріальні блага. Так само й у наші дні зростання кількості інформаційних (цифрових) об'єктів, які не мають матеріальної природи, але ставлення до них є як до фізичних речей, звертає нас до конструкції безтілесних речей для задоволення практичних потреб цивільного обороту.

Як випливає з попередніх міркувань, сучасна доктрина та судова практика вказують на необхідність переосмислення поняття права

[1] Шимон С. Теорія майнових прав як об'єктів цивільних правовідносин. К.: Юрінком Інтер, 2014. С. 286-287.

[2] Giglio F. "Pandectism and the Gaian classification of things" (2012) 62(1) The Univ of Tor LJ 1.

[3] Mousourakis G. *Roman law and the origins of the civil law tradition* (Springer 2016).

власності та речей. Нові умови існування суспільства наповнюють ці поняття новим змістом і, відповідно, дають змогу поширити їх на нові категорії благ, які не мають матеріального змісту, але мають характеристики, що дозволяють їм бути об'єктами власності.

Ще однією перешкодою для поширення режиму власності на цифрові активи вважається теорія *numerus clausus*. Цей принцип передбачає, що право власності та інші речові права виникають лише з положень закону. Необхідність цього принципу пояснюється тим, що право власності відрізняється від інших прав критерієм «абсолютності», тобто силою дії проти третіх осіб (*erga omnes*). Треті особи зобов'язані не робити нічого, що може порушити ці права. Отже, всі учасники цивільних відносин повинні бути належним чином поінформовані про існування таких надзвичайно ефективних прав. Наслідком цього принципу є необхідність реєстрації прав на нерухоме майно[1].

У зв'язку з цим дослідники зазначають, що в «класичному» приватному праві право власності протиставляється договірному праву. Оскільки право власності забезпечує надійніший рівень захисту, дозволяючи власникам протиставляти свої права всім іншим учасникам цивільних відносин, воно також вимагає суворішого обов'язкового регулювання, враховуючи той факт, що кожен повинен підкорятися його вимогам без особистої згоди. Принцип *numerus clausus* був запроваджений під час переходу від феодальної системи до класичного права власності з метою захисту унітарного права власності від повернення квазі прав власності. Цей принцип обмежує не лише кількість та зміст речових прав, але й способи їх виникнення, передачі та припинення. Через дію цього принципу класичне право власності не так швидко визнає нові об'єкти права, оскільки воно прагне обмежити кількість об'єктів, на які може претендувати право власності. *Numerus clausus* об'єктів права «передбачає обмеження щодо об'єктів і тим самим відокремлює більш обмежену категорію того, що може бути об'єктом права власності, від ширшої категорії того, що може бути об'єктом права договору» [2].

Однак, принцип *numerus clausus* останнім часом зазнає критики. Дослідники зазначають, що використання *numerus clausus*

[1] Ossowska M. "The numerus clausus issue in property law – European private las and the polish perspective" (2020) 82 Studia Iuridica 211.

[2] Sief van Erp, "Ownership of data and the numerus clausus of legal objects" (2017) 6 Maastr Eur PLI WP 1.

створює ризик досить повільної еволюції правових інститутів. У часи динамічного розвитку світової економіки жорстке дотримання старих, фіксованих рішень може бути шкідливим[1]. Висловлюються думки, що в сучасних умовах глобалізації необхідно впроваджувати концепцію сутнісного (функціонального) розуміння речових прав, формувати збалансоване співвідношення закритого (*numerous clausus*) та відкритого (*numerous apertus*) переліку речових прав. Актуальним визнається систематичне впровадження принципу відкритого переліку речових прав, згідно з яким мають бути зареєстровані не лише речові права, визначені законом, а й інші права того ж характеру, навіть якщо вони не визначені законом як речові права[2].

Таким чином, усі заперечення, висунуті проти можливості поширення режиму власності на цифрові активи, спростовуються при детальнішому аналізі. Потреби практики вимагають перегляду сучасного поняття права власності та речі з метою охоплення нових об'єктів цивільних прав, що виникають в результаті змін, які відбуваються в суспільстві через процеси цифровізації.

Недоліки сучасного підходу до регулювання відносин з цифровими активами

Критика сучасного підходу до регулювання відносин щодо цифрових активів зводиться до того, що визначення прав та обов'язків їх учасників за допомогою Terms of Service чи ліцензійних угод не враховує сучасних змін правової природи цифрових активів. Останнім часом цифрові активи набувають все більшої цінності, перетворюючись на самостійні об'єкти цивільного обігу. Відповідно, регулювання відносин щодо таких активів має враховувати всіх учасників ринку та забезпечувати належним чином захист прав їх володільців. Відносини щодо цифрових активів часто виходять за рамки користувацьких угод, на підставі яких вони виникають. Та й самі ці угоди,

[1] Akkermans B. 'The Numerus Clausus of Property Rights' in Graziadei M, Smith L (eds.) *Comparative Property Law. Global Perspectives* (Cheltenham–Northampton 2017).

[2] Майданик Р., Майданик Н., Попова Н. Переосмислення загальної частини речового права в умовах європеїзації та кодифікації. *Підприємництво, господарство і право*. 2021.

як було зазначено раніше, далекі від досконалості, оскільки суттєво обмежують права користувачів на користь розробників.

Згідно з останніми дослідженнями, типові контракти (включаючи користувацькі угоди як їхній різновид) часто є «нечитабельними», або як мінімум складними для розуміння через їхню довжину, зміст і юридичний жаргон[1]. Ситуація в онлайн-середовищі ще гірша, хоча б тому, що проведене дослідження виявило, що час, необхідний для простого ознайомлення з користувацькою угодою, приголомшує. Зокрема, користувачі мали б витрачати вісім годин на день протягом 76 днів лише на те, щоб прочитати політику конфіденційності 1500 веб-сайтів, які вони відвідують щороку[2]. Зрештою, більшість користувачів не читають угоди Terms of Service, і переважна більшість не звертає уваги на потенційно небезпечні умови[3].

Неоднозначною є і судова практика щодо захисту прав користувачів щодо їхніх цифрових активів на підставі користувацьких угод. Одним із прикладів успішного захисту прав користувачів є справа *Li Hongchen v. Beijing Arctic Ice Technology Development Co*, у якій «мешканець» віртуального світу подав позови проти розробника через те, що його віртуальну власність було захоплено хакером. Суди першої та апеляційної інстанції зобов'язали провайдера повернути майно його законному володільцю[4].

Однак в іншій справі, *Bragg v. Linden Research, Inc.*, спроба користувача захистити свої права не увінчалася успіхом. Суть справи полягала в тому, що аватар користувача в MMOG Second Life придбав земельну ділянку на аукціоні, використовуючи лазівку в програмному забезпеченні. Після того, як розробник дізнався про порушення, він заблокував обліковий запис користувача, що призвело до фак-

[1] Obar J., Oeldorf-Hirsch A. "The biggest lie on the Internet: ignoring the privacy policies and terms of service policies of social networking services" (2020) 23(1) Inf Com Soc 128; Bakos Y., Marotta-Wurgler F., Trossen D. "Does anyone read the fine-print? Consumer attention to standard form contracts" (2014) 43(1) JLS 1.

[2] Belli L., Venturini J. Private ordering and the rise of terms of service as cyber-regulation. 2016. № 5 (4) Int Pol Rev 1.

[3] Obar J., Oeldorf-Hirsch A, "The biggest lie on the Internet: ignoring the privacy policies and terms of service policies of social networking services" (2020) 23(1) Inf Com Soc 128; Bakos Y., Marotta-Wurgler F., Trossen D. "Does anyone read the fine-print? Consumer attention to standard form contracts" (2014) 43(1) JLS 1.

[4] Knight W. Gamer Wins Back Virtual Booty in Court Battle. *New Scientist*, 23 December 2003. URL: https://www.newscientist.com/article/dn4510-gamer-wins-back-virtual-booty-in-court-battle/> accessed 10 February 2025.

тичної конфіскації всього віртуального майна, яке належало користувачеві[1]. Цей випадок демонструє, що розробники укладають угоди з користувачами таким чином, що вони залишають за собою право позбавляти користувачів їхніх цифрових активів, у які вони інвестували значні гроші та час, без будь-якої можливості отримати будь-яку компенсацію чи оскаржити дії розробників.

До недоліків користувацьких угод можна віднести й те, що користувачі та розробники можуть по-різному трактувати їх умови. Прикладом цього може бути ситуація в грі EVE Online, коли розробник відмовився застосувати санкції до користувача на прохання іншого користувача, оскільки вважав, що не було порушено користувацьку угоду. Однак детальний аналіз користувацької угоди, проведений незалежною експертною комісією, дозволив дійти висновку, що порушення все ж таки мало місце[2]. Крім того, навіть у випадку коли розробник вирішує застосувати санкції до користувача за порушення угоди, єдиним доступним покаранням є блокування облікового запису користувача. Якщо були порушені інтереси інших користувачів, компенсація для них не передбачена.

Таким чином, хоча положення Terms of Service можуть застосовуватися для вирішення суперечок між користувачем і розробником, вони є абсолютно незастосовними до відносин між користувачами. Адже користувацька угода регулює відносини лише між користувачами та розробниками, вона не пов'язує користувачів жодними правами та обов'язками щодо один до одного[3]. Отже у разі порушення прав одного користувача іншим, єдиним способом захисту порушеного інтересу є звернення до розробника з вимогою застосувати до порушника санкції. Однак розробник не зобов'язаний вирішувати суперечки між користувачами та захищати їх порушені інтереси, тому вирішення проблеми в кожному конкретному випадку залишається на його власний розсуд. При цьому розробники досить часто відмовляються визнавати факт порушень, особливо якщо порушення відбулося з використанням недоліків програмного забезпечення, оскільки розголошення такого факту ставить під сумнів безпеку інших корис-

[1] *Bragg v. Linden Research, Inc.* (2007) USDC EDP 487 F. Supp. 2d 593.

[2] Lim HYF. Who monitors the monitor? Virtual world governance and the failure of contract law remedies in virtual worlds. 2009. 11 Vand J Ent & Tech L 1053.

[3] Ludwig J. Protections for virtual property: a modern restitutionary approach. 2011. № 32(1) LLA Ent L Rev 1.

тувачів і може призвести до їх відмови від використання програми, що для розробника означатиме втрату клієнтів.

Недосконалість Terms of Service спонукає дослідників до думки про необхідність заборони необмежених можливостей розробників, які вони встановлюють для себе в користувацьких угодах. Так, П. Палка вказує на необхідність розробки так званого «користувацького права» за аналогією із захистом прав споживачів, що дозволить забезпечити баланс у фактичній нерівності в цифрових відносинах на законодавчому рівні[1].

Аналіз судової практики[2] виявляє тенденцію надання судами більшого захисту користувачам всупереч умовам користувацької угоди, незважаючи на те, що користувацькі угоди визнаються договорами та, відповідно, зобов'язують сторони й мають застосовуватися переважно перед законом. Проте суди обмежують невиправдано широкі повноваження розробників на користь користувачів. Ситуація, що склалася, свідчить про необхідність встановлення певних обмежень для розробників на законодавчому рівні, щоб захистити користувачів як слабшу сторону. Адже сучасні платформи фактично стали монополістами у віртуальному середовищі та явно зловживають своїм становищем при встановленні правил поведінки. Тому, за аналогією з реальними монополіями, виникає нагальна потреба втручатися в «правила гри», встановлені розробниками для користувачів, щоб забезпечити баланс інтересів.

Першим кроком у цьому напрямку можна вважати прийняті у 2022 році Закон про цифрові ринки (Digital Markets Act) та Закон про цифрові послуги (Digital Services Act). Як зазначає Європейська комісія, Закон про цифрові послуги та Закон про цифрові ринки були прийняті для створення безпечнішого цифрового простору, де захищені основні права користувачів[3]. Закон про цифрові ринки визначає поняття так званого «брамника» (gatekeeper), яким визнаються дуже

---

1 Palka P. *Virtual property: towards a general theory* (European University Institute 2017) 218.

2 *Ajemian v. Yahoo!, Inc.* 84 N. E.3d 766 [2017]. № 17-1005, 2018 WL 489291 (U. S. Mar. 26, 2018); 'Facebook Ruling: German Court Grants Parents Rights to Dead Daughter's Account' (*BBC News*, 12 July 2018) <https://www.bbc.com/news/world-europe-44804599> accessed 10 February 2025.

3 The Digital Services Act Package. *Shaping Europe's digital future.* 2022. URL: https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package > accessed 10 February 2025.

великі онлайн-платформи або дуже великі онлайн-пошукові системи, що мають понад 45 мільйонів користувачів, тобто 10% населення Європи. Для таких великих гравців у цифровому просторі встановлюються істотні обмеження, спрямовані на запобігання зловживання ними своїми правами та захист прав кінцевих і бізнес-користувачів. Було вирішено застосувати такі обмеження, щоб запобігти «серйозному дисбалансу в переговорній силі та, як наслідок, несправедливій практиці та умовам для бізнес-користувачів, а також для кінцевих користувачів основних сервісів платформи, що надаються гейткіперами»[1]. Основні обов'язки гейткіперів викладені в статтях 5-8 Закону про цифрові ринки.

Закон про цифрові послуги, переслідуючи мету забезпечення кращого захисту споживачів і основних прав користувачів, визначає деякі вимоги до змісту Terms of Service. Зокрема, ст. 14 згаданого Закону вимагає, щоб постачальники посередницьких послуг включали до своїх умов положення про будь-які обмеження, які вони встановлюють щодо використання їхніх послуг. Ці положення повинні включати інформацію про будь-яку політику, процедури, заходи та інструменти, що використовуються для модерування вмісту, включно з алгоритмічним прийняттям рішень і перевіркою персоналу, а також правила процедури внутрішньої системи розгляду скарг. Ця інформація має бути викладена чіткою, простою, зрозумілою, зручною та недвозначною мовою та має бути загальнодоступною у легкодоступному та машиночитаному форматі. Крім того, постачальники посередницьких послуг повинні повідомляти користувачів про будь-які істотні зміни в умовах. Ще одне надзвичайно важливе правило полягає в тому, що постачальники посередницьких послуг повинні діяти старанно, об'єктивно та пропорційно, належним чином враховуючи права та законні інтереси всіх залучених сторін, включаючи основні права одержувачів послуг. Ці фундаментальні права включають, але не обмежуються: для одержувачів послуг – право на свободу вираження поглядів та інформації, право на повагу до приватного та сімейного життя, право на захист персональних даних, право недискримінації та право на ефективний засіб правового захисту; для

[1] European Parliament and Council Regulation (EU) 2022/1925 of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) [2022] *OJ L 265 /1.*

постачальників послуг – свобода ведення бізнесу, включаючи свободу договору; для сторін, які постраждали від незаконного контенту – право на людську гідність, права дитини, право на захист власності, включаючи інтелектуальну власність, і право на недискримінацію[1].

Проблема захисту прав користувачів неодноразово обговорюється й під час критики End User License Agreement (EULA), яку називають «міксом між конституцією та священною книгою» для віртуального середовища[2]. Дж. Фейрфілд зазначає, що за останні двадцять років відбулося безпрецедентне розширення прав інтелектуальної власності, які компанії використовують як важелі контролю над приватними власниками. На думку дослідника, це сталося через те, що правове регулювання було орієнтоване на стару цифрову економіку, яка більше фокусувалася на ліцензіях, ніж на продажу цифрових товарів. Однак настав час змінити законодавчу базу, щоб врахувати нові технологічні можливості[3].

Сучасні цифрові активи, такі як NFT, стикаються зі значними юридичними перешкодами для свого розвитку, оскільки всі відносини у сфері цифрових активів регулюються переважно через контракти та ліцензійні угоди. У результаті користувачі (споживачі) отримують лише тимчасовий доступ до цифрових активів на основі ліцензій, без права їх продажу. Таким чином, користувачі не отримують права власності на цифрові об'єкти, які вони створюють або купують.[4] Наприклад, якщо хтось купує електронну книгу, він фактично лише отримує право використовувати книгу на основі ліцензії, але не стає її власником. Цей підхід заснований на тому, що щоразу, коли користувач збирається прочитати електронну книгу, він фактично створює її копію. Однак у реальному світі ситуація інша. Споживачеві, який придбав фізичну книгу, не потрібна ліцензія на її читання, оскільки він не створює її копії. Така, здавалося б, суто технологічна різниця насправді породжує суттєві відмінності в становищі власників елек-

[1] European Parliament and Council Regulation (EU) 2022/2065 of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) [2022] *OJ L 277/1.*

[2] Glushko B. Note. Tales of the (virtual) city: governing property disputes in virtual worlds. 2007. № 22 Berkeley Tech LJ 507.

[3] Fairfield J. Tokenized: the law of non-fungible tokens and unique digital property. 2022. № 97(4) ILJ 1266.

[4] Perzanowski A., Schultz J. *The end of ownership: personal property in the digital economy* (MIT Press 2016).

тронних і фізичних книг. Власник фізичної книги може її віддати, продати або заповідати, тобто вільно нею розпоряджатися, а власник електронної книги обмежений у своїх повноваженнях ліцензійною угодою і не може передавати її третім особам. Таким чином, незважаючи на те, що у користувачів створюється ілюзія покупки книги, вони не можуть вільно розпоряджатися своїм цифровим активом, який ними було придбано[1].

Несправедливість цієї ситуації посилюється тим фактом, що найчастіше споживачі помилково вважають, що вони стають власниками цифрових активів, які вони придбали, а не лише ліцензіатами, оскільки на сторінці продажу не згадується, що транзакція є по суті наданням ліцензії, а не продажем. Щоб зрозуміти, що транзакція є, по суті, наданням ліцензії, користувачеві найчастіше доводиться читати розгорнуті умови на веб-сайтах роздрібних продавців. Більшість користувачів не витрачають на це свій час, зокрема виявилося, що лише 8% користувачів читають EULA[2].

Тому правове регулювання у сфері цифрових активів із застосуванням EULA суттєво обмежує можливості власників цифрових об'єктів порівняно з власниками фізичних об'єктів. Зокрема, враховуючи те, що на підставі ліцензії права на використання цифрових об'єктів надаються лише протягом життя користувача, ці права припиняються з його смертю, навіть якщо договір між провайдером і користувачем не містить спеціальних положень з цього питання. Тобто цифрові активи не можна успадковувати за законом або згадувати в заповіті, що викликає активну критику EULA з боку дослідників у сфері спадкування цифрових активів.[3]

Таким чином, ситуація, що склалася у сфері правового регулювання відносин щодо цифрових активів із застосуванням договірних положень та права інтелектуальної власності свідчить про неефективність такого підходу до захисту прав володільців цифрових активів. Натомість у підходах до правового регулювання цих

---

[1] Fairfield J. Tokenized: the law of non-fungible tokens and unique digital property. 2022. № 97(4) ILJ 1294-1295.

[2] Sauro J. Do Users Read License Agreements?. *MeasuringU.* 2011. URL: https://measuringu.com/eula/ > accessed 10 February 2025.

[3] Edwards L and Harbinja E, ''What Happens to My Facebook Profile When I Die?': Legal Issues around Transmission of Digital Assets on Death' (SSRN, 21 February 2013) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2222163>accessed 10 February 2025.

відносин простежується дисбаланс інтересів, коли провайдери та розробники отримують комплексний захист і гарантії, а користувачі перебувають у дуже вразливому становищі. Тому виникає необхідність переглянути підхід до правового регулювання відносин щодо цифрових активів з метою забезпечення балансу інтересів розробників і користувачів та ефективного захисту інтересів останніх. У попередніх дослідженнях нами вже неодноразово визначалася інша модель регулювання відносин щодо цифрових активів, яка може забезпечити більш ефективний захист інтересів володільців цифрових активів[1]. Сучасні доктринальні й регулятивні розробки та історичні передумови дають підстави стверджувати про можливість поширення положень про право власності на окремі категорії цифрових активів, які відповідають визначеним ознакам. За умови поширення положень про право власності на цифрові активи, користувацькі та ліцензійні угоди повинні будуть розроблятися таким чином, щоб права користувачів не були утисненими з боку розробників. Крім того, такий підхід забезпечить вирішення суперечок, що виникають за участі інших учасників ринку.

Право цифрової власності як парадигма для цифрових активів

Вчені зазначають, що регулювання у сфері новітніх технологій має бути адаптовано до того, як люди їх використовують. Якщо користувачі купують цифрові активи як майно, ставляться до них як до майна, заповідають їх як майно (що, наприклад, дозволено в більшості штатів США[2]), закон повинен ставитися до них як до майна[3].

Виявилося, що психологічно власники цифрових активів сприймають віртуальні об'єкти як своє майно. Про це свідчить той факт, що користувачі не лише використовують доступні механізми для забо-

[1] Nekit K. Digital ownership as a reflection of the Rule of Law. Rule of Law in a transitional spectrum. Ed. by Rigmor Argren. Uppsala: Iustus. 2024. 470 p. P. 405-439.

[2] Edwards L and Harbinja E, ''What Happens to My Facebook Profile When I Die?' : Legal Issues around Transmission of Digital Assets on Death' (*SSRN*, 21 February 2013). URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2222163>accessed 10 May 2025.

[3] Fairfield J. Tokenized: the law of non-fungible tokens and unique digital property. 2022. № 97(4) ILJ 1261, 1288-89, 1291, 1293.

рони іншим особам користуватися своїми речами, але й звертаються до судів з позовами проти тих, хто порушує їхні права на віртуальні об'єкти[1].

Враховуючи важливість цифрових активів для їх власників, Правова Комісія Великобританії у своїх останніх розробках зазначає про необхідність розглядати цифрові активи як вид майна та застосовувати до них положення про право власності, оскільки «право власності визнається проти всього світу, тоді як особисті права визнаються лише проти того, хто взяв на себе відповідний юридичний обов'язок»[2]. На думку Комісії, застосування положень про право власності до цифрових активів забезпечить їх більш надійний захист та гарантуватиме права власників цифрових активів.

Дійсно, як було виявлено раніше, сучасні підходи до регулювання цифрових активів із застосуванням положень договірного права та права інтелектуальної власності є досить дискримінаційними щодо володільців цифрових активів. Вони значно обмежені у своїх правах порівняно з провайдерами та повністю незахищені у відносинах з іншими користувачами. Для забезпечення інтересів володільців цифрових активів необхідне абсолютне право, яке надасть їм гарантії у відносинах з третіми особами. Тому право власності є найбільш очевидним та надійним інструментом, який забезпечить реалізацію та захист інтересів володільців цифрових активів.

Серед аргументів на користь поширення режиму права власності на цифрові активи, окрім необхідності забезпечення балансу інтересів між провайдерами та користувачами, є необхідність захисту користувачів від крадіжки їхньої віртуальної власності третіми особами[3], а також той факт, що такі активи купуються та продаються за реальні гроші[4]. Ще одним вагомим аргументом на користь визнання необхідності цифрової власності є той факт, що люди часто інвестують значну кількість часу та зусиль у створення цифрових активів[5].

[1] Sheldon D. Claiming ownership, but getting owned: contractual limitations on asserting property interests in virtual goods. 2007. № 54 UCLA L Rev, 761.

[2] Digital Assets. *Law Commission January*. 2023. № 6. URL: https://www.lawcom.gov.uk/project/digital-assets/> accessed May 7, 2025.

[3] Fairfield J. Virtual Property. 2005. № 85 B Univ L Rev 1081.

[4] Lastowka G., Hunter D. The laws of the virtual worlds. 2004. № 92(1) Cal L Rev 1, 51.

[5] Lastowka G., Hunter D. The laws of the virtual worlds. 2004. № 92(1) Cal L Rev 1, 51; Stephens M. Sales of in-game assets: an illustration of the continuing failure of intellectual property law to protect digital-content creators. 2002. № 80 Tex L Rev 1513.

Ця ситуація спонукає дослідників застосувати теорію праці Локка[1] для обґрунтування можливості поширення режиму права власності на цифрові активи.

Ще однією теорією, яка використовується для обґрунтування застосовності положень права власності до цифрових активів, є теорія утилітаризму Бентама[2]. Ця теорія зводиться до того, що право власності має виникати, коли загальний ефект від його виникнення призведе до збільшення загальної корисності або суспільного добробуту. В утилітаризмі суспільне благо складається з індивідуальних благ. Кількість часу та грошей, що інвестуються в цифрові активи, свідчить про те, що вони мають досить високу цінність для людей. Отже, є підстави для визнання права власності на цифрові активи з погляду їх цінності для окремих користувачів[3].

Таким чином, попри критику та заперечення щодо можливості застосування концепції права власності до цифрових активів, доктрина наводить численні аргументи, що свідчать на користь доцільності визнання права власності на цифрові активи. Однак важливо наголосити, що специфіка об'єкта (цифрових активів) визначає специфіку змісту, реалізації та захисту прав, що виникають щодо таких об'єктів. Тому доречно виділити особливий вид власності – цифрову власність, специфіка якої буде визначатися властивостями її об'єктів.

Право власності може відрізнятися певною кількістю варіацій, однак при цьому це не пов'язано з «розщепленням» права власності. У французький доктрині зустрічається протиставлення «доконаного» права власності та «недоконаного». Вважається, що право власності є повним та доконаним, коли воно є безстроковим, а річ не обтяжена речовими правами інших осіб. Недоконаним право власності є тоді, коли воно обтяжено, наприклад, узуфруктом. У такому випадку право власності називається «голим» правом власності (*nuda proprietas*)[4].

Доктрина та судова практика часто мають труднощі з кваліфікацією справ, що відрізняються від традиційних правових концепцій та визнаних правових режимів. Іноді правові інститути мають спільні риси з правом власності, але водночас відрізняються від нього. Це робить необхідним аналізувати кейси, що відрізняються від архети-

[1] Lock J. *Two Treaties of Government* (London 1823).
[2] Bentham J. An Introduction to the Principles of Morals and Legislation (Kitchener 2000).
[3] Lastowka G., Hunter D, "The laws of the virtual worlds" (2004) 92(1) Cal L Rev 1, 51.
[4] Normand S. La notion de modalité de la propriété (Québec, 2006).

пу. Звідси з'являються посилання на «модифікації права власності», «особливий стан права власності» або «особливі форми/види права власності». У кожному такому випадку виникає потреба уточнити, чим цей «особливий тип права власності» відрізняється від класичного. Це створює тенденцію кваліфікувати такі окремі випадки як «право власності *sui generis*», «право власності зі специфічними ознаками», «неповне/недосконале право власності» тощо. Такі концепції дозволяють підкреслити особливості такого права власності, незважаючи на тісний зв'язок з архетипом[1].

Дослідники зазначають, що залежно від відповідного правового об'єкта та особливостей історичного розвитку правових систем слід обрати більш прагматичний підхід, щоб уникнути непотрібних та непродуктивних академічних дебатів, заснованих на «стерильному догматичному аналізі та упереджених парадигмах 19 століття»[2]. Володіння фізичною річчю відрізнятиметься від володіння грошовою вимогою або даними. На думку вчених, використання терміна «право власності» можливе тією мірою, якою та чи інша правова система допускає існування різних видів та ступенів права власності[3].

Наприклад, законодавство деяких країн (Франції, Румунії, України) визнає такий «особливий вид права власності», як фідуціарна власність, яка має специфічний зміст та особливості здійснення. У такому випадку повноваження фідуціарного власника визначаються угодою з установником та обмежуються договором фідуціарної власності та положеннями закону[4]. За аналогією, право цифрової власності може бути визнане особливим видом права власності, поява якого була викликана розвитком інформаційних технологій.

Право цифрової власності має специфічний зміст та особливості здійснення, які вже визнані на рівні нормативних розробок та м'якого права. Зокрема, правоможність володіння як складова права власника у цьому контексті є предметом особливої уваги. У класичному речовому праві право власності передбачає фізичне панування над

1 *Там само.*

2 Sief van Erp, "Ownership of data and the numerus clausus of legal objects" (2017) 6 Maastr Eur PLI WP 1.

3 *Там само.*

4 Некіт К. Право приватної власності в інформаційному суспільстві: теорія і практика. Гельветика 2021.

річчю. Однак фізичне панування неможливе щодо цифрових активів через специфіку їх існування.

Досить детальний аналіз особливостей віртуального володіння провів П. Палка. Як зазначає дослідник, у більшості випадків володіння цифровими активами ускладнюється тим, що через архітектуру інформаційної системи фактичний контроль над цифровим об'єктом має більше однієї особи. Більшість цифрових активів контролюються користувачем та провайдером. Щоб впливати на цей об'єкт, користувач повинен мати дозвіл на доступ від провайдера. Але провайдер водночас також має доступ до цього об'єкта, може його змінювати або видаляти. Тому розробники віртуальних світів, поштових сервісів чи соціальних мереж володіють цифровими активами одночасно з користувачами. Більше того, провайдери навіть мають право змінювати або видаляти цифрові об'єкти, передбачаючи це в користувацьких угодах[1]. У цьому сенсі цифрове володіння, на відміну від традиційного володіння, не є виключним – кілька осіб можуть одночасно володіти об'єктом (тобто мати контроль над цим об'єктом).

Враховуючи такі властивості цифрових активів, доктрина та законодавчі комісії пропонують замінити категорію володіння щодо цифрових активів категорією контролю. Так, дослідники Кембриджського центру альтернативних фінансів зазначають, що є достатні підстави уникати поширення концепції володіння на нові цифрові об'єкти. Кращим рішенням є впровадження категорії виключного контролю та розробка відповідних дій і засобів правового захисту[2].

У Принципах UNIDROIT категорія контролю розуміється як «функціональний еквівалент «володіння» рухомим майном». Однак розробники Принципів наголошують, що «володіння» в цьому контексті є суто фактичним, а не юридичним поняттям. Крім того, оскільки цифровий актив є нематеріальним, ця функціональна еквівалентність володінню передбачає лише панування та владу над цифровим активом, але «не включає фізичного *situs dimension*, що застосовується до володіння рухомим майном». Вважається, що особа має контроль над цифровим активом, якщо вона має виключну можливість отримувати вигоду від цифрового активу, виключати інших

[1] Palka P. Virtual property: towards a general theory. *European University Institute.* 2017. С. 160-161.

[2] Allen J and others, 'Legal and Regulatory Considerations for Digital Assets – CCAF Publications' (Cambridge Judge Business School, 22 December 2020) accessed 9 May 2025.

з отримання вигоди від цифрового активу та виключну можливість передавати ці привілеї іншій особі[1].

Правова комісія Великої Британії також впроваджує категорію контролю, зазначаючи, що «фактичне поняття контролю (на відміну від поняття володіння) найкраще описує зв'язок між цифровими об'єктами та особами». Таким чином, категорія контролю також протиставляється категорії володіння матеріальними речами та спрямована на відображення специфіки цифрових активів. Поняття контролю розуміється Комісією як аналогічне поняттю володіння, оскільки це фактичні стосунки, які особа може мати з річчю, хоча й без елементу наміру. Тому корисним емпіричним правилом може бути те, що «особа, яка контролює цифровий об'єкт, має рівень контролю над цим активом, рівноцінний контрольному елементу володіння щодо матеріального об'єкту»[2].

Два аспекти згаданих висновків привертають увагу. По-перше, поява цифрових активів як нового об'єкта права власності спричиняє поступову зміну концепції володіння. Якщо володіння щодо фізичних речей передбачає фактичне панування над об'єктом, то володіння щодо віртуальних об'єктів перетворюється на право контролю, що ґрунтується на правових підставах, зокрема, положеннях користувацької угоди. Така можливість контролю щодо цифрового об'єкту може належати кільком суб'єктам одночасно, але лише власник цифрової речі контролює її з метою використання у власних інтересах. Тому панування над цифровими активами слід сприймати не як фізичне володіння, а як можливість фактичного контролю над річчю.

По-друге, стосовно цифрових активів може виникати так зване «подвійне» володіння, оскільки, як зазначалося вище, у деяких випадках більше однієї особи мають фактичний контроль над цифровим об'єктом. Проблема «подвійного» володіння також вирішується категорією контролю, яка дозволяє визначити, кому належить цифровий актив. Власником цифрового активу слід вважати особу, яка «контролює» об'єкт у власних інтересах, тобто має можливість отримувати вигоди від об'єкта та усувати інших від отримання цих вигод. Фактично, категорія контролю протиставляється категорії непрямого

[1] *Там само.*

[2] 'Digital Assets' (Law Commission January 6, 2023) URL: https://www.lawcom.gov.uk/project/digital-assets/> accessed May 7, 2025.

володіння (тримання), яка добре відома деяким країнам континентальної правової системи (див., наприклад, § 868 Цивільного кодексу Німеччини), оскільки провайдери не мають володіння з власного інтересу, вони виступають як «тримачі» цифрових об'єктів.

Правоможність користування цифровими активами також має певну специфіку. Станом на сьогодні право використання цифрових активів по суті обмежується ліцензією або користувацькою угодою. Як зазначалося, у більшості випадків провайдери обмежують права користувачів щодо цифрових активів на користь власних інтересів. Крім того, використання цифрових активів може бути обмежене самим програмним кодом[1].

Тому, якщо в рамках традиційних відносин власності власник задовольняє свої інтереси власними діями, то специфіка відносин цифрової власності визначається зобов'язанням між провайдером та користувачем. З одного боку, власник може самостійно використовувати цифрові активи та задовольняти свої інтереси без допомоги інших, але для того, щоб мати змогу реалізувати це право, воно має бути спочатку надане провайдером, який повинен постійно забезпечувати доступ власника до об'єкта з метою його використання.

Правоможність розпорядження цифровими об'єктами також матиме свою специфіку, оскільки залежатиме від особливостей платформи, специфіки коду та положень користувацької угоди. Крім того, право розпорядження цифровими активами має свою специфіку, оскільки, на відміну від реальних об'єктів, відчуження цифрових об'єктів вимагає сприяння провайдера. Зокрема, провайдери повинні забезпечити передачу цифрових об'єктів від однієї особи до іншої у разі їх відчуження. Однак це може бути зроблено за допомогою програмного коду, який забезпечить автоматичну передачу об'єкта від однієї особи до іншої, одночасно припиняючи доступ до цього об'єкта для першої особи.

Допомога провайдерів також необхідна для захисту цифрової власності: навіть якщо суд ухвалить рішення, наприклад, про необхідність витребування цифрового активу у незаконного володільця, реалізувати таке рішення без допомоги провайдера неможливо. З цією метою необхідно або передбачити обов'язок провайдерів спри-

[1] Sheldon D, "Claiming ownership, but getting owned: contractual limitations on asserting property interests in virtual goods" (2007) 54 UCLA L Rev 764.

яти виконанню судових рішень, або надати виконавцям судових рішень можливість доступу до платформи, або заздалегідь забезпечити можливість виконання судових рішень за допомогою програмного коду.

Висновки

Кількість та вартість цифрових активів зростають з кожним днем, тому потреба в забезпеченні належного регулювання відносин щодо цифрових активів стає все гострішою. Механізми, що використовуються наразі для регулювання відносин щодо цифрових активів, недостатньо ефективні для захисту прав користувачів. Користувацькі та ліцензійні угоди розробляються провайдерами та побудовані таким чином, щоб захистити, перш за все, їхні власні інтереси. Водночас користувачі залишаються у вкрай вразливому становищі. Така ситуація спонукає звернутися до права власності як парадигми, в рамках якої захист інтересів власників цифрових активів є найефективнішим. Сучасні доктринальні розробки та історичні передумови дають підстави стверджувати про можливість поширення положень про право власності на певні категорії цифрових активів. Це стало б можливим у випадку переосмислення категорії «річ». При визначенні цієї категорії слід виходити не з фізичних властивостей об'єкта, а з юридично визначених властивостей об'єкта. У рамках такого підходу слід розрізняти категорію речей у широкому сенсі (як *res corporales* та *res incorporales*), і у вузькому сенсі (як речі в матеріальній, тілесній формі).

Нова категорія *res incorporales,* цифрова річ, також може включати цифрові активи. Однак не всі цифрові активи можуть бути охоплені поняттям «цифрова річ». Цифрові активи, у свою чергу, можна розуміти в широкому сенсі (усі цифрові об'єкти) та вузькому сенсі (як цифрові об'єкти, які можна вважати різновидом майна). Цифрові активи у вузькому сенсі (або цифрові речі) – це цифрові об'єкти, які відповідають певним характеристикам, зокрема: 1) нематеріальність; 2) економічна цінність; 3) відчужуваність (можуть бути відокремлені від однієї особи та передані іншій); 4) можливість бути об'єктом контролю або конкуретоздатність (rivalrousness), тобто властивість

об'єкту, за якій він може в конкретний час контролюватися однією особою з усуненням усіх інших осіб від доступу до нього; 5) можливість повторного використання (стабільність, тривалість); 6) можливість знищення.

Положення про право власності можуть застосовуватися до цифрових об'єктів з метою найефективнішого гарантування інтересів їхніх володільців. Однак право власності на такі об'єкти буде відрізнятися від традиційної категорії права власності, що зумовлено властивостями його об'єктів. Тому доцільно запровадити категорію права цифрової власності як окремого виду права власності. Право цифрової власності матиме свій специфічний зміст та особливості здійснення. Зокрема, зміна сприйняття категорії володіння є особливо важливою в цьому контексті. Для цифрових активів володіння замінюється категорією контролю, що дозволяє відійти від класично усталеного сприйняття володіння як фізичного панування над річчю.

Ключові слова: цифрові активи, криптовалюта, цифрова річ, право власності, права користувачів, цифрова власність, володіння, майно, користувацька угода, Terms of Service, криптоактиви, NFT.

Розділ 8

ЗАХИСТ НЕМАЙНОВИХ ПРАВ У МЕДІАПРОСТОРІ В ПЕРІОД ГІБРИДНОЇ ВІЙНИ

DOI

Алла Кирилюк
кандидатка юридичних наук, доцентка

Лариса Галупова
кандидатка юридичних наук, доцентка

Особливості захисту немайнових прав у медіапросторі в період гібридної війни

У сучасному світі медіапростор став вагомим інструментом впливу на громадську думку, формування політичних наративів та конструювання соціальної реальності. В умовах гібридної війни, що передбачає поєднання традиційних військових операцій із інформаційно – психолочічними кампаніями, питання захисту немайнових прав набуває особливого значення. Інформаційні атаки, спрямовані на дискредитацію осіб, маніпуляцію свідомості та підрив довіри до державних інституцій, є не менш небезпечними, ніж фізичне насильство, оскільки їх наслідки можуть мати довготривалий вплив на осіб, національну безпеку та демократичний лад.

Загрози немайновим правам у медіапросторі під час гібридної війни виявляються у поширенні дезінформації, спотворенні фактів, незаконному використанні персональних даних, а також у цілеспрямованих кампаніях щодо приниження честі, гідності та ділової репутації осіб. Ці загрози сприяють формуванню викривленої громадської думки, маніпуляції масовою свідомістю та посиленню соціальної напруженості. В умовах гібридної війни інформаційні атаки можуть використовуватися як інструмент психологічного тиску, підриву довіри до державних інституцій та дестабілізації суспільства.

Особливістю сучасних інформаційних загроз є широке використання цифрових технологій, включаючи алгоритми штучного інтелекту для створення deepfake – контенту, автоматизовані системи поширення фейкових новин та персоналізовані атаки через соціальні мережі. У цьому контексті традиційні механізми захисту майнових прав стають недостатньо ефективними, оскільки законодавство не завжди встигає адаптуватись до нових викликів цифрової епохи. Відповідальність за порушення немайнових прав у медіапросторі під час гібридної війни залишається складним питанням, оскільки правопорушники часто користуючись тим, що в законодавстві є прогалини, діють через анонімні акаунти або спеціально створені платформи, що ускладнює притягнення їх до відповідальності. Так, держави стикаються з необхідністю балансування між свободою слова та необхідністю протифії інформаційним атакам, що вимагає нових законодавчих підходів та інструментів правозастосування.

Актуальним, на сьогоднішній день, є питання визначення та забезпечнння належного рівня захисту потерпілих від інформаційних атак. У правовій площині потерпілим від інформаційних атак слід вважати особу (фізичну чи юридичну), яка зазнала негативного впливу внаслідок поширення дезінформації, наклепу, маніпулятивних матеріалів або інших форм інформаційного впливу, що призводить до порушення її прав, завдання матеріального або моральної шкоди, а також спричиняє інші юридично значущі наслідки.

Згідно з міжнародними стандартами, такими як Резолюція Генеральної Асамблеї ООН № A/RES/75/267 щодо боротьби із дезінформацією та захисту інформаційного простору, потерпіла сторона має право на ефективний захист від інформаційних загроз, включаючи судовий захист[1]. В українській правовій площині визначення потерпілої сторони не знайшло ще свого відображення, проте у Цивільному кодексі України є норми (ст. 22, 23) щодо відшкодування збитків та моральної шкоди[2], які були завдані в тому числі і інформаційними атаками. Ключовими критеріями визначення особи потерпілою від інформаційних атак є: доведення факту поширення недостовірної

[1] United Nations General Assembly. Resolution A/RES/75/267, Combating Disinformation and Strengthening Information Space. United Nations, 2020. URL: https://undocs.org/en/A/RES/75/267

[2] Цивільний кодекс України: Закон України від 16.01.2003 № 435-IV. URL: https://zakon.rada.gov.ua/laws/show/435-15.

або маніпулятивної інформації; встановлення причинно – наслідкового зв'язку між інформаційною атакою та завданою шкодою; наявність правових підстав для притягнення винних осіб до відповідальності[1]. Особливо набуває актуальності це питання в період дії воєнного стану, коли інформаційні атаки можуть мати стратегічний характер і спрямовуватись на підрив державної стабільності. Таким чином, захист немайнових прав у медіапросторі під час гібридної війни є не лише правовою, а й національною необхідністю, що вимагає комплексного підходу, який включає вдосконалення законодавства та розвиток інструментів для боротьби з дезінформацією, а також посилення інформаційної стійкості суспільства.

Нормативно – правова база, що регулює питання немайнових прав, в тому числі в сучасному інформаційному суспільстві включає Конституцію України, яка гарантує кожному право на повагу до честі, гідності, недоторканості особистого життя (статті 3, 21, 32). Основні положення цивільно – правового регулювання немайнових прав містяться у Цивільному кодексі України, зокрема у книзі другій, що визначає загальні засади особистих немайнових прав фізичних осіб, їх зміст та способи захисту (книга друга ЦКУ). Також Закон України «Про інформацію» встановлює правові гарантії захисту інформаційної безпеки громадян та механізми відповідальності за поширення недостовірної або наклепницької інформації.

Цивілістичний аспект захисту немайнових прав у медіапросторі значною мірою визначається нормами щодо дифамації, поширення недостовірної інформації та посягання на право приватності. З даного питання важливою є практика Європейського суду з прав людини (ЄСПЛ), яка забезпечує баланс між правом на свободу вираження поглядів (ст. 10 ЄКПЛ) та правом на повагу до приватного і сімейного життя (ст. 8 ЄКПЛ). Судові рішення у справах «Axel Springer AG v. Germany»[2], «Delfi AS v. Estonia»[3], «Oliari and Others v. Italy»[4] демон-

[1] Ziccardi Giovanni. Digital Activism, Internet Control, Transparency, Censorship, Surveillance and Human Rights: An International Perspective, Chapter 6, 2012. P 201.

[2] Alex Springer AG v. Germany. no. 39954/08, ECHR 2012. URL: https://hudoc.echr.coe.int/eng#{«itemid»:[«001-152697»]}

[3] Delfi AS v. Estonia. no. 64569/09, ECHR 2015. URL: https://hudoc.echr.coe.int/eng#{«itemid»:[«001-163044»]}

[4] Oliari and Others v. Italy. nos. 18766/11 and 36030/11, ECHR 2015. URL: https://hudoc.echr.coe.int/fre#{«itemid»:[«002-10668»]}

струють підходи до розмежування критики та наклепу та особливу увагу приділено питанням визначення способу отримання достовірної інформації.

Немайнові права є однією із ключових категорій цивільного права, що особисті немайнові блага, які належать людині від народження або визначаються за нею законом. Вони не мають економічного змісту, проте їх порушення може спричинити значні негативні наслідки для особи, зокрема моральну шкоду. У цифровому середовищі, яке характеризується високою динамікою інформаційних процесів та поширенням нових технологій, немайнові права набувають особливого значення, адже їх порушення може відбуватись масово та з труднощами у притягненні правопорушників до відповідальності.

На основі аналізу ст. 270 Цивільного кодексу України[1] науковці пропонують класифікувати особисті немайнові права фізичної особи на такі, що забезпечують природне існування фізичної особи (право на життя, здоров'я, безпеку тощо), та такі, що забезпечують соціальне існування особи (право на честь, гідність, ділову репутацію, особисте життя, таємницю кореспонденції тощо)[2]. У цифровому середовищі найбільшу актуальність мають права другої групи, оскільки саме вони найчастіше порушуються шляхом поширення недостовірної інформації або маніпулятивного впливу через соціальні мережі та цифрові платформи.

Особливістю немайнових прав у цифровому середовищі є їх вразливість до інформаційних загроз. Наприклад, право на особисте життя зазнає значних порушень через неконтрольоване використання даних у соціальних мережах, незаконне стеження, витоки конфіденційної інформації. Аналогічно, право на захист честі, гідності та ділової репутації може порушуватись шляхом поширення фейкових новин, дифамаційних матеріалів, deepfake – контенту.

На міжнародному рівні регулювання немайнових прав у цифровом середовищі здійснюється через Європейську конвенцію з прав людини (ст. 8 «право на повагу до приватного і сімейного життя»;

---

[1] Цивільний кодекс України: Закон України від 16.01.2003 № 435-IV. URL: https://zakon.rada.gov.ua/laws/show/435-15

[2] Юркевич Ю. М., Дутко А. О. та ін. Особисті немайнові права особи: навч. посібн. За ред. А. О. Дутко. Львів: *Львівський державний університет внутрішніх справ*, 2021. 444 с.

ст. 10 «свобода вираження поглядів»)[1]. Європейський суд з прав людини у рішенні «Delfi AS v. Estonia» підкреслив, що онлайн – платформи можуть нести відповідальність за поширення дифамаційного контенту, навіть якщо вони є лише посередниками[2]. Це рішення є важливим для розуміння меж між свободою слова та необхідністю захисту особистих немайнових прав у цифровому просторі. Отже, рішення у справі «Delfi AS v. Estonia» створило прецедент щодо відповідальності онлайн – платформ за поширення незаконного контенту, зокрема дифамаційних висловлювань користувачів. Європейський суд з прав людини зазначив, що навіть за відсутності безпосередньої участі у створенні контенту, платформи можуть бути відповідальними, якщо вони не вживають достатніх заходів для його видалення. Цей підхід має фундаментальне значення для формування стандартів відповідальності у сфері цифрових комунікацій.

З одного боку, таке рішення зміцнює захист честі, гідності та репутації осіб у мережі, встановлюючи обов'язок платформ діяти не лише як нейтральні посередники, але і як активні суб'єкти цифрової екосистеми, здатні попереджати та припиняти правопорушення. Відсутність ефективного контролю за контентом може сприяти порушенню особистих немайнових прав, поширенню мови ворожнечі та маніпуляцій громадською думкою.

З іншого боку, надмірне покладання відповідальності на онлайн – платформи може викликати ризики для свободи вираження думок в цифровому середовищі. У ситуаціях, коли механізми модерації будуть застосовуватися надмірно жорстко, це може призвести до цензури, унеможливлення конструктивної критики або обмеження плюралізму думок. Таким чином, баланс між захистом особистих немайнових прав і свободою слова потребує чітких правових механізмів та пропорційності заходів обмеження.

Юридично значущою відповіддю на ці виклики став Акт про цифрові послуги (Digital Services Act, DSA), який регламентує обов'язки онлайн – платформ у сфері модерації контенту та забезпечує механізми правового захисту для осіб, чиї права порушені. Важливим елементом DSA є запровадження категоризації платформ за рівнем

[1] Європейська конвенція з прав людини. URL: https://www.echr.coe.int/Documents/Convention_UKR.pdf

[2] Delfi AS v. Estonia. no. 64569/09, ECHR 2015. URL: https://hudoc.echr.coe.int/eng#{«itemid»:[«001-163044»]}

впливу, що дозволяє встановлювати диференційовану відповідальність залежно від масштабу діяльності. Так, розрізняють кілька категорій платформ, які мають різний рівень зобов'язань, відповідно до масштабів їх діяльності та потенційного впливу на цифровий простір.

Найменші онлайн – сервіси, зокрема малі та мікроплатформи, мають не великий вплив на суспільний дискурс і тому звільняються від частин вимог, що містяться в DSA. До прикладу, вони не зобов'язані впроваджувати складні механізми контролю за контентом, однак повинні мати базові системи реагування на поширення незаконної інформації.

Онлайн – платформи середнього масштабу, які мають значну кількість користувачів, але не досягають критеріїв «дуже великих онлайн – платформ», повинні забезпечувати ефективні механізми модерації контенту, гарантувати прозорість алгоритмів рекомендацій та створювати систему оскарження рішень щодо блокування матеріалів.

Найсуворіші вимоги висуваються до *дуже великих онлайн – платформ* (Very Large Online Platforms – VLOPs) та *дуже великих онлайн – пошукових платформ* (Very Large Online Search Engines – VLOSEs), до яких належать сервіси з понад 45 мільйонами активних користувачів у ЄС на місяць, зокрема Google, Facebook (Meta), Amazon, TikTok, Twitter (X) тощо. Ці компанії несуть підвищену відповідальність за поширення інформації та мають виконувати низку додаткових зобов'язань. Зокрема, вони повинні систематично оцінювати ризики, пов'язані з маніпуляцією громадською думкою, дезінформацією та поширенням незаконного контекту[1].

Варто також зазначити, що у рішенні «M. L. and W. W. v. Germany» ЄСПЛ підтвердив, що право на приватність може превалювати над свободою слова у випадках, коли поширювана інформація стосується приватного життя особи та не має суспільної значущості[2].

Окрему категорію немайнових прав у цифровому середовищі становлять права на цифрову ідентичність та право на забуття. Регламент ЄС 2016/679 (GDPR) встановлює, що особам має право вимагати видалення своїх персональних даних, якщо вони більше не є

[1] The Digital Services Act. URL: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en

[2] M. L. and W. W. v. Germany no. 60798/10, ECHR 2018. URL: https://hudoc.echr.coe.int/eng#{«itemid»:[«002-12041»]}

необхідними для обробки, або якщо вона відкликає свою згоду на їх використання (ст. 17 GDPR)[1]. Таке положення є ключовим для забезпечення інформаційної безпеки громадян та запобігання тривалому негативному впливу опублікованих у мережі відомостей.

Зміст немайнових прав у цифровому середовищі також охоплює право на інформаційну безпеку, що включає захист від цифрового переслідування (cyberstalking), онлайн – насильства (cyberbullying), а також неправомірного використання персональних зображень, голосу та біометричних даних. У рішенні ЄСПЛ «Von Hannover v. Germany» було підкреслено, що навіть публічні особи мають право на захист від втручання в їх особисте життя, особливо якщо воно не стосується суспільного інтересу[2].

Немайнові права у цифровому середовищі має також і економічний вимір, оскільки репутація фізичної чи юридичної особи може мати значну ринкову вартість. Це має велике значення для суб'єктів господарювання, коли дифамаційна кампанія, неправдива інформація або незаконне використання бренду в цифровому просторі можуть спричинити значні збитки.

Серед найбільш вразливих немайнових прав в цифровому середовищі варто виокремити право на честь, гідність, ділову репутацію, право на приватність, а також авторські права. Інформаційні атаки, маніпуляції громадською думкою, кібербулінг та порушення прав інтелектуальної власності стають інструментами впливу в медіапросторі та формує ряд викликів для механізмів ефективного захисту цих прав.

1. Право на честь, гідність і ділову репутацію є особистими немайновими правами, що гарантують захист особи від поширення неправдивої інформації, яка може принизити її соціальний статус чи іншим чином негативно позначитись на її репутації. Відповідно до відчизняного законодавства, особа в такому випадку може вимагати спростування недостовірних відомостей, які порушують її права[3]. У цифровому середовищі загрозами щодо порушення вищевказаних прав є дифамаційні кампанції, поширення фейкових новин, deepfake – контент, а також висловлювання в мережі Інтернет, що

[1] Регламент ЄС 2016/679 (GDPR). URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj

[2] Von Hannover v. Germany, ЄСПЛ (2004). URL: https://hudoc.echr.coe.int/eng?i=001-61853

[3] Цивільний кодекс України: Закон України від 16.01.2003 № 435-IV. URL: https://zakon.rada.gov.ua/laws/show/435-15

здатні маніпулювати суспільною думкою. Відповідно до практики Європейського суду з прав людини онлайн – платформи можуть нести відповідальність за розміщення образливих коментарів, якщо вони не вживають належних заходів щодо їх видалення[1].

2. Право на особисте життя гарантується ст. 32 Конституції України та ст. 8 Європейської конвенції з прав людини, що встановлює заборону на втручання у приватне життя особи без її згоди. Загрозами в медіапросторі є витоки особистих даних, незаконний збір та використання інформації, цифрове стеження та використання особистих фото чи відео без згоди особи. На рівні ЄС захист персональних даних регулюється GDPR (Регламент ЄС 2016/679), який передбачає право на видалення інформації («право на забуття») та встановлює жорсткі вимоги до збереження та обробки персональних даних та особистих відомостей про особу – власника [2].

3. Авторське право. Цифрове середовище значно ускладнює захист авторських прав, адже оригінальні твори можуть бути легко копійовані, змінені або поширені без дозволу автора та за лічені хвилини. Відповідно до Закону України «Про авторське право і суміжні права», автор має виключні права дозволяти або забороняти використання свого твору[3]. Загрозами в медіапросторі є піратство, незаконне використання контенту в соціальних мережах, та deepfake – технології, які на основі фото чи відео із зображеням реальної особи створюють інші провокаційні фото чи відео.

4. Право на ідентичність. Із розвитком цифрових технологій актуальності набуло право на цифрову ідентичність, яке включає захист особи від неправомірного використання її імені, фото, відео чи інших ідентифікаційних даних. Це право безпосередньо пов'язане з проблемою крадіжки особистості (identity theft), що використовується як для шахрайства, так і для інформаційних атак. У медіапросторі під час гібридної війни порушення цифрової ідентичності може набувати форм створення фейкових акаунтів, поширення від імені жертви маніпулятивного контенту або викривлення її публічного образу. Такі дії не лише завдають шкоди репутації та честі особи, а й можуть використовуватися для дискредитації державних діячів, ак-

[1] Delfi AS v. Estonia, ЄСПЛ (2015). URL: https://hudoc.echr.coe.int/eng?i=001-155105

[2] GDPR (Регламент ЄС 2016/679). URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj

[3] Про авторське право і суміжні права: Закон України № 2811-IX від 1 грудня 2022 року. URL: https://zakon.rada.gov.ua/laws/show/2811-20

тивістів чи журналістів, посилюючи інформаційний хаос і недовіру в суспільстві.

5. Право на свободу слова. Свобода слова є фундаментальним правом людини, закріпленим у ст. 10 Європейської конвенції з прав людини, проте її реалізація у цифровому середовищі має певні обмеження, зокрема щодо закликів до насильства або поширення дезінформації[1]. У період гібридної війни інформаційна зброя стає ключовим інструментом впливу на суспільну думку, що потребує балансування між свободою вираження поглядів та захистом від шкідливого контенту. Нерідко під прикриттям свободи слова у медіапросторі поширюється дезінформація, яка порушує немайнові права осіб, завдаючи шкоди їх честі, гідності та діловій репутації. Цілеспрямовані кампанії з маніпуляції фактами, розповсюдження неправдивих відомостей або використання персональних даних без згоди можуть мати руйнівні наслідки для окремих осіб і суспільства загалом, підриваючи довіру до правдивої інформації та демократичних інституцій.

6. Право на інформацію. Дезінформація є потужним інструментом інформаційної війни. Вона порушує права громадян на доступ до інформації, може впливати на репутацію осіб та компаній, а також маніпулювати політичними та соціальними настроями суспільства. До прикладу, рішення ЄСПЛ у справі «Cengiz and Others v. Turkey» підтвердило, що обмеження доступу до онлайн – ресурсів повинно бути пропорційним і не порушувати загальних прав громадян на отримання інформації[2].

Гібридна війна є складним феноменом сучасних міжнародних конфліктів, в яких особливе місце займають інформаційні технології. У науковій літературі гібридна війна визначається як комплексна стратегія, яка включає застосування військових, економічних, політичних, інформаційних, кібератак та інших методів з метою досягнення політичних або стратегічних цілей[3]. Така форма агресії особливо небезпечна тим, що розмиває межі між миром і війною, що ускладнює її ідентифікацію та правове регулювання.

---

[1] Європейська конвенція з прав людини. URL: https://www.echr.coe.int/Documents/Convention_UKR.pdf

[2] Cengiz and Others v. Turkey, ЄСПЛ (2015). URL: https://hudoc.echr.coe.int/eng?i=001-157460

[3] Яворська Г. М, Їжак О. І. Феномен гібридної війни. Світова гібридна війна: український фронт: *монографія* /за заг. ред. В. П. Горбуліна. Харків: Фоліо, 2017. С.19.

Гібридні методи ведення війни унеможливлюють швидку ідентифікацію агресора та ускладнюють механізми міжнародного правового реагування, що вимагає нових підходів до захисту державного суверенітету та прав людини. Одним із ключових інструментів гібридної війни є інформаційний вплив, що здійснюється через ЗМІ, соціальні мережі, дезінформаційні кампанії та спеціальні операції з психологічного тиску на суспільство. Наприклад, за даними Європейської служби зовнішніх дій (EUvsDisinfo), тільки у 2023 році було зафіксовано понад 5 000 випадків дезінформації, спрямованої проти України з боку РФ, включаючи маніпуляції щодо війни, європейської підтримки України та міграційних питань[1].

В умовах гібридної війни інформаційна агресія стала одним із ключових інструментів впливу на суспільну свідомість, політичну стабільність та міжнародні відносини. Сучасні технології дозволяють здійснювати масові інформаційні атаки, які мають деструктивний вплив на немайнові права особи, зокрема на честь, гідність, ділову репутацію, право на приватність та авторські права. До основних методів інформаційної агресії належать дезінформація, пропаганда, маніпуляції суспільною думкою, поширення фейків та використання deepfake-технологій.

Дезінформація – це навмисне поширення неправдивої або маніпулятивної інформації з метою введення аудиторії в оману, формування викривленого світогляду або підриву довіри до офіційних джерел. Головна відмінність дезінформації від звичайної неправдивої інформації (misinformation) полягає в її цілеспрямованому характері та системності.

Основні форми дезінформації:

– фальсифікація фактів – створення або перекручення інформації для формування потрібного наративу (наприклад, маніпуляції щодо війни в Україні);
– контекстуальна маніпуляція – подача правдивої інформації у викривленому контексті для зміни її сприйняття;
– селективне висвітлення – акцентування на певних аспектах подій із замовчуванням важливих деталей.

Прикладом дезінформаційної кампанії є активне використання російськими ЗМІ неправдивих фактів про конфлікт в Україні, що

[1] EUvsDisinfo – Database of Disinformation Cases. URL: https://euvsdisinfo.eu

зафіксовано в базі EUvsDisinfo[1]. Громадянам гарантується право на достовірну інформацію, а дезінформація порушує вказане право та підриває довіру до медіа, державних установ та експертної спільноти. Крім того дезінформація може вводити громадян в оману, створювати паніку, підривати стабільність суспільства, а також впливати на політичні процеси та економічну ситуації.

Пропаганда – це систематичне поширення ідей, фактів або думок з метою маніпулювання суспільною свідомістю. На відміну від дезінформації, пропаганда може містити частково правдиву інформацію, але її подача є однобокою та спрямованою на досягнення політичних або ідеологічних цілей. Так, Драбюк С. С. пропонує розглядати наступні види пропаганди залежно від сфери: культурна, інформаційна, політична[2].

Культурна пропаганда спрямована на формування певних цінностей, норм і світоглядних орієнтирів у суспільстві через мистецтво, літературу, кіно та інші засоби масової комунікації. Вона може використовуватися як для збереження національної ідентичності, так і для нав'язування чужорідних культурних моделей, що особливо актуально в умовах гібридної війни.

Інформаційна пропаганда передбачає маніпуляцію фактами, подачу однобокої або викривленої інформації з метою впливу на суспільну свідомість. Це може включати поширення дезінформації, цензуру або створення альтернативної реальності через медіа, соціальні мережі та інші цифрові платформи.

Політична пропаганда має на меті формування певних політичних уподобань, підтримку або дискредитацію владних структур, лідерів та ідеологій. Вона активно використовується під час виборчих кампаній, у міждержавних відносинах та під час конфліктів для мобілізації громадськості на підтримку конкретних рішень або дій.

Пропагандистські наративи можуть формувати суспільну думку через масові кампанії в медіа та соціальних мережах, що призводить до розколу суспільства та знищення довіри до демократичних інституцій.

Маніпуляції суспільною думкою через цифрові технології. Сучасні інформаційні технології дозволяють застосовувати складні алго-

[1] EUvsDisinfo – Database of Disinformation Cases. URL: https://euvsdisinfo.eu

[2] Драбюк С. С. Пропаганда та її види. Шляхи протидії пропаганді. *Аналітично-порівняльне правознавство.* С. 153-157. URL: https://app-journal.in.ua/wp-content/uploads/2022/05/30.pdf

ритми для цільової маніпуляції громадською думкою. Основними методами маніпуляції в цифровому середовищі є: використання ботів і тролів (автоматизовані акаунти та платні коментатори створюють ілюзію громадської думки); псевдоекспертні думки (залучення контрольованих експертів для створення альтернативних наративів); таргетована реклама в соцмережах (використовується для впливу на певні групи населення з урахуванням їхніх інтересів та політичних поглядів). Дослідження Facebook Transparency Report[1] показує, що політично мотивовані рекламні кампанії активно використовують персоналізовані алгоритми для маніпуляцій суспільною думкою.

Фейки – це повністю або часткового вигадані новини, які часто оформлюються як справжні журналітські матеріали[2]. Вони можуть містити неправдиві заяви, вигадані подіх сбо спотворені коментарі реальних осіб. На основі запронованого науковцями поняття фейків, можемо запропонувати основні його категорії:

- Клікбейтні заголовки – маніпулятивні заголовки, що змішіють користувачів, по – перше звернути увагі на таку новину, зацікаватись нею та поширити без належної перевірки;
- Фейкові сайти – веб – ресурси, які імітують ЗМІ або урядові установи;
- Інформаційні вкидки – це масоові розсилки фейкових новин через соціальні мережі або інші комунікаціні платформи.

Розвиток новітніх технологій дає можливість створювати нові фейки, які важко відрізнити від досмтовірної інформації через максимально наближене до реальності наповненя. Сьогодні, за допомогою штучного інтелекту можуть бути сворені наближені до реальності зображення будь-кого із відомих осіб (політиків, виконавців, блогерів і т.д.). Використовуючи згенероване зображення впливових осіб в потрібному інформаційному напрямку суспільство стає довіряти такій новині та стає прихильним до позиції авторитетної особи зображеної на фото чи відеоконтенті. Прикладом може бути кампанія «Pizzagate» у США, коли фейкові новини про політичну змову призвели до реальних наслідків, включаючи збройний напад[3].

---

[1] Facebook Transparency Report. URL: https://about.fb.com/news/tag/transparency-report/

[2] Фейк. Велика Українська Енциклопедія URL: https://vue.gov.ua/Фейк

[3] Pizzagate: Anatomy of a Fake News Scandal. URL: https://www.nytimes.com/2020/12/10/us/politics/pizzagate.html

Deepfake – це технологія, що дозволяє створювати реалістичні відео та аудіозаписи з підробленими обличчями або голосами. Вона базується на використанні алгоритмів глибинного навчання та використовується як для розваг, так і для маніпуляції суспільною думкою. Таким чином використання технологій deepfake може викликати певні загрози, такі як:

- Фальсифікація політичних заяв – створення відео, в яких відомі особи нібито висловлюють шкідливі або компрометуючі думки;
- Дискредитація осіб – підробка компроментуючих відео для шантажу чи репутаційної атаки;
- Маніпуляції на фондових ринках – фейкові виступи впливових осіб у сфері фінансових відносин (фінансових лідерів), які можуть впливати на курси акцій.

За даними Deeptrace Lab, у 2023 році вичявлено понад 100 000 deepfake-відео, значна частина яких використовувалася в політичних та інформаційних війнах[1].

Методи інформаційної агресії стали невід'ємною частиною сучасних конфліктів, зокрема в умовах гібридної війни. Дезінформація, пропаганда, маніпуляції суспільною думкою, поширення фейків та використання deepfake – технологій створюють серйозні загрози для демократії, прав людини та міжнародної безпеки. Для ефективної боротьби з цими викликами необхідне удосконалення законодавства, впровадження технологічних рішень для виявлення фейків та посилення цигрооі грамотності громадян.

Інформаційна війна є складовою гібридної агресії та передбачає комплексний вплив на суспільні процеси через маніпуляцію інформацією. Основна мета такої війни – дискредитація державних інституцій, створення хаосу в суспільстві та підрив довіри до демократичних цінностей. Дезінформація та пропаганда можуть спотворювати громадську думку, змінювати пріаоритети та провокувати соціальні конфлікти. Дослідження Європейської служби зовнішніх дій (EU DisinfoLab) підтверджують, що систематичні дезінформаційнв кампаніх в соціальних мережах сприяють радикалізації суспільних настроїв і формують антагоністичні групи громадян[2]. Це створює ґрунт для політичної поляризації та дестабілізації.

[1] Deeptrace Lab Report on Deepfake Trends. URL: https://www.deeptracelab.com/reports
[2] EU DisinfoLab. URL: https://www.disinfo.eu

Одним із ключових прав людини є право отримання достовірної інформації. Проте в умлвах інформаційної війни це право часто порушується через самове поширення фейків, маніпуляцій та викревлення фактів. Сучасні алгоритми штучного інтелекту сприяють поширенню дезінформації, оскільки контент із сенсаційними заголовками та емоційно забарвленими повідомленнями має вищу вірусність. Це призводить до того, що неправдива інформація поширюється швидше, ніж спростування або об'єктивний аналіз.

Згідно з дослідженням Массачусетського технологічного інституту фейкові новини поширюються у Twitter в шість разів швидше, ніж правдива інформація[1]. Це означає, що громадяни, навіть не бажаючи того, стають жертвами інформаційних атак і маніпуляцій.

З одного боку, інформаційна війна створює ілюзію свободи слова, оскільки всі можуть висловлювати свою думку в цифровому просторі. З іншого боку, масові дезінформаційні кампанії та «фабрики тролів» навмисно створюють токсичне середовище для вільного обміну думками. На сьогоднішній день, основні загрозами свободі слова в умовах інформаційної війни є: *координаційні атаки (mass reporting*), які здійснюються організованими групами користувачів, які масово скаржаться на контент або акаунт незалежних журналістів, активістів, блогерів задля того, щоб їх заблокували.; *кібербулінг або погрози* – націлені на залякування осіб, які поширюють незручну для агресора правду; *автоцензура* – громадяни уникають висловлення своєї думки через страх репресій чи соціального тиску. Наприклад, за даними дослідження Freedom House, рівень інтернет-свободи у світі знижується п'ятий рік поспіль, зокрема через урядові маніпуляції та інформаційні війни[2].

Крім викликів, що становить гібридна війна для інформаціного поля та медіа простору, вона загрожу' порушенням прав інтелектуалбної власності. При цьому, в період гібридної війни порушення прав на результати інтелектуальної творчої діяльності носить массовий та систематичний характер. Наслідки порушення прав на твори науки, літератури та мистецтва можуть зачіпати наступні категорії осіб:

[1] MIT Study on Fake News Spread. URL: https://news.mit.edu/2018/study-twitter-false-news-travels-faster-true-stories-0308

[2] Freedom House Internet Freedom Report. URL: https://freedomhouse.org/report/freedom-net

1. Автори творів науки, літератури та мистецтва. Авторами творів можуть бути фізичні особи, які своєю творчею працеюс творили твір. До даної категорії осіб можуть відноситись журналісти, блогери, які створюють новий оригінальний та творчий контент. Такий контент може бути використаний без дозволу правовласників або привласнений повністю або частково. Крім того, до даної категорії осіб можуть відноситись художники, фотографи або музиканти, творчі здобутки яких можуть бути використані для створення пропагандистських цілей або для поширення фейків та deepfake. Окремою категорією є науковці, які здійснюють фундаментальні чи прикладні дослідження та наукові здобутки яких можуть бути використані, спотворені чи перекручені для пропагандистських цілей або поширення фейків.

2. Правонаступники. Зазначені суб'єкти є вторинними, тому їм належать майнові права інтелектуальної власності. До даної групи осіб можуть належати як фізичні так і юридичні особи. Вторинними є суб'єкти права інтелектуальної власності, яким було передано право на використання результату інтелектуальної творчої діяльності. Якщо при використання творів першої категорії осіб, мова йде про порушення як майнових так і немайнових права авторів, то при використанні творів правонаступників, можуть бути порушені їх майнові права. При цьому, необхідно підкреслити, щи використання об'єктів авторського права в інформаційній війні може як порушувати права інтелектуальної власності так і зачіпати інтереси суб'єктів цих прав. Так використання твору, авторські права на які належить правонаступнику може зачіпати право на ділову репутацію, якщо твір буде використовуватись для фейкових новин або буде взятий за основу при створенні deepfake. Порушення авторських прав у медіапросторі також є серйозною проблемою, оскільки воно підриває довіру до первинних джерел інформації та доброчесних правоволодільців.

Крім того, в умовах сьогодення, постає питання про те, чи можуть такі твори підпадати під правову охорону як об'єкти авторського права, якщо вони відповідають критеріям охороноздатності, але водночас їхнє призначення полягає у маніпуляції суспільною свідомістю або поширенні дезінформації.

Відповідно до міжнародних стандартів, зокрема Бернської конвенції про охорону літературних і художніх творів, авторське право надається будь-якому твору, що є оригінальним результатом творчої

діяльності. Законодавства більшості країн світу не містить положень щодо вимоги правдивості чи соціальної корисності твору для надання йому охорони. Це означає, що навіть твори, які містять дезінформацію або пропаганду, формально можуть підпадати під охорону, якщо вони відповідають критеріям оригінальності та творчого характеру. Попри загальну концепцію нейтральності авторського права щодо змісту творів, існує низка дискусійних питань. У деяких правових системах (наприклад, у праві Франції та Німеччини) діє принцип «ordre public», який може обмежувати правову охорону творів, що суперечать сусіпльним цінностям та моральним принципам. Якщо фейк має на меті ввести в оману громадськість, його охорона може бути поставлена під сумнів. Якщо фейковий контент є механічним відтворенням фактів без значної творчої обробки, він може не відповідати критерію оригінальності, необхідному для авторсько – правової охорони. Якщо авторське право на фейкові твори використовується для недобросовісного обмеження поширення достовірної інформації (наприклад, через масові скарги на видалення матеріалів із соціальних мереж), це може бути підставою для обмеження охорони таких творів у судовому порядку.

На сьогоднішній день не вснує єдиного законодавчо встановленого підходу до вирішення даного дискусійного питання. Закон «Про авторське право та суміжні права» не містить прямої заборони щодо охорони творів, які містять заклики по насильства, зміни державного устрою та територіальної цілісності при цьому кримінальний кодекс визначає відповідальність за вчинення таких дій, однією із таких санкцій може бути вилучення примірників із цивільного обігу. Проблема правової охорони фейкових творів і пропагандистських матеріалів є складною та багатоаспектною. Відсутність правдивості як критерію для надання охорони у традиційному авторському праві створює потенційні ризики зловживань. Однак, з іншого боку, занадто жорсткі обмеження можуть створити небезпеку цензури та надмірного контролю над контентом.

Отже, в Україні захист немайнових прав у медіапросторі регулюється комплексом нормативно – правових актів, що забезпечують охорону честі, гідності та ділової репутації громадян. Конституція України гарантує кожному право на повагу до його гідності та честі. Зокрема, стаття 28 Основного Закону проголошує: «Кожен має право

на повагу до його гідності». Це положення закладає фундамент для захисту особистих немайнових прав громадян у всіх сферах суспільного життя, включно з медіапростором.

Цивільний кодекс України деталізує механізми захисту немайнових прав. Стаття 277 ЦК України передбачає право особи на спростування недостовірної інформації, яка порочить її честь, гідність або ділову репутацію. У випадку поширення такої інформації особа має право вимагати її спростування та відшкодування моральної шкоди. Важливо зазначити, що обов'язок доведення достовірності поширеної інформації покладається на відповідача, тобто на особу, яка цю інформацію поширила. Це положення спрямоване на забезпечення ефективного захисту прав потерпілої сторони та стимулює відповідальне ставлення до поширення інформації в медіапросторі.

Окрім загальних норм, в Україні діють спеціальні закони, що регулюють діяльність засобів масової інформації та визначають відповідальність за порушення немайнових прав. Закон України «Про інформацію» встановлює правові основи інформаційної діяльності та гарантує право кожного на інформацію, одночасно визначаючи обмеження щодо поширення відомостей, які можуть завдати шкоди честі, гідності або діловій репутації особи. Зокрема, стаття 31 цього закону забороняє поширення інформації, яка порушує особисті немайнові права громадян. Це положення сприяє формуванню відповідального інформаційного середовища та захищає громадян від неправомірних посягань на їхню репутацію.

Закон України «Про телебачення і радіомовлення» регулює відносини між суб'єктами діяльності в галузі телебачення і радіомовлення незалежно від їхньої форми власності, мети створення, виду статутної діяльності, а також від способу розповсюдження телерадіопрограм та передач, розрахованих на масове приймання споживачами. Держава, через засоби телебачення та радіомовлення, гарантує право на інформації. При цьому ст. 59 Закону містить положення яке вказує, що елерадіоорганізація зобов'язана поширювати достовірну інформацію, а разі поширення недостовірної інформації – розмістити спростування поширеної інформації, визнаної недостовірною, наклепницькою тощо. Таке положення забезпечує оперативне відновлення порушених прав та мінімізує негативний вплив неправдивих відомостей на репутацію особи.

Однак, незважаючи на наявність розвиненої нормативно-правової бази, на практиці виникають певні проблеми. Однією з них є відсутність чіткого визначення поняття «недостовірна інформація» в законодавстві, що ускладнює процес доведення факту порушення в суді. Крім того, швидкий розвиток цифрових технологій та анонімність в Інтернеті створюють додаткові виклики для захисту немайнових прав у медіапросторі. Тому необхідно постійно вдосконалювати законодавство та адаптувати його до сучасних реалій інформаційного суспільства.

У підсумку, нормативно – правова база України щодо захисту немайнових прав у медіапросторі є комплексною та багаторівневою, охоплюючи конституційні гарантії, положення цивільного законодавства та спеціалізовані нормативні акти. Ефективна реалізація цих норм вимагає не лише їхнього дотримання, але й постійного оновлення та вдосконалення відповідно до викликів сучасного інформаційного середовища.

Сучасні цифрові технології значно розширюють можливості поширення інформації, водночас створюючи нові загрози для репутації, приватності та авторських прав громадян. Масові інформаційні атаки, кампанії дискредитації, використання фейкових акаунтів та deepfake-технологій стали потужним інструментом маніпуляцій, що використовується як у політичних, так і в комерційних цілях. У таких умовах особи, які стають жертвами інформаційних нападів, мають діяти швидко та ефективно, використовуючи всі доступні юридичні та технічні засоби для захисту своїх прав.

Одним із ключових механізмів є звернення до цифрових платформ, на яких було поширено неправомірний контент. Відповідно до норм міжнародного та національного законодавства, більшість соціальних мереж та онлайн-ресурсів передбачають процедуру подання скарг на неправомірний контент, що порушує честь, гідність чи приватне життя особи. Однак практика показує, що не завжди такі звернення є ефективними, оскільки алгоритми модерації часто діють вибірково, а адміністрації платформ не завжди оперативно реагують на порушення. Крім того, деякі матеріали можуть бути розповсюджені на ресурсах, які не мають ефективної процедури видалення контенту або перебувають у юрисдикціях, де правове регулювання подібних питань є слабким або відсутнім.

У таких випадках необхідно звертатися до суду за захистом свої немайнових прав та з вимогою про спростування недостовірної інформації та відшкодування моральної шкоди. Проте судові процеси є довготривалими, що створює додаткові труднощі для осіб, чиї права були порушені. Крім того, судочинство грунтується на принципі відкритості судового процесу. Інколи особи не бажать розголосу порушення своїх прав, які пов'язані із честю, гідністю та репутацією. Особливо у випадках, коли особа є відомою, такі судові засідання привертають увагу журналістів та активістів. Такі спори стають обговорювані суспільством та можуть нести небажаний ефект для позивачів. Саме тому, на нашу думку актуальним та ефективним способам захисту особистих немайнових прав є звернення до медіації як альтернативного способу вирішення спору. Медіація є ефективним інструментом вирішення конфліктів щодо особистих немайнових прав, оскільки вона дозволяє сторонам знайти взаємоприйнятне рішення без звернення до суду, зберігаючи при цьому довірчі відносини та мінімізуючи публічний розголос. Однією з ключових переваг медіації є її конфіденційність, що особливо важливо у справах, пов'язаних із захистом честі, гідності та ділової репутації, де публічне судове розглядання може ще більше загострити конфлікт.

Додатковою перевагою є швидкість та економічність цього методу порівняно з судовим процесом. Судові спори щодо немайнових прав можуть тривати роками, тоді як медіація дозволяє досягти результату в стислі строки без значних фінансових витрат[1]. Важливим аспектом є також гнучкість процесу: сторони самостійно визначають умови врегулювання спору та можуть знаходити нестандартні рішення, які суд не зміг би ухвалити в силу законодавчих обмежень. Крім того, рішення, досягнуті в межах медіації, мають значно більший рівень добровільного виконання, оскільки сторони самі беруть участь у їх виробленні, а не отримують примусове рішення суду.

Медіація як альтернативний спосіб врегулювання конфліктів у сфері немайнових прав у медіапросторі є ефективним інструментом, що дозволяє досягти балансу між правовою захищеністю особи та оперативністю врегулювання конфлікту. Визначення більше ефективного спсобу захисту немайнових прав в медіапро-

[1] Галупова Л. І. Альтернативні способи врегулювання конфліктів у сфері права інтелектуальної власності: дис.... канд. юрид. наук: 12.00.03. Одеса, 2021. 207 с. С. 122.

сторі обумовлено складністю правовілносин, характером порушення прав та готовністю сторін до компромісного врегулювання кофнлікту.

Спори щодо честі, гідності та ділової репутації, які виникають внаслідок поширення оціночних суджень, критичних висловлювань або непідтверджених відомостей, можуть бути ефективно врегульовані шляхом медіації, оскільки сторони часто зацікавлені саме в конфіденційному та швидкому врегулюванні спору та недопущенні ескалації конфлікту. Медіація в даному випадкудозволяє уникнути додаткового розголосу, забезпечити добровільне спростування або уточнення поширеної інформаціх, а також узгодити питання компенсації моральної шкоди без тривалого судового процесу. У випадку коли йдеться про систематичну дифамацію або наклеп, що завдає істотної шкоди для репутації судовий розгляд є доцільним, оскільки суд може ухвалити рішення про офіційне спростування та стягнення компенсації.

Особливої актуальності набувають спори щодо порушення права на власний образ і голос (право на індивідуалізацію), зумовлені використанням фото-, відеоматеріалів або аудіозаписів, що ідентифікують особу без її дозволу. У разі, якщо публікація здійснена без наміру завдати шкоди або особа не розуміла наслідків для особистих немайнових прав, а сторона, що поширила контент, готова до переговорів, медіація є ефективним способом досягнення згоди щодо видалення, редагування чи належного маркування матеріалів. Водночас, коли йдеться про використання образу особи в комерційних цілях без згоди, що має безпосередні фінансові наслідки, судовий захист забезпечує належну правову охорону інтелерів потерпілої сторони та дозволяє допомогти припинення правопорушення або стягнення матеріальної компенсації.

Медіація також є ефективним способам врегулювання конфліктів щодо авторського права. Так, конфлікт щодо авторських прав може виникати при присвоєнні авторства. Розголошення інформації про подібні випадки може нести негативні наслідки як для автора – доброчесного творця нового оригінального об'єкта, так і для особи яка вчинила порушення, оскільки це може вплинути на репутацію обох сторін. Тому, медіація дає можливість конфіденційно та без шкоди для честі та репутації сторін врегулювати конфлікт. Однак у випад-

ках, коли сторони не можуть знайти компроміс а мирним шляхом врегулювати конфлікт, судовий розгляд є необхідним механізмом правового захисту, що забезпечує можливість притягнення порушника до відповідальності.

Конфлікти між журналістами, блогерами, медіа та публічними особами є особливо чутливими, оскільки зачіпають баланс між свободою слова та захистом немайнових прав. У цьому контексті медіація дозволяє уникнути довготривалого судового процесу та знайти компромісне рішення, що враховує як потребу у збереженні правдивості та об'єктивності журналістських матеріалів, так і право особи на захист від безпідставних звинувачень. Разом із тим, у випадках, коли розповсюджена інформація має ознаки зловмисної маніпуляції або є частиною систематичної інформаційної кампанії, судовий розгляд є доцільнішим, оскільки лише суд може ухвалити рішення, яке матиме обов'язкову силу.

Окремо слід розглядати спори, пов'язані з кібербулінгом та поширенням дезінформації, що завдають шкоди психологічному стану потерпілої сторони. Медіація може бути ефективним інструментом, якщо конфлікт виник між приватними особами та є наслідком непорозумінь або необережної поведінки в соціальних мережах. Проте, коли йдеться про систематичні атаки, мову ворожнечі або погрози, судове втручання є необхідним, оскільки лише через суд можна забезпечити правовий механізм притягнення винних до відповідальності та застосування санкцій відповідно до законодавства.

Враховуючи специфіку немайнових прав у медіапросторі, вибір між медіацією та судовим розглядом має ґрунтуватися на таких ключових критеріях: характер та масштаб порушення, наявність конструктивного діалогу між сторонами, суспільний інтерес до справи, можливість конфіденційного врегулювання та необхідність юридично обов'язкового рішення. Якщо сторони зацікавлені у швидкому врегулюванні спору без значних фінансових витрат та публічного розголосу, медіація є пріоритетним механізмом. У випадках, коли порушення має системний або загрозливий характер, а правопорушник не виявляє готовності до співпраці, судовий розгляд є єдиним ефективним способом захисту прав потерпілої сторони.

Відповідальність користувачів за поширення неправдивої інформації

Розвиток цифрових технологій та Інтернет-середовища ставить перед урядами країн та міжнародними організаціями нові виклики в контексті забезпечення безпеки в Інтернеті та запобігання поширенню недостовірної інформації. У цьому контексті особливу увагу привертають правові ініціативи, що спрямовані на регулювання діяльності Інтернет-платформ і посередників, зокрема в частині боротьби з кіберзагрозами, дезінформацією та іншими небезпеками. Однак, на жаль, існуюче законодавство все ще значною мірою відстає від швидкості розвитку технологій, що ускладнює ефективне врегулювання таких питань.

Європейський Союз став однією з провідних юрисдикцій у світі щодо розробки та впровадження цифрового законодавства, орієнтуючись на захист прав людини, громадян і забезпечення безпеки в Інтернеті. У зв'язку з різними соціальними та економічними ризиками для користувачів, були розроблені кілька важливих нормативних актів:

а) Акт про цифрові послуги (Digital Services Act, DSA) є ключовим документом для регулювання діяльності онлайн-платформ у ЄС. Основною метою DSA є забезпечення безпеки користувачів, запобігання поширенню незаконного контенту та боротьба з дезінформацією, а також прозорість дій платформ. Платформи повинні мати механізми для швидкого видалення контенту, який порушує закони ЄС, зокрема, контент, що стосується тероризму, насильства, дитячої порнографії або дезінформації. Користувачі, чиї матеріали були видалені, можуть оскаржити це рішення, що сприяє прозорості та захисту їхніх прав. Також, платформи повинні мати чітко прописані засоби модерації контенту та надавати користувачам можливість контролювати алгоритми.

б) Акт про цифрові ринки (Digital Markets Act, DMA) – розроблений для того, щоб покращити конкуренцію в цифровій індустрії, а також захистити основні права споживачів. Цей акт орієнтований на врегулювання діяльності великих технологічних компаній, які контролюють значну частину ринку цифрових послуг. Його мета – забезпечити рівні умови для конкуренції в Інтернет-просторі, обмежити антиконкурентні практики і забезпечити більшу прозорість.

в) Загальний регламент захисту даних (GDPR) є стандартом для захисту персональних даних в ЄС. Це один з найсуворіших і найпередовіших правових актів у світі, який встановлює високі вимоги до обробки персональних даних, зокрема в Інтернет-просторі. Закон дає громадянам право контролювати свої персональні дані та захищає їх від різного роду зловживань.

Україна також активно працює над створенням правового поля, яке б забезпечувало безпеку в цифровому просторі та захищало громадян від кіберзагроз. Зупинимося на основних нормативно-правових актах:

а) Закон України «Про основні засади забезпечення кібербезпеки України» – визначає загальні принципи кібербезпеки в Україні, зокрема захист критичної інфраструктури, моніторинг і реагування на кіберзагрози. Закон передбачає створення національної системи кібербезпеки, яка буде здійснювати захист від кіберзлочинців та кібертероризму.

б) Закон України «Про захист персональних даних» – визначає вимоги щодо обробки та захисту персональних даних громадян та спрямований на захист основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя, у зв'язку з обробкою персональних даних. Це дозволяє створити більш безпечне середовище для користувачів Інтернету, адже особиста інформація не може бути використана без їхнього дозволу. Однак, для досягнення ефективної захищеності персональних даних Україні необхідно враховувати міжнародний досвід, зокрема стандарт GDPR.

в) Закон України «Про електронну комерцію» – встановлює правила для діяльності в Інтернеті, включаючи питання онлайн-торгівлі, захисту прав споживачів і забезпечення безпеки фінансових операцій через Інтернет[1].

г) Закон України «Про боротьбу з тероризмом» – встановлює основи для боротьби з тероризмом, захисту критичної інфраструктури і протидії цифровим загрозам з боку терористичних організацій.

Згідно зі статтею 32 Конституції України, кожна особа має право на судовий захист від неправдивої інформації щодо себе та своєї родини, вимагати її спростування та видалення, а також на компен-

[1] Про електронну комерцію: Закон України від 03.09.2015 р. № 675-VIII. URL: https://zakon.rada.gov.ua/laws/show/675-19#Text

сацію шкоди, завданої поширенням недостовірних відомостей. Крім того, кожен має гарантоване право на свободу думки та вираження своїх переконань, а також на вільне висловлювання своїх поглядів. Право на вільне вираження думок гарантоване частинами 1 та 2 статті 34 Конституції України, згідно з якими кожен має право вільно збирати, зберігати, використовувати та поширювати інформацію в усній, письмовій або будь-якій іншій формі на свій розсуд. Жодна ідеологія не може бути визнана державою як обов'язкова. При цьому поширення такої інформації повинно відповідати законодавчим вимогам щодо її достовірності та не порушувати права інших осіб[1]. Головною проблемою при визнанні інформації недостовірною та її спростуванні в суді є знаходження розумного балансу між правом на свободу думки та вираження поглядів і правом кожної особи на захист своєї гідності та честі[2].

Згідно зі статтею 10 Конвенції про захист прав людини і основоположних свобод 1950 року, а також Першим протоколом і Протоколами № 2, 4, 7, 11 до цієї Конвенції, кожна особа має право на свободу вираження думок[3]. Це право визнається в ЄС як важлива цінність, що має велике значення для функціонування демократичного суспільства. Отже, кожному гарантується свобода дотримуватися власних поглядів, отримувати та поширювати інформацію і ідеї без втручання державних органів, незалежно від кордонів. Водночас, свобода слова охоплює не лише інформацію, яка є належно отриманою або не викликає образи, а й відомості, які можуть спричинити обурення, образу чи занепокоєння.

Хоча особа має право вільно здійснювати свої цивільні права на власний розсуд (ст. 12 ЦК України), вона повинна робити це в межах, визначених договором або актами цивільного законодавства, та утримуватися від вчинення дій, які можуть порушити права інших осіб (ст. 13 ЦК України). У демократичному суспільстві свободи можуть бути обмежені законодавчими нормами, якщо це необхідно для захисту національної безпеки, територіальної цілісності, громадського

[1] Конституція України: Закон України від 28.06.1996 № 254к/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text

[2] Рішення Європейського суду з прав людини у справі «Українська прес-група» проти України» від 29.03.2005. URL: https://ips.ligazakon.net/document/SO1052

[3] Конвенція про захист прав людини і основоположних свобод: ратифіковано Законом № 475/97-ВР від 17.07.97. URL: https://zakon.rada.gov.ua/laws/show/995_004

порядку, запобігання злочинам, охорони здоров'я, моралі, прав інших осіб або авторитету правосуддя.

Отже, кожна особа має право вільно збирати, зберігати, використовувати та поширювати інформацію (ст. 302 ЦК України)[1]. Подібне положення міститься і в ст. 5 Закону України «Про інформацію», де право на інформацію передбачає можливість її вільного отримання, використання, поширення, зберігання та захисту для реалізації своїх прав, свобод і законних інтересів[2]. Проте поширення такої інформації повинно відбуватись відповідно до законодавчих вимог щодо її достовірності. Таким чином, кореспондуючим обов'язком до права на свободу думки і слова є обов'язок не поширювати недостовірну інформацію про інших осіб, факти чи події.

Інформація, яка поширена з порушенням цієї вимоги, визнається недостовірною. Так, у своїй постанові від 27 лютого 2009 року № 1 «Про судову практику у справах про захист гідності та честі фізичної особи, а також ділової репутації фізичної та юридичної особи» Пленум Верховного Суду України зазначив, що праву на свободу думки та вираження поглядів відповідає обов'язок не поширювати недостовірну інформацію, а також таку, що принижує гідність, честь чи ділову репутацію особи[3].

У правовій доктрині терміни «недостовірна інформація» та «неправдива інформація» нерідко використовуються як синоніми, проте вони мають суттєві відмінності як у змістовому, так і в юридичному аспектах.

Недостовірна інформація – це дані, які не мають належного підтвердження або обґрунтування. Її поширення може бути результатом помилки, недостатньої перевірки фактів або ненадійності джерел. Недостовірність такої інформації полягає в неможливості встановлення її відповідності дійсності на момент публікації. Зазвичай її

---

[1] Цивільний кодекс України: Закон України від 16.01.2003 № 435-IV. URL: https://zakon.rada.gov.ua/laws/show/435-15#Text

[2] Про інформацію: Закон України від 02.10.1992 № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text

[3] Про судову практику у справах про захист гідності та честі фізичної особи, а також ділової репутації фізичної та юридичної особи: Постанова Пленуму Верховного Суду України від 27.02.09 р. № 1. URL: https://ips.ligazakon.net/document/view/VS090016?utm_source=jurliga.ligazakon.net&utm_medium=news&utm_content=jl03&_ga=2.225057370.1733520195.1725937230-537030540.1723262605#_gl=1*wxm5o6*_gcl_au*MTMwODM3MDgzNi4xNzIzMjYyNjA0

не поширюють із метою обману, а радше через необачність чи недбалість у зборі та аналізі відомостей.

Неправдива інформація, своєю чергою, є відомостями, які не відповідають дійсності та мають свідомо викривлений або вигаданий характер. Основною відмінною рисою такої інформації є її завідомо хибний зміст, що може мати на меті маніпуляцію, введення в оману або дискредитацію певних осіб чи явищ. Поширення неправдивої інформації може нести правові наслідки, зокрема у випадках наклепу, дезінформації або поширення фейкових новин.

З точки розу правоих наслідків, неправдива інформація може завдавати шкоди честі, гідності, діловій репутації або громадському порядку. Водночас недостовірна інформація також може мати негативні наслідки, проте вона частіше піддається спростуванню або коригуванню.

Таким чином, неправдива інформація є однією із форм проявів недостовірної інформації, але не вся недостовірна інформація є свідомо неправдивою. Правова оцінка цих понять залежить від контексту, ступеня доведеності недостовірності та можливих наслідків її поширення.

Недостовірною є інформація, яка не відповідає реальності або викладена неправдиво, тобто містить відомості про події та явища, що не мали місця, або які відбулися, але інформація про них є неточною (неповною чи спотвореною)[1].

Недостовірна інформація може мати різні форми, від неправдивого чи оманливого контенту, який поширюється з наміром ввести в оману або здобути політичну чи економічну вигоду, до матеріалів, які завдають шкоди суспільству – це можуть бути пости в соціальних мережах (пропаганда, містифікації, фішинг), мультимедійні лонгріди чи неправдиві повідомлення, які поширюються без зловмисних намірів, хоча й мають шкідливі наслідки (чутки, образи, жарти). Проте найбільший руйнівний потенціал мають діпфейки (deepfakes), які не лише суперечать об'єктивному відображенню подій, але й можуть замінювати реальність. Діпфейки дозволяють створювати аудіо- та відеоматеріали, в яких використовується голос і (або) зображення

[1] Гришанова Н. Розповсюдження недостовірної інформації: яка відповідальність передбачена. 2021 р. URL: https://jurliga.ligazakon.net/news/203326_rozpovsyudzhennya-nedostovrno-nformats-yaka-vdpovdalnst-peredbachena

іншої людини. Ця технологія доступна кожному власнику смартфона, і за допомогою таких додатків, як FaceApp, ReFaceApp, FaceMagic тощо, можна створити діпфейк за дуже короткий час.

Технологія діпфейку може бути застосована в різних сферах політичної боротьби, зокрема для дискредитації окремих осіб, формування хибних уявлень у громадськості щодо певних подій чи процесів, а також для підробки доказів у судових справах. Таке використання технології завжди порушує права на свободу слова і самовираження, право на приватність, доступ до інформації та інші основні права.

Інформація є конструкцією реальності та однією з соціальних цінностей, тому неправдиві відомості, що не відповідають дійсності, можуть призвести до спотвореного сприйняття реальності у людини. Відповідальність за поширення недостовірної інформації в соціальних мережах ускладнюється через специфіку Інтернету, де інформація поширюється через різні ресурси. Сучасні технології дозволяють інформації поширюватися швидко, різними способами, у різних формах та обсягах, незалежно від відстані і державних кордонів, стаючи доступною мільйонам людей за лічені хвилини. З одного боку, це реалізація свободи слова та права на поширення, передачу й отримання інформації. З іншого – це створення ризиків і небезпек для прав людини через маніпуляції, збір персональних даних та поширення недостовірних відомостей. На жаль, держава і суспільство виявились неготовими до стрімкого розвитку глобальної мережі, і як правова наука, так і законодавство в цій сфері відстають. Хоча існують правові механізми захисту, їх не можна назвати ефективними та вдосконаленими – багато випадків поширення відомостей, що принижують честь і гідність, залишаються безкарними.

Способи поширення інформації в сьогоднішніх реаліях дуже різноманітні. Відмінними рисами сучасної цивілізації є розвиток інформаційних систем та глобалізація комунікаційного простору. Сьогодні Інтернет-технології увійшли абсолютно у всі сфери суспільного життя. На жаль, у цифровому світі практично неможливо уникнути зіткнення з фейковими новинами та великою кількістю різних типів дезинформації в Інтернеті, які справедливо характеризуються вченими як виклики цифрового медіапростору.

Дезінформація в Інтернеті залежить від мотивації тих, хто розповсюджує хибні новини. Це може бути пропаганда, метою якої є вве-

дення аудиторії в оману та просування політичної програми або упередженої точки зору через спотворення фактів та надання неправдивої інформації. Не менш поширена і журналістика низької якості, причини якої є різними. Зокрема, у бажанні збільшити кількість аудиторії та заробітком грошей, а часом і проведенням власного піару вони не приділяють належної уваги перевірці фактів перед публікацією, внаслідок чого їхні помилки можуть спричинити поширення фейкових новин.

Дуже поширене також використання «клікбейтів» або заголовків, що вводять в оману, чим привертають увагу значної аудиторії. Для цього достатньо використати сенсаційний заголовок або обурливу тему, що має суспільний резонанс. Для «підігрівання» інтересу аудиторії до деяких новин такі ЗМІ часто гіперболізують достовірну інформацію, використовують фальшиві факти або гучні заголовки.

Нерідко фейкова інформація розповсюджується через фальшиві сайти новин, які створюються шахраями. Зовнішній вигляд таких сайтів максимально нагадує вигляд справжніх, що має викликати довіру користувачів. Фейкові новини в соціальних мережах також можуть поширюватися ботами, які масово випускають статті незалежно від надійності їх джерел. Вони можуть створювати підроблені акаунти, на які накручуються підписники.

Наслідки поширення фейкових новин можуть бути досить серйозними і нести в собі низку небезпек, у тому числі:

– розпалювання та загострення соціальних конфліктів, підрив засад національної безпеки;
– дезінформація, що призводить до відчуття, що не можна вірити всьому, що читаємо. Безумовно, це підриває довіру до серйозних джерел новин;
– вплив на психоемоційну поведінку людини, що вганяє в паніку та підштовхує до вчинення нерозумних, необдуманих, а іноді навіть небезпечних вчинків.

Особливе загострення питання про поширення фейкових новин та фейкову інформацію про діяльність держав і представників влади набуло в період пандемії нової коронавірусної інфекції. В силу особливостей нового захворювання, а також прискорених темпів розробки вакцин та проведення програм вакцинації особливу популярність набули фейки антидержавного характеру, як правило, двох видів:

– антидержавні фейки, що дискредитують вакцинацію та вводять категорії небезпечних/шкідливих вакцин, – мала місце так звана антивакцинаторська пропаганда;
– антидержавні фейки, які дискредитують державну систему як нездатну впоратися з новою інфекційною небезпекою.

Багато країн (зокрема, Китай, Сінгапур) стали на законодавчому рівні вводити обмеження щодо ЗМІ за поширення фейків про коронавірусну інфекцію та особливості протистояння їй.

Вже на стадії пандемічної фейкоістерії можна було відзначити кілька особливостей, що притаманні сучасному медіапростору в даному аспекті:

1) особливості людської взаємодії в масовому суспільстві неминуче полягають у формуванні та поширенні чуток. Процес формування чуток схожий на міфотворчість і полягає у зміцненні соціальних зв'язків, дає фундамент для вибудовування суспільного дискурсу, дозволяє людям діяти в рамках єдиного інформаційного поля. Крім цього чутки, що будуються на поширенні найбільш «гострої» інформації, приваблюють людей через певну міру прихильності до «обраних», які нею володіють. Когнітивними психологами з Університету Канзасу Д. Салліваном, М. Ландау та З. Ротшильдом було проведено науковий експеримент, в результаті якого вчені дійшли висновку, що поширення чуток дозволяє людині відчувати уявне почуття контролю над ситуацією в умовах, коли насправді вона не здатна на неї вплинути. Це спричиняє помітне зниження стресу. Причому, як показала пандемія COVID-19, найбільш схильні до розповсюдження чуток емоційно нестабільні, нестійкі люди, на психіку яких вплинула якась подія, пов'язана з об'єктом їх чуток, або люди, які не мають жодного відношення до ситуації, що дозволяє їм знаходитися якнайдалі від ситуації та формувати цифічні картини того, що відбувається;

2) в рамках поширення фейкової інформації ніякої ролі не відіграє ступінь поширюваних чуток і домислів. Будь-яка інформація, яка потрапляє в поле зору людини, незалежно від її довіри до неї, неминуче буде транслюватися далі з однаковим ступенем «ефірної частки». Більш того, якщо людина має сумніви щодо будь-якої інформації, шанс, що вона займатиме більше медіапростору для міркувань на її рахунок, значно вищий, через що інтерес до неї та її подальшого подальше розповсюдження збільшиться;

3) зростання кількості чуток пропорційне ступеню нестабільності ситуації в державі. Як правило, на поширення чуток не впливають ні стать, ні вік, ні освіта особи, яка розповсюджує інформацію. Основним фактором виступає ступінь соціальної нестабільності, внаслідок чого за рахунок деформацій колективного мислення деформується і суспільний дискурс разом із суспільним інформаційним потоком, який формує рамки для міркувань і неминуче втягує людину в безодню, в рамках якої неможливо мислити поза фейковими поняттями та категоріями.

На момент особливого загострення коронавірусної інфекції вкрай високий ступінь провини у великій кількості фейків та високого ступеня недовіри суспільства до вакцин лежав на ЗМІ. Треба відзначити, що ЗМІ не впоралися з роллю посередником між суспільством та державою, не змогли створити необхідне інформаційне поле для розповсюдження достовірної інформації щодо вакцинації, що коштувало багатьом людям життя.

В умовах воєнного стану проблема поширення фейків стала ще більш актуальною і набула високого ступеня державної ваги. Новини поширюються всюди – у соціальних мережах, пошті, телебаченні та інших ЗМІ, що поставило на порядок денний найсерйозніше і найзлоденніше питання – здійснення оперативної та всебічної боротьби з фейками.

Враховуючи масштаби фейкових новин, серйозність їх наслідків, у тому числі той факт, що фейки – це дієвий інструмент інформаційної війни, представники влади у боротьбі з ними мають консолідувати зусилля з різними інститутами громадянського суспільства, щоб небайдужі громадяни отримували достовірну та своєчасну інформацію про умови воєнного стану, що зрештою сприятиме мінімізації інформаційного тиску на населення. На даний момент ведеться активна робота щодо надання інформації про те, що відбувається на території України. Представники державної влади регулярно проводять брифінги з метою інформування громадян про поточну воєнно-політичну ситуацію.

Попри це кількість фейків залишається на високому рівні. На жаль, далеко не всі користувачі розуміють те, як влаштовано індустрію фейків і що ми знаходимося на полі інформаційної війни. Найстрашніше, що більшість користувачів не вміють правильно розпізнавати

та «відфільтрувати» фейкову інформацію. У розповсюдження фейків є і економічне підґрунтя, оскільки фейки призначені також для заробітку на Інтернет-трафіку та розповсюдженні хибної інформації. Більш того, сьогодні значно зросла кількість аудиторії, серед яких користувачі, які відвідують підроблені сайти та канали, які, крім психологічного тиску та дезінформації, активно збирають пожертви, які далеко не завжди йдуть за призначенням.

Держава веде активну боротьбу з фейками, спростовує недостовірні новини, публікує власні дані щодо перебігу воєнного стану. Однак, психологічно людина влаштована так, що при отриманні дози стресу та страху перед швидкими змінами вона прагне великих емоцій. Саме тому людей так легко обдурити на емоційному тлі, чим уміло користуються творці фейкових новин.

В силу особливостей сучасних геополітичних конфліктів протистояння між державами в наш час є гібридною сумішшю різного роду негативних впливів, що передбачають тиск на противника в різних аспектах його державного життя. Найбільш популярними методами тиску під час ведення гібридного протистояння є політичні та економічні. Формування несприятливої економічної обстановки країни за рахунок тиску через певні обмеження, з паралельною дискредитацією влади та правлячого режиму всередині самої країни, створює серйозні передумови для різноманітних хвилювань соціального характеру, що дестабілізує державу і здатне вивести її з геополітичної боротьби.

Згідно з чинними нормативно-правовими актами та загально-теоретичними принципами, особу можна притягнути до юридичної відповідальності лише за наявності фактичних (вчинення правопорушення) та нормативних (існування норми права, що прямо передбачає застосування санкцій) підстав[1].

При поширенні недостовірної інформації особа, чиї права були порушені, має право звернутися до суду для захисту своїх особистих немайнових чи майнових прав та інтересів (ч. 1 та 2 ст. 16 ЦК України)[2]. Наслідки поширення недостовірної інформації в соціальних мережах можуть проявлятися в різних формах, таких як відмова від

[1] Штрафи за фейки. У Мінкульті представили законопроект про дезінформацію. URL: https://nv.ua/ukr/biz/markets/u-minkulti-predstavili-zakonoproekt-pro-dezinformaciyu-novini-ukrajini-50065133.html.

[2] Цивільний кодекс України: Закон України від 16.01.2003 № 435-IV. URL: https://zakon.rada.gov.ua/laws/show/435-15#Text

укладеного договору, відмова від продажу товарів, робіт і послуг, а також у вигляді публічного осуду (бойкотування, цькування, тролінг, масове обурення в соцмережах). Важливо відзначити, що це не залишається без наслідків для особи, щодо якої поширюється така інформація. Поширення недостовірної інформації має цивільно-правові наслідки майнового характеру. Так, це може не лише призвести до завершення професійної діяльності, але й призвести до додаткових витрат, реальної шкоди та/або упущеної вигоди. Крім того, поширення недостовірної інформації може бути непропорційним або необґрунтованим і призвести до моральних страждань і моральної шкоди. Враховуючи ці наслідки, особа має право вибрати способи захисту порушеного права, спираючись на ст. 16 ЦК України та інші відповідні норми права (ст. 276, 277 ЦК України)[1].

Згідно з ч. 4 ст. 32 Конституції України, ст. 16, 277, 278 Цивільного кодексу України та п. 6 Постанови Пленуму Верховного Суду України «Про судову практику у справах про захист гідності та честі фізичної особи, а також ділової репутації фізичної та юридичної особи»[2], способами захисту прав фізичної особи у випадку поширення недостовірної інформації є: спростування недостовірних відомостей (ч. 1 ст. 277 ЦК України); право на відповідь (ч. 1 ст. 277 ЦК України, ст. 65 Закону України «Про телебачення і радіомовлення»[3], ст. 37 Закону України «Про друковані засоби масової інформації (пресу) в Україні»[4]); встановлення факту недостовірності інформації та її спростування (ч. 4 ст. 277 ЦК України); відкликання документа, в якому була розповсюджена недостовірна інформація; заборона на поширення інформації, що порушує особисті немайнові права (ст. 278 ЦК України)[5]; відшкодування матеріальних збитків; компенсація моральної (немайнової) шкоди.

---

1 Цивільний кодекс України: Закон України від 16.01.2003 № 435-IV. URL: https://zakon.rada.gov.ua/laws/show/435-15#Text

2 Про судову практику у справах про захист гідності та честі фізичної особи, а також ділової репутації фізичної та юридичної осо- би: Постанова Пленуму Верховного Суду України від 27.02.2009 № 1. URL: https://zakon.rada.gov.ua/laws/show/v_001700-09#Text

3 Про телебачення і радіомовлення: Закон України від 21.12.1993 № 3759-XII. URL: https://zakon.rada.gov.ua/laws/show/3759-12

4 Про друковані засоби масової інформації (пресу) в Україні: Закон України від 16.11.1992 № 2782-XII. URL: https://zakon.rada.gov. ua/laws/show/2782-12

5 Цивільний кодекс України: Закон України від 16.01.2003 № 435-IV. URL: https://zakon.rada.gov.ua/laws/show/435-15#Text

У спорах щодо поширення недостовірної інформації в соціальних мережах та Інтернеті найскладнішим є питання доведення наявності правопорушення. Воно включає дві основні складові: по-перше, правові підстави, порядок збору та забезпечення доказів; по-друге, їх допустимість з погляду процесуального права.

Аналіз судової практики показує, що в основному захист «інформаційних» прав осіб здійснюється в рамках цивільного судочинства, зокрема через забезпечення права на честь, гідність і ділову репутацію, які є особистими немайновими правами (ст. ст. 201, 297 Цивільного кодексу України). Подібно, в ст. ст. 94, 299 Цивільного кодексу України закріплено право юридичних та фізичних осіб на недоторканність їх ділової репутації[1].

Однак це питання є досить проблемним, оскільки в чинних нормативно-правових актах відсутні чіткі визначення понять гідності, честі та ділової репутації. Ці терміни є не лише морально-етичними категоріями, але й особистими немайновими правами, які закон визнає самостійними об'єктами судового захисту.

Зокрема, гідність означає визнання цінності кожної фізичної особи як унікальної біопсихосоціальної одиниці. Честь пов'язана з позитивною соціальною оцінкою особи в очах оточуючих, що базується на відповідності її вчинків (поведінки) загальноприйнятим уявленням про добро та зло. Ділова репутація фізичної особи – це суспільна оцінка її ділових і професійних якостей, що формується в процесі виконання трудових, службових, громадських чи інших обов'язків. Ділова репутація юридичної особи, зокрема підприємницьких товариств, фізичних осіб-підприємців, адвокатів, нотаріусів та інших, полягає в оцінці їх підприємницької, громадської, професійної чи іншої діяльності, яку вони здійснюють як учасники суспільних відносин[2].

Захист порушених прав внаслідок поширення фейкової інформації також здійснюється шляхом вимагання спростування недостовірних відомостей у судовому порядку. Зокрема, згідно з ч. 1 ст. 277 Цивільного кодексу України, якщо порушено немайнові права фізичної особи через поширення недостовірної інформації про неї чи членів

[1] Цивільний кодекс України від 16 січня 2003 р. No 435-IV. Офіційний вебпортал Верховна Рада України. URL: http://zakon2.rada.gov.ua/laws/show/435-15/conv/page.

[2] Про судову практику у справах про захист гідності та честі фізичної особи, а також ділової репутації фізичної та юридичної особи: Постанова Пленуму Верховного Суду України від 27 лютого 2009 р. № 1. URL: https://zakon.rada.gov.ua/laws/show/v_001700-09.

її сім'ї, вона має право на відповідь, а також на спростування цієї інформації[1].

Однак, по-перше, це положення стосується лише порушених прав фізичної особи. По-друге, при реалізації права на відповідь виникають проблеми, пов'язані з відсутністю відповідальності за відмову в його реалізації. Оскільки в Кодексі України про адміністративні правопорушення (КУпАП) передбачено можливість притягнення до юридичної відповідальності за ненадання можливості оприлюднити відповідь лише щодо інформації, поширеної про суб'єкта виборчого процесу (ст. 212-11 КУпАП)[2]. Таким чином, у разі відмови в оприлюдненні відповіді на вимогу інших осіб, особа, яка поширює інформацію, не несе відповідальності.

Якщо зацікавлена особа бажає захистити своє порушене право шляхом вимоги спростування недостовірної інформації, вона повинна враховувати положення Цивільного кодексу України, згідно з якими спростування цієї інформації має здійснювати особа, що її поширила; спростування проводиться незалежно від вини особи, яка поширила інформацію (діє презумпція вини); спростування відбувається тим самим способом, яким була поширена інформація.

У Цивільному кодексі України передбачено ще один спосіб захисту порушених прав. Зокрема, в ст. 278 цього нормативно-правового акту йдеться про заборону поширення інформації, яка порушує особисті немайнові права, у таких засобах масової інформації, як газети, книги, кінофільми, теле- та радіопередачі тощо, які готуються до випуску або вже були опубліковані.

Одним із способів впливу на особу, яка завдає шкоди охоронюваним правам інших суб'єктів у інформаційній сфері, є санкції з боку оператора або провайдера телекомунікацій. Наприклад, ст. 38 Закону України «Про телекомунікації» надає таким суб'єктам право: «... скорочувати перелік або припиняти надання телекомунікаційних послуг споживачам, які порушують правила надання та отримання цих послуг, або відключати кінцеве обладнання споживача, якщо воно не має відповідного документа про підтвердження відповідності ви-

[1] Цивільний кодекс України від 16 січня 2003 р. № 435-IV. URL: http://zakon2.rada.gov.ua/laws/show/435-15/conv/page.

[2] Кодекс України про адміністративні правопорушення (статті 1–212- 20): Кодекс: Закон України від 7 грудня 1984 р. No 8073-X. URL: http://zakon0.rada.gov.ua/laws/show/80731-10.

могам нормативних актів у сфері телекомунікацій, у порядку, визначеному цими правилами; відключати на підставі рішення суду кінцеве обладнання, якщо воно використовується абонентом для вчинення протиправних дій або дій, що загрожують національній безпеці...»[1]. Однак ця процедура є довготривалою, і при цьому правопорушник може звернутися до іншого оператора або провайдера телекомунікацій для отримання послуг, використовуючи мережу Інтернет.

У контексті спростування фейкової інформації та можливості захисту своїх порушених прав є дискусійними положення ч. 2 ст. 47-1 Закону України «Про інформацію», яка визнає оціночними судження, за винятком образи та наклепу, висловлювання, що не містять фактичних даних, зокрема критику, оцінку дій, а також висловлювання, які не можуть бути витлумачені як фактичні дані через характер використання мовних засобів, таких як гіперболи, алегорії, сатира. Оскільки оціночні судження не підлягають спростуванню та доведенню їхньої правдивості, захист оціночних суджень не є предметом судового захисту.

Тобто, якщо фейк буде визнано судом оціночним судженням, захист порушених прав стане практично неможливим.

Одним із найбільш проблемних аспектів є захист прав зацікавленого суб'єкта у випадку поширення фейку в соціальних спільнотах Інтернету або «Інтернет-ЗМІ». По-перше, це зумовлено тим, що в Україні на законодавчому рівні не закріплено обов'язок для власників та процедуру їх реєстрації Інтернет-ЗМІ (деякі з них реєструються у Міністерстві юстиції України як «газети» або «інформаційні агентства», для «легалізації» своєї діяльності). По-друге, на законодавчому рівні робляться лише перші кроки щодо блокування Інтернет-ресурсів, які прямо чи опосередковано пов'язані з поширенням такої інформації, або ж не відповідають належним чином на зазначені дії.

Зважаючи на можливі проблеми, що можуть виникнути через «зловживання правом» під час притягнення потенційно винної фізичної особи до юридичної відповідальності, доцільно спрямувати зусилля на розробку механізму співпраці між державою та власниками найбільших соціальних мереж. Адже, як показує статистика, саме ці мережі найчастіше стають майданчиками для поширення фейкової інформації.

[1] Закон України «Про телекомунікації». URL: https://zakon.rada.gov.ua/laws/show/1280-15.

Однак, обмеження лише санкціями не дозволить досягти бажаних результатів. Співпраця повинна ґрунтуватися на створенні ефективної взаємодії з глобальними інформаційними лідерами (Google, Facebook, Twitter тощо)[1].

Однією з основних проблем є питання визначення належного відповідача, якого можна притягнути до відповідальності за публікацію недостовірних відомостей. Законодавство та судова практика вказують, що відповідачем є особа, яка поширила таку інформацію (ст. 277 Цивільного кодексу України[2] та п. 9, 12 Постанова Пленуму Верховного Суду України[3]). Тобто, належним відповідачем у випадку поширення спірної інформації в Інтернеті є фізична або юридична особа, яка поширила недостовірну інформацію, а також автор відповідного матеріалу та власник веб-сайту. Позивач має вказати цих осіб у позовній заяві та довести факт поширення інформації саме відповідачем[4] або, у разі неможливості встановлення цієї особи, надати дані про власника веб-сайту, на якому була розміщена інформація.

Дані про власника веб-сайту можуть бути отримані відповідно до положень Цивільного процесуального кодексу України через адміністратора системи реєстрації та обліку доменних імен українського сегмента Інтернету (ч. 3 п. 12 Постанова Пленуму ВСУ[5]). У випадку, якщо ця інформація не була отримана, суд повинен відмовити у відкритті провадження, вказавши на невиконання заявником права на отримання даних щодо встановлення належного відповідача у судовому порядку[6]. Суд також наголошує на важливості подання довідки від Консорціуму «Український центр підтримки номерів і

---

1 Черниш Р. Ф. Правовий досвід країн Європейського Союзу у сфері протидії поширенню фейкової інформації. Підприємництво, господарство і право. URL: http://pgp-journal.kiev.ua/archive/2019/10/22.pdf.

2 Цивільний кодекс України: Закон України від 16.01.2003 № 435-IV. URL: https://zakon.rada.gov.ua/laws/show/435-15#Text

3 Про судову практику у справах про захист гідності та честі фізичної особи, а також ділової репутації фізичної та юридичної осо- би: Постанова Пленуму Верховного Суду України від 27.02.2009 № 1. URL: https://zakon.rada.gov.ua/laws/show/v_001700-09#Text

4 Постанова Верховного Суду від 14.12.2022 у справі № 454/2743/19. URL: https://reyestr.court.gov.ua/Review/107938372

5 Про судову практику у справах про захист гідності та честі фізичної особи, а також ділової репутації фізичної та юридичної осо- би: Постанова Пленуму Верховного Суду України від 27.02.2009 № 1. URL: https://zakon.rada.gov.ua/laws/show/v_001700-09#Text

6 Постанова Верховного Суду від 07.12.2021 у справі № 905/902/20. URL: https://reyestr.court.gov.ua/Review/102342551

адрес» про власника веб-сайту (або про неможливість його встановлення) або обґрунтованої заяви про неможливість отримання цієї довідки[1]. Така довідка або документ від дочірнього підприємства Консорціуму «Центр компетенції адресного простору мережі Інтернет» є належним і допустимим доказом[2]. В судовій практиці часто підкреслюється необхідність подання такої довідки, оскільки скріншоти з соціальних мереж, таких як Facebook, не доводять, що аккаунт створений саме відповідачем, а також не підтверджують, що саме відповідач поширив інформацію, яка є предметом спору[3]. Ця правова позиція також відображена в інших судових рішеннях. Якщо оспорюється авторство контенту, суди часто роблять висновок, що через можливість реєстрації акаунтів у соціальних мережах будь-якою особою під будь-яким іменем, достовірно з'ясувати належність сторінки конкретній особі неможливо. Тому скріншоти веб-сторінок є неналежним доказом. Особа, чиї права були порушені через поширення недостовірної інформації, повинна довести, що акаунт чи веб-сторінка належать відповідачу, в тому числі шляхом звернення до відповідної установи. Якщо неможливо встановити особу, яка поширила недостовірну інформацію, або автора контенту та його місце проживання, відповідальність несе власник веб-сайту, на якому була розміщена інформація. Згідно зі ст. 1 Закону України «Про авторське право і суміжні права», власник веб-сайту – це особа, яка володіє обліковим записом і визначає порядок використання сайту. Якщо немає інших доказів, власником веб-сайту є реєстрант доменного імені, що забезпечує доступ до сайту, або отримувач послуг хостингу[4]. Володільці веб-сайтів та постачальники послуг хостингу зобов'язані публічно розміщувати достовірну інформацію про себе, зокрема через бази даних WHOIS[5]. Така позиція є обґрунтованою, оскільки ці особи можуть контролювати інформацію, що публікується на сайті, вида-

[1] Ухвала Приморського районного суду м. Одеси від 10.10.2018 у справі № 522/17690/18. URL: http://www.reyestr.court.gov.ua/ Review/77095370

[2] Постанова Верховного Суду від 05.06.2024 у справі № 742/853/20. URL: https://reyestr.court.gov.ua/Review/119579601

[3] Постанова Верховного Суду від 01.12.2021 у справі № 310/6999/19-ц. URL: https://reyestr.court.gov.ua/Review/101584115

[4] Про авторське право і суміжні права: Закон України від 01.12.2022 № 2822-IX. URL: https://zakon.rada.gov.ua/laws/show/2811-20#Text

[5] Постанова Верховного Суду від 14.12.2022 у справі № 454/2743/19. URL: https://reyestr.court.gov.ua/Review/107938372

ляти недостовірні, образливі чи наклепницькі дані, тим самим запобігаючи порушенню конституційних прав громадян і юридичних осіб.

Інформацію про власника веб-сайту можна отримати через звернення до адміністратора системи реєстрації та обліку доменних імен українського сегмента Інтернету. Однак варто зазначити, що цей процес має певні обмеження. Така інформація може бути отримана лише в межах судового провадження або при поданні клопотання про забезпечення доказів. Це створює значні труднощі для швидкого визначення учасників потенційного судового процесу. Такий підхід має як позитивні, так і негативні сторони. З одного боку, він захищає приватність власників веб-сайтів від безпідставних запитів, але з іншого – може істотно затягнути та ускладнити процес підготовки до судового розгляду для позивачів, які мають обґрунтовані претензії.

Крім того, така ситуація може призвести до затримок у здійсненні правосуддя, оскільки сторони не можуть вчасно ідентифікувати всіх необхідних учасників процесу. Це особливо важливо в справах про поширення недостовірної інформації в соціальних мережах, де швидкість реагування є критичною.

Таким чином, ця процедура призводить до дисбалансу між захистом приватності власників веб-сайтів та ефективністю судового процесу, що потребує подальшого законодавчого врегулювання для забезпечення оптимального балансу інтересів усіх учасників.

Зокрема, судова практика розглядає власників веб-сайтів або, у випадку відсутності інформації про них, реєстрантів доменних імен як належних відповідачів у справах цієї категорії. Верховний Суд підкреслив, що якщо відповідач стверджує, що він є лише реєстрантом домену, а не власником веб-сайту, він повинен вказати, хто є власником відповідного сайту, доступ до якого здійснюється через зареєстрований ним домен, або надати докази, що підтверджують передачу права користування доменом[1] іншій особі, повністю або частково. У разі відсутності таких доказів, суд має визначити, чи здійснювалося користування доменом без належної правової підстави іншою особою[2]. Таку правову позицію підтримано і в інших

[1] Постанова Верховного Суду від 25.11.2020 у справі № 753/7999/19. URL: https://reyestr.court.gov.ua/Review/93373639

[2] Постанова Верховного Суду від 09.04.2020 у справі № 742/3715/17. URL: https://reyestr.court.gov.ua/Review/88739566

Постановах Верховного Суду[1], де акцентується увага на презумпції відповідальності власника веб-сайту чи реєстратора за поширення недостовірної інформації.

Багато медіа-ресурсів та публічних осіб використовують YouTube-канали для поширення контенту. У разі розміщення спірної інформації виникає необхідність визначити реального власника каналу. Фактичні дані про власників доступні лише YouTube (Google LLC). Відповідач може заперечувати свою причетність до каналу, стверджуючи, що канал міг бути створений будь-ким. В якості доказу належності каналу є гіперпосилання на YouTube-канал з ідентифікаторами власника, яке може розмістити тільки сам володілець[2]. Однак часто виникають ситуації, коли веб-сайти не зареєстровані в Україні, і встановити інформацію про їхніх власників стає майже неможливо. В такому разі, згідно з правовою позицією Верховного Суду України, суд може за заявою зацікавленої особи встановити факт недостовірності інформації та спростувати її в рамках окремого провадження (ч. 4 ст. 277 ЦК України, п. 13 Постанови Пленуму[3]). Це також стосується ситуацій, коли особа, що поширила інформацію, невідома (наприклад, при надсиланні анонімних або псевдонімних повідомлень, смерті фізичної особи чи ліквідації юридичної особи, поширення інформації в Інтернеті особою, яку неможливо ідентифікувати тощо[4]). Якщо заявник доведе недостовірність інформації, суд лише підтвердить це і спростує її. Однак, якщо під час судового процесу стане відома особа, яка поширила спірну інформацію, суд має залишити заяву без розгляду і роз'яснити сторонам, що вони можуть подати позов на загальних підставах.

Заінтересована особа повинна надати суду докази, що неможливо встановити відомості про власника веб-сайту чи особу, яка поширила інформацію (наприклад, довідку від Центру компетенції, що відсутні відомості про власника веб-сайту чи реєстратора домену, або інфор-

[1] Постанова Верховного Суду від 01.12.2021 у справі № 742/287/17. URL: https://reyestr.court.gov.ua/Review/101634356

[2] Рішення Господарського суду м. Києва від 11.12.2018 у справі № 910/6647/18. URL: http://www.reyestr.court.gov.ua/ Review/78926333

[3] Про судову практику у справах про захист гідності та честі фізичної особи, а також ділової репутації фізичної та юридичної осо- би: Постанова Пленуму Верховного Суду України від 27.02.2009 № 1. URL: https://zakon.rada.gov.ua/laws/show/v_001700-09#Text

[4] Постанова Верховного Суду від 11.12.2023 у справі № 504/4099/16-ц. URL: https://reyestr.court.gov.ua/Review/115750120

мацію про те, що їх неможливо ідентифікувати). Якщо ці докази не будуть надані, суд відмовить у розгляді справи в порядку окремого провадження через відсутність вжитих заходів для встановлення володільця веб-сайту[1] або ненадання обґрунтованої заяви про неможливість отримання цієї довідки. Для посилення доказової бази заінтересована особа може звернутися за експертним висновком[2] Центру компетенції, який може бути отриманий після проведення фіксації та дослідження змісту веб-сторінки в Інтернеті. Крім того, така особа повинна довести, що зверталася до уповноваженої установи з запитом про визначення володільців цієї інформації, і у разі відсутності відповіді – надати відповідні документи. Для підтвердження належних зусиль та обґрунтування необхідності судового втручання, у разі безрезультатності своїх дій, заявник повинен подати клопотання про витребування доказів, супроводжуючи його доказами попередніх спроб отримання інформації.

Насправді, коли заінтересована особа збере всі необхідні докази, автор недостовірної інформації може легко її видалити, або ж спільнота в соціальній мережі може вже й не згадувати про це повідомлення, що зробить спростування малоефективним. На наш погляд, не варто відкладати дії на потім. Краще одразу зафіксувати факт поширення недостовірної інформації та підтвердити це електронним підписом за допомогою фотознімка або скріншоту екрану, на якому будуть чітко зазначені назва веб-сторінки, дата та час публікації, а також інформація, яка є недостовірною.

Ще однією проблемою є те, що деякі блогери та анонімні коментатори в Інтернеті фактично не підлягають судовому переслідуванню, поки їх не буде ідентифіковано, і поки суд не визнає їх комунікацію публічним розповсюдженням недостовірної інформації. Тому такі особи, які перебувають поза межами національної юрисдикції, можуть без остраху поширювати будь-яку інформацію, зокрема негативну чи недостовірну, і називати конкретні імена у спірних матеріалах. Важливо зазначити, що на даний момент не існує жодного наднаціонального нормативного акту, який би регулював цей процес.

[1] Ухвала Дніпровського районного суду м. Києва від 29.05.2024 у справі № 755/3303/24. URL: https://reyestr.court.gov.ua/ Review/119354314

[2] Постанова Верховного Суду від 27.01.2021 у справі № 753/13197/18. URL: https://reyestr.court.gov.ua/Review/95042314

З огляду на це, юридичний склад правопорушення, який є підставою для задоволення позову, включає такі обставини[1]: а) поширення інформації, тобто її доведення до відома хоча б однієї особи будь-яким способом; б) поширена інформація стосується конкретної фізичної чи юридичної особи, тобто позивача; в) поширення недостовірної інформації, тобто такої, що не відповідає дійсності; г) поширення інформації, яка порушує особисті немайнові права, тобто завдає шкоди особистим немайновим благам або перешкоджає особі в повному та своєчасному здійсненні її особистих немайнових прав. Така правова позиція підтверджується майже в кожній судовій справі, яка надходить на розгляд.

Для того, щоб встановити факт поширення недостовірної інформації про себе в соціальній мережі, особа повинна довести наступні обставини: 1) факт поширення інформації на веб-сторінці чи сайті відповідача в конкретному домені і в певний час, тобто її доведення до відома хоча б однієї особи будь-яким способом у межах соціальної мережі; 2) поширення недостовірної інформації в соціальній мережі; 3) те, що ця недостовірна інформація стосується саме позивача; 4) підтвердження недостовірності цієї інформації; 5) порушення його немайнових прав через поширення такої інформації. Водночас відповідач має довести лише те, що поширена ним інформація є правдивою. Це є однією з найбільших проблем, оскільки професійно створена недостовірна (неправдива) інформація часто включає елементи, які можуть виглядати правдоподібно або є частково правдивими, але спотвореними для створення негативного враження.

Згідно з матеріалами судової практики, під поширенням інформації розуміється: її публікація у ЗМІ, передача через радіо, телебачення чи інші засоби масової інформації; поширення в Інтернеті або через інші засоби телекомунікаційного зв'язку; викладення в характеристиках, заявах, листах, адресованих третім особам; повідомлення у публічних виступах, електронних мережах або в іншій формі хоча б одній людині (п. 15 Постанови ВСУ № 1 від 27.02.2009). Звісно, способи та форми поширення недостовірної інформації можуть змінюватися з часом, але це визначення враховує всі можливі

[1] Про судову практику у справах про захист гідності та честі фізичної особи, а також ділової репутації фізичної та юридичної осо- би: Постанова Пленуму Верховного Суду України від 27.02.2009 № 1. URL: https://zakon.rada.gov.ua/laws/show/v_001700-09#Text

способи її розповсюдження на сьогодні. Тому цей перелік не є вичерпним. Недостовірною вважається інформація, яка не відповідає дійсності або викладена неправдиво, тобто містить відомості про події чи явища, яких не було взагалі, або які дійсно мали місце, але їх опис є неповним або перекрученим (п. 15 Постанови ВСУ № 1 від 27.02.2009). Негативною є інформація, що містить ствердження про порушення особою норм чинного законодавства або вчинення інших дій (наприклад, порушення моральних принципів, загальноприйнятих норм співжиття, неетичної поведінки в особистому, суспільному чи політичному житті), що, на думку позивача, порушує його право на повагу до гідності, честі чи ділової репутації.

Слід зазначити, що необхідно розрізняти публічну та приватну сфери, адже кожна людина має право на свободу слова та вираження особистої думки. На наш погляд, для того, щоб підтвердити факт поширення інформації, потрібно довести, що Інтернет-сторінка є публічною, тобто доступною для кожного користувача без обмежень на вхід. Таким чином, блоги чи веб-сторінки, що мають обмежений доступ і призначені лише для певного кола осіб, на нашу думку, не можуть бути розцінені як платформи для поширення інформації, навіть якщо вона є недостовірною чи негативною. Отже, для доведення факту поширення недостатньо лише підтвердити факт наявності інформації, потрібно також надати докази того, що сторінка (блог) в соціальній мережі є публічною та орієнтована на доступ необмеженого кола осіб. Лише в такому випадку можна притягнути до відповідальності власника цієї веб-сторінки.

Враховуючи необхідність забезпечення балансу між правом на свободу думки та слова і правом кожного вимагати поваги до своєї гідності та честі, суду слід звертати увагу на характер недостовірної інформації та визначати, чи є вона фактичним твердженням, чи оціночним судженням (п. 19 Постанови Пленуму ВСУ)[1]. Це важливо, оскільки, відповідно до ч. 1 ст. 30 Закону України «Про інформацію», особа не може бути притягнута до відповідальності за висловлювання оціночних суджень. Згідно положень ч. 2 цієї статті, оціночними судженнями, окрім наклепу, є висловлювання, що не містять фак-

[1] Про судову практику у справах про захист гідності та честі фізичної особи, а також ділової репутації фізичної та юридичної осо- би: Постанова Пленуму Верховного Суду України від 27.02.2009 № 1. URL: https://zakon.rada.gov.ua/laws/show/v_001700-09#Text

тичних даних, критика, оцінка дій або такі висловлювання, які не можуть бути трактовані як фактичні, зокрема, через використання мовно-стилістичних засобів, таких як гіперболи, алегорії чи сатира. Оціночні судження не підлягають спростуванню та доведенню їх правдивості. Тому доречним є підхід, що розрізняє судження і фактичні твердження: судження – це вираження думки, що має оціночний характер і відображає ставлення того, хто висловлює думку, до її змісту, що пов'язано з такими психологічними станами, як віра, впевненість або сумнів. Оскільки правдивість чи точність судження неможливо перевірити, воно не є предметом судового розгляду. Натомість, фактичне твердження являє собою логічне викладення конкретних фактів або групи фактів, які є об'єктивними явищами дійсності, що відбуваються в певному місці та часі за певних умов. Оскільки факт є об'єктивною категорією, що не залежить від думок чи поглядів інших осіб, його відповідність дійсності може бути перевірена та встановлена судом[1].

Факти можна довести або продемонструвати, тоді як правдивість оціночних суджень практично неможливо встановити. Вимогу доводити достовірність оціночних суджень не можна виконати, оскільки вона порушує основне право на свободу думки, яке гарантується ст. 10 Конвенції[2] (Lingens v. Austria № 9815/82 § 46 від 08.07.1986). Особа не зобов'язана доводити правдивість своїх власних думок, ідей, поглядів або критичних висловлювань стосовно третіх осіб. Це право на власну точку зору захищене ст. 10 Конвенції і поширюється на перебільшення, порівняння, сатиру та оцінку дій особи. Вимога доводити такі судження суперечить основному праву на свободу вираження думок.

Слід наголосити, що оціночні судження, особисті думки, переконання та критичні оцінки фактів не підлягають судовому захисту. Такі вираження суб'єктивної позиції відповідача не можна перевірити на достовірність або спростувати, на відміну від фактичних тверджень (ст. 277 ЦК України). Будь-яке оціночне судження, критика чи оцінка дій, вираження особистих думок щодо виконання публічних

[1] Луспеник Д. Захист гідності, честі та ділової репутації у контексті дифамаційного спору: практика Верховного суду. Верховний суд: веб-сайт. URL: https://supreme.court.gov.ua/userfiles/media/new_folder_for_uploads/supreme/PREZ_Luspenyk_21_10_2021.pdf

[2] Конвенція про захист прав людини і основоположних свобод: ратифіковано Законом № 475/97-ВР від 17.07.97. URL: https://zakon.rada.gov.ua/laws/show/995_004

функцій або результатів діяльності не є підставою для захисту права на честь, гідність та ділову репутацію і, відповідно, не може бути предметом судового захисту[1].

Водночас, оціночне судження повинно бути висловлене в межах, що не порушують закон і моральні принципи суспільства. Іноді формулювання можуть бути такими, що викликають образу або обурення, тобто є надмірними та не мають фактичних підстав (Jerusalem v. Austria)[2]. Суд може визнати таке судження надмірним, якщо воно не базується на жодних фактах, і покласти на відповідача обов'язок відшкодувати моральну шкоду (аб. 2 ч. 2 ст. 30 ЗУ «Про інформацію», п. 19 Постанови Пленуму ВСУ № 1 від 27.02.2009)[3].

При розгляді справ щодо захисту честі, гідності та ділової репутації може виникнути проблема суб'єктивного підходу при розмежуванні понять «відомості, що ганьблять або применшують честь і гідність» та «оціночні судження, думки, переконання». Перші з них підлягають захисту правом, а другі – лише у випадку, якщо містять елементи образи. Оцінка суддями цих понять може призвести до неоднозначних результатів у судовій практиці. Крім того, слід розуміти, що ці категорії є оціночними за своєю природою і їх точне визначення важко встановити. Тому кожна особа сприйматиме їх по-різному. Проте, необхідно розробити чіткі критерії, за якими та чи інша інформація може бути кваліфікована як недостовірна.

Основною особою, відповідальною за поширення недостовірної інформації, є її автор. Якщо автор інформації невідомий або неможливо встановити його особу та/або місце проживання (місцезнаходження), а також коли інформація поширюється анонімно, відповідальність покладається на власника медіа, на якому було опубліковано такий матеріал. Саме він створив умови та технологічні можливості для розповсюдження цієї недостовірної інформації.

Щодо відповідальності, то особа, щодо якої була поширена недостовірна інформація, має право перш за все звернутися до суду для

---

[1] Постанова Верховного Суду від 20.05.2019 у справі № 591/7099/16-ц. URL: http://www.reyestr.court.gov.ua/Review/82119183

[2] Jerusalem v. Austria: Judgment of European Court of Human Rights, 27 February 2001, № 26958/95. URL: https://hudoc.echr.coe.int/ eng#{%22itemid%22:[%22001-59220%22]}

[3] Про інформацію: Закон України від 02.10.1992 № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text

захисту своєї честі, гідності та ділової репутації. Крім того, ця особа може вимагати компенсації матеріальної та моральної шкоди.

До способів захисту особистих немайнових прав, таких як право на повагу до гідності та честі, а також право на недоторканість ділової репутації, належать спростування недостовірної інформації та/або право на відповідь, заборона на поширення інформації, що порушує особисті немайнові права, та інші заходи.

Законодавство України встановлює порядок спростування недостовірної інформації та надання права на відповідь. Основною різницею між цими двома заходами є те, що при реалізації права на відповідь особа має можливість висвітлити свою точку зору щодо поширеної інформації та обставин порушення особистих немайнових прав без необхідності визнавати її недостовірною. Натомість, спростування недостовірної інформації здійснює особа, яка її поширила, а відповідь надається особою, стосовно якої ця інформація була поширена.

У певних випадках фізична особа має право на захист своїх особистих немайнових прав у разі поширення недостовірної інформації щодо інших осіб. Це особливо стосується членів її сім'ї, таких як другий з подружжя, батьки, діти, бабусі, дідусі, прабабусі, прадідусі, внуки, правнуки тощо. Однак, поширення неправдивої інформації стосовно членів сім'ї повинно порушувати саме особисті немайнові права фізичної особи, яка звертається за захистом.

Наприклад, якщо поширюється недостовірна інформація про те, що фізична особа є дружиною «зрадника», вона має право вимагати спростування цієї інформації не через порушення прав її чоловіка на честь та гідність, а через те, що така інформація порушує саме її право на гідність та честь. Водночас, її чоловік має право вимагати спростування цієї інформації, оскільки вона порушує його особисте право на повагу до честі та гідності.

Спростування недостовірної інформації повинно здійснюватися особою, яка її поширила, незалежно від того, чи є її вина, і тим самим способом, яким інформація була оприлюднена. Якщо особу, яка поширила недостовірну інформацію, неможливо встановити, фізична особа, чиї права були порушені, має право звернутися до суду із заявою про встановлення факту недостовірності цієї інформації та її спростування (абзац третій частини четвертої статті 277 Цивільного кодексу України).

Якщо в друкованих чи інших засобах масової інформації, включаючи Інтернет, виявлено інформацію, що порушує честь, гідність або ділову репутацію особи, права якої ймовірно порушено, вона має право на відповідь або може безпосередньо звернутися до особи, яка поширила таку інформацію, з вимогою її спростування, а також подати позов до суду.

Згідно з пунктом 12 Постанови, належним відповідачем у разі поширення спірної інформації в мережі Інтернет є автор відповідного інформаційного матеріалу та власник веб-сайту. Позивач має встановити та вказати цих осіб в позовній заяві.

Якщо автор поширеної інформації не встановлений або його особу та/або місце проживання (місцезнаходження) неможливо визначити, а також коли інформація є анонімною і доступ до сайту є вільним, належним відповідачем є власник веб-сайту, на якому розміщено інформацію, оскільки саме він створив умови та технологічну можливість для її поширення. Інформація про власника веб-сайту може бути отримана через адміністратора системи реєстрації доменних імен в українському сегменті Інтернету відповідно до вимог Цивільного процесуального кодексу України.

Водночас, відповідно до положень Цивільного процесуального кодексу України позивач у вказаній категорії справ має належним чином довести, що поширена про нього недостовірна інформація є саме фактичним твердженням, а не оціночним судження.

Згідно зі статтею 30 Закону України «Про інформацію», особа не може бути притягнена до відповідальності за висловлення оціночних суджень. Оціночними судженнями, за винятком наклепу, є висловлювання, які не містять конкретних фактів, а є критикою, оцінкою дій або висловлювань, що не можуть бути розтлумачені як фактичні дані, зокрема через використання мовно-стилістичних засобів (наприклад, гіпербол, алегорій, сатири). Оціночні судження не підлягають спростуванню та перевірці на їх правдивість.

Якщо особа вважає, що оціночні судження чи думки порушують її гідність, честь, ділову репутацію або інші особисті немайнові права, вона має право скористатися законним правом на відповідь та подати своє тлумачення ситуації в тому ж самому засобі масової інформації, щоб довести безпідставність поширених суджень, надавши їм альтернативну оцінку. Якщо така суб'єктивна думка була висловлена

в грубій, принизливій чи непристойній формі, що порушує гідність, честь або ділову репутацію, особа, яка так висловилася, може бути зобов'язана відшкодувати моральну шкоду.

Особа може бути притягнута до цивільно-правової відповідальності за поширення недостовірної інформації, а завдану шкоду можуть понести як фізичні, так і юридичні особи. Якщо особа, яка поширила недостовірну інформацію, відмовляється її спростувати чи компенсувати матеріальну та (або) моральну шкоду, то особа, щодо якої була поширена така інформація, має право захищати свої права та інтереси через звернення до суду.

Позовна давність для вимог про спростування недостовірної інформації, опублікованої в засобах масової інформації, становить один рік. Вона обчислюється з дня публікації цієї інформації в засобах масової інформації або з дня, коли особа дізналася або могла дізнатися про ці відомості (пункт 2 частини другої статті 258 Цивільного кодексу України).

У деяких випадках винна особа може понести адміністративну відповідальність за поширення неправдивих чуток, що здатні викликати паніку серед населення або порушити громадський порядок. Це може призвести до накладення штрафу в розмірі від десяти до п'ятнадцяти неоподатковуваних мінімумів доходів громадян або до застосування виправних робіт на строк до одного місяця з відрахуванням 20% заробітку (стаття 1731 Кодексу України про адміністративні правопорушення).

Ключові слова: немайнові права, авторські права, право на ідентичність, право на інформацію, медіапростір, гібридна війна, інформаційна безпека, фейкові новини, дезінформація, репутація, честь, гідність, цифрові права людини, свобода слова.

Розділ 9

ІТ-ПРАВОЧИНИ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

DOI

Ірина Давидова
докторка юридичних наук, професорка

Головною підставою виникнення цивільних правовідносин є правочин – один з найбільш поширених юридичних фактів сфери приватного права. Дослідження категорії «правочин» становить інтерес для багатьох науковців, практиків, здобувачів освіти. Разом з тим, в даному випадку важливим вважаємо послідовність та комплексність такого вивчення, аналіз факторів «сьогодення» (відповідно до часу проведеного дослідження) та формування в результаті такого дослідження уточнених теоретичних положень та практичних рекомендацій.

На даний час послідовність такого дослідження мною становить понад п'ятнадцять років, однак в даному розділі будуть підсумовані результати основних досліджень (на опубліковані дослідження будуть зроблені відповідні посилання), які стосуються розвитку категорії правочину в умовах розвитку інформаційного суспільства, в умовах дії екстраординарних правових режимів, а також в умовах ведення гібридної війни. Для зручності виділимо певні підрозділи.

«Традиційні» правочини[1]

Згідно з частиною 1 ст. 202 ЦК України правочином є дія особи, спрямована на набуття, зміну або припинення цивільних прав та обов'язків.

Як правова категорія, правочини характеризуються сукупністю ознак, що дають можливість відмежовувати їх від інших юридичних

[1] Харитонов Є. О., Давидова І. В. Особливості підстав виникнення цивільних правовідносин у ІТ-сфері. *ІТ-право: поняття та сутність*: моногр. За ред. О. І. Харитонової, Є. О. Харитонова. Одеса: Фенікс, 2017. С. 170-184.

фактів. Це те, що правочин: 1) завжди є вольовим актом; 2) є дією, спеціально спрямованою на досягнення певного правового результату; 3) є дією суб'єктів цивільного (приватного) права; 4) завжди правомірна дія. Названі ознаки є загальними для усіх правочинів, а тому стосуються і правочинів, які укладаються в ІТ-сфері.

Варто згадати також, що в ІТ-сфері набули поширення дво- та багатосторонні правочини (договори). Зокрема, це ІТ-договори надання послуг програмного забезпечення або його розробки; ІТ-договори роботи із ФОП або програмістами; договори про юридичний супровід фрі-лансерів; договори про юридичний аудит ІТ-компаній;договори купівлі-продажу сайту, домену, бренду тощо; будь-які договори, укладені за участі інтернет-магазинів; договори про правове забезпечення діяльності інтернет-магазинів; концесійні договори; ліцензійні угоди; договори про сумісну діяльність у сфері ІТ-відносин; договори, об'єктом яких є права інтелектуальної власності.

Усі згадані договори мають відповідати загальним цивільно-правовим вимогам, що висуваються чинним законодавством до договорів, що зумовлене універсальністю категорії «договір» і придатністю її для використання у різноманітних сферах людського буття, в тому числі і в ІТ-сфері.

Разом із тим, між «ІТ-правом» і правочинами (договорами) існує своєрідний «зворотний зв'язок», що проявляється у коригуванні за допомогою його специфічних засобів «класичних» вимог, ознак, правил, які стосуються розуміння сутності, порядку укладення угод, їхньої форми тощо.

Це пов'язано з тим, що розвиток ІТ дозволяє створювати нові технологічні рішення та інструменти, які спрощують наше життя: як у виконанні простих буденних задач, так і у проведенні надзвичайно складних обчислень, моделювань та ін. Удосконалюються і елементарні процеси у здійсненні базових правовідносин, зокрема й у сфері ідентифікації.

Розглянемо це твердження спочатку на прикладі динаміки оформлення правочинів.

ЦК України (частини 1-3 ст. 207) визначає умови, за яких правочин може вважатися вчиненим в письмовій формі, а саме: якщо його зміст зафіксований в одному або кількох документах, у листах, телеграмах, якими обмінялися сторони; якщо воля сторін виражена за

допомогою телетайпного, електронного або іншого технічного засобу зв'язку; якщо він підписаний його стороною (сторонами). Правочин, який вчиняє юридична особа, підписується особами, уповноваженими на це її установчими документами, довіреністю, законом або іншими актами цивільного законодавства, та скріплюється печаткою. Використання при вчиненні правочинів факсимільного відтворення підпису за допомогою засобів механічного або іншого копіювання, електронно-числового підпису або іншого аналога власноручного підпису допускається у випадках, встановлених законом, іншими актами цивільного законодавства, або за письмовою згодою сторін, у якій мають міститися зразки відповідного аналога їхніх власноручних підписів.

Отже, положення чинного законодавства даю можливість говорити про те, що використання ідентифікації, як інструменту встановлення особи, залишається необхідним при здійсненні відповідних правовідносин в електронній площині. Тому існує практична необхідність існування дієвої системи, яка б чітко надавала дозвіл на вчинення певних дій, отримання інформації саме тій особі, яка має право на отримання такої інформації, або вчинення відповідних правочинів. В даному випадку неможливо обійтися без електронних засобів ідентифікації, які мають прив'язку до особи (яку треба ідентифікувати за абсолютно різними характеристиками).

Однак, не достатньо розробити та застосовувати на практиці такі електронні засоби ідентифікації, має також існувати правове закріплення їх функціонування та правовий захист, яке сьогодні в українському законодавстві не є досконалі та потребують доопрацювання та оновлення. Ці питання є особливо актуальними, зважаючи на новизну у технічному застосуванні та необхідність врегулювання процесів встановлення особи, адже це найголовніша стадія здійснення будь-якому правочину.

Електронні правочини[1]

За останні роки електронні правочини досить міцно укріпилися в нашому житті та набули особливого значення. Якщо спочатку це

[1] ІТ-право: практичний посібник. К.: Норма права, 2025. С. 132-138.

було спричинено розвитком технологій, як таких, та практичним їх застосуванням, то з часом додалися обмеження внаслідок запобігання розповсюдження короно вірусної хвороби, а тепер і введення воєнного стану та ведення на певних територіях нашої країни активних бойових дій.

Законодавець розрізняє поняття електронного правочину та електронного договору в Законі України «Про електронну комерцію». Зокрема, під електронним договором розуміється домовленість двох або більше сторін, спрямована на встановлення, зміну або припинення цивільних прав та обов'язків і оформлена в електронній формі, а під електронним правочином – дія особи, спрямована на набуття, зміну або припинення цивільних прав та обов'язків, здійснена з використанням інформаційно-телекомунікаційних систем. Також ЦК України (починаючи з вересня 2015 року) прирівнює електронну форму вчинення правочину до письмової.

Вже згадуваний Закон під електронною формою представлення інформації розуміє спосіб документування інформації, що означає створення, запис, передачу або збереження інформації у цифровій чи іншій нематеріальній формі за допомогою електронних, магнітних, електромагнітних, оптичних або інших засобів, здатних до відтворення, передачі чи зберігання інформації. Таке документування інформації повинно надавати змогу її відтворювати у візуальній формі, придатній для сприйняття людиною.

Не секрет, що укладення договорів он-лайн має такі переваги, як швидкість, оперативний обмін інформацією, зручність зберігання, оброблення, відправлення документів тощо. А сьогодні можна й додати наявність такого важливого фактора, як безпека сторін, що є дуже важливим в умовах воєнного часу.

Договір як в «традиційному» розумінні, так і «електронний», мають відповідати чинному законодавству. Зокрема, пропозиція укласти договір (оферта) має містити істотні умови, передбачені законодавством для відповідного договору, і виражати намір особи, яка її зробила, вважати себе зобов'язаною у разі її прийняття.

Умови дійсності електронного договору можна поділити на традиційні та особливі. До традиційних можна віднести загальні умови дійсності, які передбачені законодавством (ст. 203 ЦК України) та додаткові, які передбачені сторонами і є обов'язковими для сторін, які

його підписали. До особливих умов можна віднести такі умови, які випливають із суті саме електронного договору, це, зокрема: електронна форма вчинення, використання відповідних засобів ідентифікації, електронна форма представлення інформації, спеціальні засоби безпеки тощо.

Отже, електронний договір, крім визначених ЦК України істотних умов для відповідного виду договору, може містити інформацію про: технологію (порядок) укладення договору; порядок створення та накладання електронних підписів сторонами договору; можливість та порядок внесення змін до умов договору; спосіб та порядок прийняття пропозиції укласти електронний договір (акцепту); порядок обміну електронними повідомленнями та інформацією між сторонами під час виконання ними своїх зобов'язань; технічні засоби ідентифікації сторони; порядок внесення змін до помилково відправленого прийняття пропозиції укласти електронний договір (акцепту); посилання на умови, що включаються до договору, шляхом перенаправлення (відсилання) до іншого електронного документа і порядок доступу до такого документа; спосіб зберігання та пред'явлення електронних документів, повідомлень, іншої інформації в електронній формі та умови доступу до них; умови виготовлення та отримання паперових копій електронних документів; можливість вибору мови, що використовується під час укладення та виконання договору тощо.

Електронний договір в межах чинного законодавства України розглядається як складова електронної комерції, а отже учасниками є суб'єкти електронної комерції, постачальники послуг проміжного характеру в інформаційній сфері, органи державної влади та органи місцевого самоврядування в частині виконання ними функцій держави або місцевого самоврядування. Законом визначено, що однією із сторін електронного договору обов'язково є юридична особа або фізична особа – підприємець (продавець (виконавець, постачальник) товарів, робіт, послуг). Слід зазначити, що на практиці велика кількість електронних договорів укладається саме між фізичними особами, які по суті відповідають спеціальному законодавству, однак не маючи статусу як мінімум ФОП, до них буде застосоване лиш базове законодавство, зокрема, ЦК України.

Відзначаючи специфіку електронних договорів, і враховуючи те, що важливим етапом укладення будь-якого договору є його підписан-

ня, зазначимо, що при укладенні договорів у цифровій (електронній) площині мова йде, насамперед, про ідентифікацію особи. Під такою ідентифікацією законодавець розуміє процедуру використання ідентифікаційних даних особи з документів, створених на матеріальних носіях, та/або електронних даних, в результаті виконання якої забезпечується однозначне встановлення фізичної, юридичної особи або представника юридичної особи, де ідентифікаційними даними особи є унікальний набір даних, який дає змогу однозначно встановити фізичну, юридичну особу або представника юридичної особи.

Враховуючи те, що оригіналом електронного документа вважається електронний примірник документа з обов'язковими реквізитами, у тому числі з електронним підписом автора або підписом, прирівняним до власноручного підпису (відповідно до Закону), законодавець закріпив рівні електронної ідентифікації, які можуть бути застосовані при вчиненні тих чи інших правочинів. Це, зокрема, високий, середній або низький рівні. Кожному з зазначених рівнів відповідають: кваліфікований, удосконалений та (просто) електронний підписи (КЕП, УЕП та ЕП відповідно).

Базовим законом в сфері ідентифікації осіб у електронній площині є Закон України «Про електронну комерцію», у ст. 12 якого зазначається, що «коли відповідно до акта цивільного законодавства або за домовленістю сторін електронний правочин має бути підписаний сторонами, моментом його підписання є використання: електронного підпису відповідно до вимог законів України «Про електронні документи та електронний документообіг» та «Про електронну ідентифікацію та електронні довірчі послуги», за умови використання засобу електронного підпису усіма сторонами електронного правочину; електронного підпису одноразовим ідентифікатором, визначеним цим Законом; аналога власноручного підпису (факсимільного відтворення підпису за допомогою засобів механічного або іншого копіювання, іншого аналога власноручного підпису) за письмовою згодою сторін, у якій мають міститися зразки відповідних аналогів власноручних підписів»[1].

У такому контексті виникає необхідність більш детально розглянути поняття криптографічного захисту інформації. У більшості

[1] Про електронну комерцію: Закон України від 03.09.2015 № 675-VIII. https://zakon.rada.gov.ua/laws/show/675-19#Text

країн, діяльність, яка пов'язана з криптографічним захистом інформації, підлягає правовому регулюванню. В Україні розробки в сфері криптографічного захисту інформації, також законодавчо закріплені. Зокрема, відповідно до ст. 7 Закону України «Про ліцензування видів господарської діяльності»[1] діяльність, пов'язана з наданням послуг в галузі криптографічного захисту інформації, ліцензується.

Визначення основних понять у сфері криптографічного захисту інформації міститься в Положенні про порядок здійснення криптографічного захисту інформації в Україні, затвердженому Указом Президента України[2].

Отже, криптографічний захист – це вид захисту, що реалізується за допомогою перетворень інформації з використанням спеціальних даних (ключових даних) з метою приховування (або відновлення) змісту інформації, підтвердження її справжності, цілісності,авторства тощо.

Разом з тим, безліч аспектів використання криптографії на законодавчому рівні в Україні залишаються неврегульованими. Зокрема, відсутні норми, які регламентують участь в діяльності, пов'язаної з криптографічним захистом інформації, фізичної особи без статусу суб'єкта господарювання. Також відкритим залишається питання про можливість примусового розкриття ключів шифрування користувачами на вимогу правоохоронних органів.

Особи, які прагнуть захистити власний особистий простір від несанкціонованого втручання шляхом розробки і застосування криптографічних алгоритмів і систем, в Україні мають можливість це зробити.

Технологія електронного підпису продовжує динамічно розвиватись. Наразі вже працюють сервіси, які допомагають встановити додаткові підстави довіри до особи, яка поставила на документі свій електронний підпис. В такому випадку, справжність електронного підпису перевіряється іншими сторонами правочину за раніше відомими ідентифікаторами, у відповідності до яких вони можуть ототожнити отриманий підпис з особою, яка вказана, за набором даних, доданих провайдером до електронного підпису.

---

[1] Про ліцензування видів господарської діяльності: Закон України від 02.03.2015 № 222-VIII. URL: https://zakon.rada.gov.ua/laws/show/222-19#Text

[2] Про Положення про порядок здійснення криптографічного захисту інформації в Україні: Указ Президента України від 22.05.1998 р.№ 505/98. URL: http://zakon3.rada.gov.ua/laws/show/505/98

Така перевірка може відбуватись за номером телефону або електронною адресою, яка вказується при реєстрації в системі надавача послуги електронного підпису. Обов'язок провайдера – перевірити за допомогою спеціального посилання-активації профілю та одноразового смс-паролю справжність вказаних додаткових ідентифікаторів, а також їх належність особі, яка створила акаунт в системі.

Проте, відповідний ризик компрометації електронного підпису усе ж залишається, хоча і складно уявити одночасний несанкціонований доступ і до електронної пошти особи, і до мобільного телефону, попри те, що окремі сервіси реєструють користувачів у системах надання електронних підписів виключно на основі вказаної при реєстрації електронної пошти.[1]

Ще одним введеним у дію електронним ідентифікатором в українському правовому полі на даний час є електронний підпис одноразовим ідентифікатором.[2] У Законі електронний підпис одноразовим ідентифікатором визначено як «дані в електронній формі у вигляді алфавітно-цифрової послідовності, що додаються до інших електронних даних особою, яка прийняла пропозицію (оферту) укласти електронний договір, та надсилаються іншій стороні цього договору. [3]

Отже, виникає ситуація, коли особі, що прийняла оферту, на етапі підтвердження укладання відповідного електронного договору, надсилається одноразовий ідентифікатор, який згодом вводиться нею для підтвердження укладання такого договору. Такий спосіб здається цілком прийнятним, адже відбувається і перевірка контактного номеру, і встановлюється сам факт волевиявлення з приводу укладання такого договору.

Проте, в загальному ланцюгу забезпечення чинності договору, обов'язок ідентифікації покладається на самого акцептанта – замовника товарів чи послуг. Такий висновок можна зробити на основі частини 8 ст. 11 закону, в якій зазначається, що у разі, коли укладення електронного договору відбувається в інформаційно-телекомунікаційній системі суб'єкта електронної комерції, для прийняття пропо-

---

[1] Горкуша М. Встановлення довіри до електронного підпису в Україні. URL: https://ilaw.net.ua/vstanovlennya-doviry-do-elektronnoho-pidpysu-v-ukrajini/

[2] Горкуша М. Правові засади регулювання ідентифікаторів в Україні. URL: https://ilaw.net.ua/pravovi-zasady-rehulyuvannya-identyfikatoriv-v-ukrajini/

[3] Про електронну комерцію: Закон України від 3 вересня 2015 р. № 675 VIII. *Офіційний вісник України.* 2015. № 78.

зиції укласти такий договір особа має ідентифікуватися в такій системі та надати відповідь про прийняття пропозиції. Іншими словами, йдеться про реєстрацію на сайті продавця із зазначенням відповідних ідентифікуючих даних, необхідних для укладання електронного договору, зокрема ім'я та прізвища, номера мобільного телефону (в контексті використання електронного підпису електронним ідентифікатором), e-mail та інших даних.

Однак магазин, все одно, не може перевірити надані параметри для ідентифікації. Адже повідомлення з одноразовим ідентифікатором буде надсилатись на вказаний особою мобільний телефон без встановлення особи. По суті, відбуватиметься лише підтвердження волевиявлення щодо особи із вказаними реєстраційними даними,. Натомість, встановити дійсну належність цих даних зазначеній особі неможливо.

Крім того, в контексті пошуку використання більш безпечного варіанту слід згадати, що існує ще один ідентифікатор, більш універсальний за значенням і такий, що містить в собі той самий електронний цифровий підпис, – картка громадянина, або ж ID-картка, яка в українському законодавстві відображена як паспорт громадянина України у формі картки з безконтактним електронним носієм.

Важливим також є доповнення, зроблене в ЦК України (ч. 2 ст. 639 ЦК України) у грудні 2020 року, а саме: «Якщо сторони домовилися укласти договір за допомогою інформаційно-телекомунікаційних систем, він вважається укладеним у письмовій формі». Отже, в даному випадку ми бачимо, що мова йде про вчинення електронного правочину.

Аналізуючи судову практику можна зробити висновок, що електронна ідентифікація та підтвердження волі сторони договору укласти даний договір (взяти на себе передбачені даним договором права та обов'язки) шляхом використання електронного підпису, одноразових ідентифікаторів тощо є відповідним засобом ідентифікації особи, а тому на підставі використання електронних ідентифікаторів не можна говорити про визнання укладеного договору недійсним. В підтвердження цьому виступив і Верховний Суд, який розглянув у порядку письмового провадження справу про захист прав споживачів, визнання недійсним договору, захист персональних даних[1]. Ана-

[1] Постанова Верховного Суду від 14 червня 2022 року у справі No 757/40395/20. URL: https://reyestr.court.gov.ua/Review/104769406

логічним є й висновок в Постанові Верховного Суду від 12 січня 2021 року[1].

Отже, можна погодитися з позицією Верховного Суду стосовно того, що будь-який вид договору, який укладається на підставі Цивільного або Господарського кодексів України, може мати електронну форму. Нині можна спостерігати значні можливості в сфері укладання договорів, підписування звітів, отримання державних послуг тощо он-лайн, доступ до яких відкривається шляхом електронної ідентифікації через електронний підпис.

Блокчейн[2]

Розвиток технологій у всьому світі з кожним днем набирає обертів. За останні роки, в умовах карантинів, можна було спостерігати не лише розширення застосування на практиці різного роду технологічних рішень, а й бачити все нові і нові відкриття. Важливою рушійною силою такого розвитку є, зокрема, бажання зекономити час, кошти (витрати), бути конкурентоздатним за умови великої конкуренції. Технологія блокчейн активно почала обговорюватися в більшості країн, зокрема, і в Україні, у 2017 році.

Під блокчейном необхідно розуміти розподілений публічний реєстр, заснований на сучасних криптографічних алгоритмах, що містить базу даних про всі раніше здійснені операції. Такий реєстр по своїй суті є децентралізованим. Дана система, за твердженням розробників, виключає крадіжку, шахрайство, порушення майнових прав тощо. Факти, що зберігаються в блокчейн не можуть бути загублені. Вони залишаються там назавжди. Крім того, блокчейн зберігає не лише кінцевий стан, а й усі попередні стани. Тому кожен може перевірити правильність кінцевого стану, перераховуючи факти від самого початку.

До переваг використання системи блокчейн відносимо: децентралізацію; доказовість кожної трансакції; прозорість; безпека; неможливість внесення змін у «підписаний» блок; обчислювальна логіка; економія часу; економія ресурсів.

---

[1] Постанова Верховного Суду від 12 січня 2021 року у справі № 524/5556/19. URL: https://reyestr.court.gov.ua/Review/94102130

[2] ІТ-право: практичний посібник. К.: Норма права, 2025. С. 139-145.

Разом з тим, поки ми ще не опанували повністю дані технології, а, отже, можемо говорити й про недоліки. Зокрема, це великі витрати електроенергії, проблеми з масштабністю, інерцією гравців ринку, необхідністю в деяких питаннях досягати консенсусу між великою кількістю учасників, відсутність законодавчої бази, навчання осіб-користувачів, придбання відповідного обладнання тощо (що в умовах воєнного часу ускладнює процес розвитку, чи хоча б втримання на тому рівні, що вже був досягнутий). Важливим також є питання «ментальної» та «моральної» готовності суспільства до активного використання у своєму житті таких сучасних технологій, адже хоч ми вже і звикли до Інтернету, де можна не лише скористатися інформаційними джерелами, але й проводити деякі власні операції, обмінюватися інформацією, використовувати соціальні мережі для спілкування, проходити навчання на відстані, проводити різного роду конференції, семінари, купувати та продавати товари тощо, здійснювати різного роду дії в рамках проєктів «електронного самоврядування» (що значно скорочує час та є вельми зручним), записатися на прийом до лікаря через електронну систему, подати позов до суду та отримати від суду документи в електронному вигляді та багато іншого, однак перевести абсолютно всі сфери свого життя в цифровий простір мабуть готовий не кожний.

Тому вважаємо, що для активного впровадження таких технологій як блокчейн необхідно не просто закріпити таку можливість, а сформувати єдину концепцію, яка б дала можливість поступово впроваджувати нові технологічні розробки, даючи можливість суспільству оцінити всі їх переваги, що згодом забезпечить гармонійний розвиток суспільства (зокрема, інформаційного), поєднає всі сфери життя в цілісний діючий механізм.

Отже, законодавець має забезпечити пріоритет «права над кодом», передбачити відповідні обмеження, яким має слідувати розробник або оператор коду. Адже, навряд чи можна характеризувати позитивно, наприклад, ситуацію коли код дозволятиме банку з огляду на прострочення по кредиту автоматично віддалено заглушити двигун вашого автомобіля, який опинився взимку на трасі, або блокування житла тощо.

Закріпити поняття блокчейну на законодавчому рівні вже мали місце. Зокрема, у жовтні 2017 року у Верховній Раді України був

зареєстрований проєкт Закону України «Про обіг криптовалюти в Україні»[1], в якому під блокчейном розуміється децентралізований публічний реєстр усіх проведених криптовалютних транзакцій, які були проведені суб'єктом криптовалютних операцій, а користувачем системи блокчейн є будь-яка фізична особа, фізична особа-підприємець або юридична особа, яка за допомогою власного та/або орендованого технічного обладнання підтримує працездатність системи блокчейн, здійснює проведення криптовалютних транзакцій та захисту системи блокчейн. Однак, даний документ на даний момент так і залишився проєктом, містить лиш деякі понятійні категорії та в основному описує криптовалюту, а не технологію блокчейн, правила її застосування на практиці та наслідки такого застосування.

Також маємо два визначення блокчейну в Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки[2], які по суті можна характеризувати як технічне та технологічне, відповідно: 1) програмно-комп'ютерний алгоритм децентралізованого публічного або приватного реєстру чи бази даних, функціонування якої забезпечується шляхом взаємодії через Інтернет однорангової мережі, або будь-яким іншим способом, що гарантує належний криптографічний захист усіх записів, транзакцій, проведених з використанням відповідної технології; 2) концепція, що може трансформувати державне управління в таких сферах, як реєстрація майнових прав, правосуддя, ідентифікація особи; як технологія довіри, блокчейн у державному секторі може використовуватися для електронних референдумів, петицій, голосування та інших сервісів електронного урядування; блокчейн забезпечує високоефективні механізми захисту цілісності та доступності інформації та дозволяє створювати повністю децентралізовані системи.

На даний момент можна констатувати, що найбільш активно розвивається застосування блокчейн-технології у сфері державних реєстрів. Однак, дана технологія може бути застосована у різних сферах нашого життя, зокрема, в банківській сфері, сфері страхування, освіти, держуправління, туризму, сферах розвитку штучного інтелекту,

[1] Про обіг криптовалюти в Україні: проект Закону України № 7183 від 06.10.2017 р. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=62684

[2] Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки та затвердження Плану заходів щодо її реалізації: розпорядження КМУ від 17.01.2018 р URL: http://zakon5.rada.gov.ua/laws/show/67-2018-р

Інтернету речей, системи доменних імен, комп'ютерної безпеки, краудфандингових платформ, онлайн-ринків та ін.

Однак, задля реального та стрімкого розвитку даної технології необхідним є визначення її правового статусу, вирішення таких проблем правового характеру, як: відповідальність держави за функціонування системи («класичний» блокчейн не передбачає контролю взагалі, однак якщо мова йде про використання його державними органами, де може бути застосована інформація з обмеженим доступом тощо – має бути використаний власний «приватний» блокчейн і тут правові питання цілком можуть бути врегульовані нормами чинного законодавства щодо захисту інформації); стимул для підтримки функціонування системи користувачами; питання захищеності інформації (насамперед від втрати та спотворення).

Зокрема, користувачів точно будуть турбувати такі питання, як: можливість захисту авторських прав за допомогою блокчейна; використання інформації, яка охороняється законом, в блокчейн-продуктах (наприклад, персональні дані, державна, комерційна, банківська таємниця та ін.); наявність у сторін цивільно-правового договору право та дієздатності. Що також підтверджує необхідність законодавчого закріплення використання блокчейну.

Досить широке коло можливостей, які надає використання блокчейну, останнім часом обговорюють в сфері удосконаленні економічних процесів. Це, зокрема, його впровадження в облікову систему, використання на фінансовому ринку, бухгалтерського обліку та аудиту, в сфері туризму, називають «новітнім фінансовим інститутом».

Можливим та достатньо надійним є перспектива використання блокчейн-технології для документування доказів воєнних злочинів рф в Україні. Таке фіксування надасть можливість в майбутньому використовувати дані про злочини в міжнародних судових процесах. А враховуючи те, що технологія блокчейн не дає можливість підробити чи змінити інформацію, яка там вже розміщена та визнається у всьому цивілізованому світі як надійна, можна сподіватися що зафіксовані докази будуть прийняти судами до уваги при винесенні рішень щодо притягнення до справедливого покарання військових злочинців.

Смарт-контракти[1]

Аналіз впливу розвитку інформаційних технологій на категорію правочину свідчить про позитивні зрушення в сторону спрощення укладення правочинів. Спочатку з'явилася можливість вчинити традиційний правочин в електронній формі, яка передбачає фіксацію умов правочину не на папері, а за допомогою різноманітних електронних документів, ознайомлення з якими обов'язково має супроводжуватися використанням спеціального обладнання. Сьогодні на порядку денному – поява нового різновиду правочинів – смарт-контракту, виникнення якого пов'язують із появою криптовалют та технології блокчейн.

Смарт-контракт може існувати лише в цифровій мережі. Всі дані щодо згоди повинні знаходитися в блокчейні та мати однакову правову цінність для сторін, які домовились про вчинення правочину. Смарт-контракт також виступає посередником між сторонами, він не перераховує кошти на рахунок продавця до того часу, поки не будуть виконані певна частина, або всі дії щодо виконання смарт-контракту сторонами. Смарт-контракти дозволяють обмінюватися грошима, власністю, акціями або іншими активами у більш зручному режимі, аніж при укладенні традиційних договорів. Також, на відміну від традиційних правочинів, смарт-контракти, крім зберігання інформації про зобов'язання сторін і штрафи за їхнє порушення, самі (автоматично) забезпечують виконання всіх умов правочину. Весь цей час документ зберігається і дублюється в децентралізованому реєстрі, що забезпечує його надійність і не дозволяє жодній зі сторін змінювати умови правочину.

Практичне застосування смарт-контрактів можливе у багатьох сферах, зокрема, у фінансовій сфері при кредитуванні, бухгалтерському обліку тощо (наприклад, для оцінки ризиків та аудиту в режимі реального часу); у сфері розвитку міста (розумний автомобіль, розумний будинок тощо); в юриспруденції (наприклад, при винесенні рішення суду, за умови використання технології «комп'ютерного судді», яка була створена науковцями Університетського коледжу Лондона та Університету Шеффілда). Однак, поки йдеться про аналіз даних та визначення можливого варіанта за принципом вірогідності,

[1] ІТ-право: практичний посібник. К.: Норма права, 2025. С. 146-150.

на законодавчому рівні використовувати в повній мірі смарт-контракти як повноцінну альтернативу традиційним договорам немає підстав. Досить великі надії у впровадженні смарт-контрактів мають представники бізнесу, які вбачають в них перспективи підтримання та розвитку своїх напрямів, отриманні значних прибутків завдяки використанню передових технологій та програм, конкурентоспроможності на міжнародних ринках тощо.

Використання такого роду технологій (як блокчейн) та програм (як смарт-контракт) в зазначених сферах мають свої позитивні та негативні риси. Однак можна зазначити, що глобалізація сама по собі передбачає уніфікацію всіх процесів незалежно від країни, фактично «стираються» всі кордони, мова йде про суспільство як цілісну систему, яка живе за єдиними принципами, правилами, нормами, традиціями та законодавством, яке відповідає цим загальноприйнятим нормам.

Аналіз практичного застосування смарт-контрактів показав, що вони є доволі ефективними та дійсно мають багато позитивних рис, але поки це окремі великі угоди (як, наприклад, міжнародні операції з поставки товарів, міжбанківські комерційні договори тощо), які не є масовими та не мають єдиного технологічного «шаблону».

Цікаво, що вперше концепцію смарт-контракту було викладено ще у 1994 році, однак тоді мова йшла про електронний протокол передачі інформації. Наступним «кроком розвитку» став 2010й рік, а саме набуття популярності криптовалют. Такі контракти могли бути записані у вигляді коду, збережені і продубльовані у системі, а їх виконання забезпечить мережа комп'ютерів, керуюча блокчейном. Тобто, під смарт-контрактом вже розуміли контракт на даних розподіленого реєстру блокчейн.

Головною метою розробників смарт-контракту було – відмовитися від централізації, тобто щоб всі системи взаємодіяли але не підпорядковувалися одній головній системі. В даному контексті важливим є визначення правового статусу такої програми як смарт-контракт, визнання її на законодавчому рівні як повноцінної альтернативи традиційній формі договору, фактично, вірівненню ситуації. В умовах рекодифікації цивільного законодавства важливим є передбачення таких правових конструкцій, які б враховували не лише сучасний ступінь розвитку технологій, а й передбачали подальший їх розви-

ток, були спроможні забезпечити правове регулювання новітніх ІТ рішень у сфері укладення договорів.

Аналіз іноземного законодавства на предмет регулювання питань щодо смарт-контрактів дає можливість стверджувати, що світ лиш придивляється до даних «нових можливостей» і не має єдиного підходу до законодавчого регулювання даних питань. Зокрема, нині юридичне визнання смарт-контрактів з фіксацією правових наслідків найбільше поширене в США, зокрема в таких штатах, як Арізона, Каліфорнія, Теннессі, Делавер, Вайомінг, Небраска, Іллінойс. Їх резиденти можуть використовувати цифрові автоматизовані смарт-контракти з юридичною підтримкою, навіть якщо вони не забезпечені класичними письмовими контрактами. В Європейському Союзі дане питання частково регулюється, зокрема, дії в договірних відносинах у комерційній та цивільній сферах можуть тлумачитися як розумні контракти. Однак, є й країни які лиш «придивляються» до смарт-контрактів, або ж чітко визначають їх «різновидом» традиційного контракту. Більшість науковців та практиків переконані, що всі поточні питання адаптації смарт-контрактів до законодавства будуть усунені, а сама технологія буде стрімко розвиватися, охоплюючи все нові сфери діяльності.

Все зазначене дає можливість стверджувати, що смарт-контракт є правовим договором, який має перспективу укріпитися в практичному використанні та, з часом, зайняти провідне місце в забезпеченні сфери договірного права.

Звичайно, для смарт-контракту необхідним є існування таких обов'язкових елементів, як: цифрова ідентифікація всіх цифрових сторін договору; використання приватного децентралізованого середовища, в яке і будуть записуватися смарт-контракти; конкретно описані умови виконання смарт-контракту, які учасники підтверджують одночасно. Важливим тут є й вільне волевиявлення сторін укласти даний контракт, однак саме щодо цього пункту є досить багато дискусій, адже сторони віддалено ідентифікуються і немає впевненості в тому, що відсутній примус, обман тощо. Також задля дійсності такого контракту та визнання його на рівні з традиційним договором необхідним є й дотримання всіх інших істотних умов, які є обов'язковими при вчиненні «звичайного» договору.

Також, як і в будь-якій сфері, не обходиться без «проблем». В контексті використання смарт-контрактів можна виділити два проблемних «напрямки»: технічний та правовий. До першого можна віднести проблеми, пов'язані з тим, що самі розробники та програмісти не завжди чітко уявляють характер функціонування смарт-системи. Зокрема, можуть виникати наступні проблеми: забезпечення конфіденційності; асекурація безпеки; масштабність; не вирішено питання про можливі об'єктивні причини неможливості виконання контракту у певний час.

До проблем правового характеру можна віднести наступне: втрачається значення поняття «зобов'язання», адже в смарт-контракті сторони виражають волю один раз, а саме в момент його укладення; існує припущення, що смарт-контракт не може бути порушений, отже не може мати місця ситуація, коли одна із сторін не виконує або неналежно виконує договір у випадку коли вважає, що в світлі обставин, що змінилися його невиконання вигідніше, ніж виконання. Таким чином, сторони не можуть зважаючи на нові обставини (навіть об'єктивні) відмовитися від виконання договору. Фактично, не можна говорити і про примушування до виконання зобов'язання в натурі; смарт-контракт не враховує можливість наявності таких вад при укладенні правочину, як наприклад, вади суб'єкта, вади волі тощо. Зазначені обставини мають бути враховані і не можуть ігноруватися, вони є підставою визнання правочину недійсним; смарт-контракти не передбачають можливості захисту слабкої сторони (наприклад, споживача); можливість використання смарт-контрактів у незаконних цілях або укладання контрактів, які порушують публічний порядок. При цьому не можна ігнорувати насторожене ставлення до криптовалют з боку низки державних органів у різних країнах; надмірна автономність смарт-контракту, що визнають і програмісти, стверджуючи, що функціонуванню цього виду контрактів не потрібна правова система, оскільки такі контракти можуть існувати і поза правом, як децентралізовані альтернативи цілісній правовій системі.

Наразі, чинний Закон України «Про електронну комерцію» визначає, що документування інформації повинно надавати змогу відтворювати її у візуальній формі, придатній для сприйняття людиною. Таке формулювання не відповідає концептуальному розумінню сутності смарт-контрактів як таких, а тому даний Закон не

може застосовуватися до регулювання такого типу договорів, як смарт-контракти.

Отже, враховуючи вже існуючу практику застосування таких технологій у світі можна зробити висновок про позитивні очікування від укладення договорів у вигляді смарт-контрактів, до яких зокрема, віднесено об'єднання всіх учасників договору в загальну мережу; доступність актуальної інформації про договір відразу всім її учасникам; виписування всіх документів в оригінальному вигляді всередині системи; неможливість підробки документів; відсутність потреби пересилки паперових версій документів на великі відстані; автоматична перевірка системою документів (або взагалі контроль за фактом відвантаження) і здійснення платежів. Таким чином, можна говорити про перспективність використання блокчейну, смарт-контракту і Інтернету речей у певному симбіозі. Нині ж можна говорити про можливість поєднання традиційного та нового формату, наприклад, укласти традиційний договір та передбачити його виконання за допомогою відповідної комп'ютерної програми. Це дозволить виконати вимоги чинного законодавства щодо умов укладення договору та отримати сторонам «вигоди» смарт-контрактів, зокрема, автоматичність виконання, безпеку, швидкість тощо.

Використання штучного інтелекту для укладення смарт-контрактів

Інтеграція штучного інтелекту в процес розробки, аналізу й автоматизації смарт-контрактів відкриває нові горизонти для підвищення ефективності, надійності та безпеки цифрових трансакцій.

Термін «смарт-контракт» розуміють як: по-перше, як програмний код, що автоматично виконується при дотриманні визначених умов (його функціонування забезпечується децентралізованою мережею блокчейну); по-друге, як цифрову угоду, яка автоматично виконує умови, закладені в її коді. Такі контракти функціонують у децентралізованих середовищах, зокрема на платформах Ethereum, Binance Smart Chain, Solana тощо. Вони є незмінними, прозорими та виконуються без посередників.

Під терміном «штучний інтелект» розуміють: по-перше, сукупність алгоритмів і методів, які дозволяють комп'ютерним системам імітувати людський інтелект, включаючи навчання, логіку, прогнозування та прийняття рішень; по-друге, галузь комп'ютерної науки, яка створює системи, здатні до самостійного навчання, прийняття рішень, розпізнавання мовлення, зображень та логічного мислення. У поєднанні з блокчейн-технологіями штучний інтелект виступає інструментом для аналізу великих обсягів даних, автоматизованої генерації коду та виявлення аномалій.

Аналізуючи питання використання штучного інтелекту для укладення смарт-контрактів, можна виділити певні етапи життєвого циклу смарт-контрактів та можливість (перспективність) застосування штучного інтелекту на кожному з виокремлених етапів. До етаів життєвого циклу смарт-контрактів віднесемо їх розробку, аналіз та верифікацію, автоматизацію укладення угод, а також виконання та моніторинг.

Отже, на етапі розробки смарт-контрактів штучний інтелект може автоматично генерувати код смарт-контракту на основі текстового опису умов угоди. Наприклад, використання великих мовних моделей, таких як GPT, дозволяє конвертувати юридичну мову в код на мовах Solidity або Vyper. Наприклад, юридична компанія Legalese розробила платформу, що дозволяє створювати смарт-контракти за допомогою інтерфейсу природної мови (користувач просто вводить умови договору, а система генерує валідний код для Ethereum).

На етапі аналізу і верифікації смарт-контрактів штучний інтелект здатен виявляти логічні помилки, вразливості та невідповідності в коді контракту. Використання методів машинного навчання дозволяє аналізувати великі обсяги даних із попередніх контрактів та прогнозувати ризики, виявити вразливості до їх розгортання в мережі. Інструменти на базі штучного інтелекту вивчають тисячі попередніх смарт-контрактів, ідентифікуючи небезпечні шаблони. Наприклад, інструмент MythX (партнер ConsenSys) використовує штучний інтелект для автоматизованого аудиту смарт-контрактів, він аналізує код Solidity, виявляє помилки безпеки та пропонує виправлення.

На етапі автоматизованого укладення угод системи на базі штучного інтелекту можуть автоматично знаходити найвигідніші умови для укладення угоди (наприклад, у сфері децентралізованих фі-

нансів), проводити переговори та адаптувати умови контракту під потреби сторін. Також штучний інтелект може виступати як інтелектуальний агент-посередник, який веде переговори між сторонами, формує оптимальні умови та укладає угоду. Такі агенти здатні оцінювати ринкові умови, враховувати юридичні обмеження і навіть використовувати блокчейн-орекли для отримання актуальної інформації. Наприклад, у децентралізованих фінансах платформа Kleros використовує штучний інтелект для вирішення спорів між сторонами смарт-контракту, залучаючи децентралізованих арбітрів.

Наостанок, на етапі виконання контрактів та проведення моніторингу інтелектуальні агенти можуть контролювати зовнішні дані (oracles), аналізувати їх та ініціювати виконання контракту при настанні обумовлених подій. Після активації смарт-контракту штучний інтелект може контролювати зовнішні джерела даних (наприклад, ціни з бірж, погодні умови, результати матчів) та запускати виконання контракту при настанні обумовлених умов. Наприклад, у сільськогосподарському страхуванні смарт-контракт може автоматично виплатити компенсацію фермеру у разі посухи, якщо погодний API повідомляє про відсутність дощів понад 30 днів (штучний інтелект використовується для валідації даних та фільтрації аномалій).

До переваг інтеграції штучного інтелекту в роботу із смарт-контрактами можна віднести: автоматизацію юридичних процесів і зменшення людського чинника; підвищення безпеки за рахунок виявлення вразливостей до моменту публікації контракту; оптимізацію вартості укладення угод; гнучкість та адаптивність контрактів до динамічних умов; зменшення витрат внаслідок відсутності відсутність потреби у посередниках (нотаріуси, юристи); прогнозування ризиків, адже штучний інтелект може проаналізувати історію контрагентів та виявити шахрайські дії; масштабованість; юридична прозорість, адже коди відкриті для перевірки, а історія виконання незмінна.

Окрім переваг варто виділити й певні виклики та обмеження, які існують на практиці. Зокрема, сюди варто віднести: юридичну невизначеність (смарт-контракти та штучний інтелект не завжди мають чітке правове регулювання); проблема інтерпретації (автоматизовані контракти не завжди враховують неоднозначність юридичної мови); проблеми етики та довіри до автономних рішень, що приймаються штучним інтелектом; технічна складність у забезпеченні пов-

ної прозорості та пояснюваності рішень штучного інтелекту; питання безпеки (попри аудит, існує ймовірність хакерських атак через помилки в логіці контракту або алгоритмах штучного інтелекту).

Враховуючи перспективність даного напрямку, у майбутньому варто очікувати появу повністю автономних систем, які зможуть вести переговори, укладати угоди, перевіряти дотримання умов і забезпечувати виконання контрактів без втручання людини. Особливий інтерес викликає застосування генеративного ШІ для автоматичної розробки «легальних цифрових агентів» у сфері Web3. В межах зазначеного вважаємо за необхідне роботу в таких напрямках: розробка інструментів для підвищення довіри до рішень системи; створення стандартів юридичної відповідності для смарт-контрактів у різних юрисдикціях; вдосконалення багатомовних моделей, які дозволять працювати з договорами у різних правових системах; інтеграція смарт-контрактів у системи цифрової ідентичності; розробка легальних агентів. Тобто штучного інтелекту, що може виступати в суді або арбітражі в якості сторони угоди.

Підводячи підсумок варто зазначити, що інтеграція штучного інтелекту в екосистему смарт-контрактів є логічним кроком на шляху до повної автоматизації юридичних і фінансових процесів у цифровому середовищі. Хоча існують певні бар'єри, потенціал цієї синергії обіцяє значне підвищення ефективності, безпеки та доступності правових механізмів у цифровій економіці.

Інтеграція штучного інтелекту в екосистему смарт-контрактів є потужним кроком до формування «розумної економіки», де угоди укладаються без конфліктів, з мінімальною участю людини. Водночас подальше поширення таких рішень потребує оновлення правового поля, удосконалення технологій безпеки та розвитку інфраструктури пояснюваних ШІ-систем.

Правочини в умовах ковіду та воєнного стану[1]

Повномасштабний початок ведення війни країною-агресором проти нашої держави спонукав до необхідності швидкого реагуван-

[1] Проблеми здійснення та захисту цивільних прав в умовах воєнного стану: моногр. За ред. Харитонова Є. О., Харитонвої О. І., Некіт К. Г. 2023. С. 113-122.

ня представників влади, державних органів, населення з метою вирішення великої кількості питань, з якими раніше ми не стикалися (принаймні в такому масштабі).

Внаслідок введення воєнного стану на території України відбулося багато змін правового характеру, зокрема, ми спостерігаємо стрімке превалювання публічного інтересу над приватним, необхідність жити за «новими правилами» з різного роду обмеженнями, зокрема, інтересів приватних осіб. Однак маємо пам'ятати, що в правовій державі, якою є Україна, не можна допустити порушення законних прав та інтересів суб'єктів правовідносин, зокрема, суб'єктів цивільних правовідносин. В даному контексті інститут правочину відіграє важливу роль, адже щодня ми стикаємося з необхідністю вчинити той чи інший правочин, а воєнний стан (що є специфічним та новим для кожного з нас) іноді потребує ще більш швидкого реагування та прийняття рішення про вчинення правочину (як, наприклад, укладення договору дарування, складання заповіту, довіреності тощо).

Необхідно зазначити, що формування інформаційного суспільства, глобалізаційні та інтеграційні процеси відбуваються вже не перший рік, що зумовило необхідність удосконалення правового інструментарію торгового обігу, а відтак і перегляду низки відомих цивілістичних категорій, комплексного оновлення цивільно-правових норм, закріплених в Цивільному кодексі, що отримало назву «рекодифікації». В межах такої рекодифікації було піднято питання про формування нової концепції «правочину», трансформації розуміння даного поняття.[1]

Спочатку ми навчилися за допомогою використання інформаційних технологій готувати до укладення та здійснювати процес укладення правочинів, тобто вчиняти їх в електронній формі. З вересня 2015 року в спеціальному нормативно-правовому акті, а саме Законі України «Про електронну комерцію»[2] було закріплено такі поняття,

[1] Давидова І. В. Формування нової концепції правочину в умовах рекодифікації цивільного законодавства. *Рекодифікація цивільного законодавства в умовах євроінтеграційних процесів:* моногр. За ред. Є. О. Харитонова, О. І. Харитонової. Київ: Норма, 2020. С. 68-81; Харитонов Є. О., Давидова І. В. Договори та правочини у Книзі першій ЦК України: «рекодифікаційний» потенціал: *Оновлення Цивільного кодексу України: формування підходів:* колективна моногр; за ред. Довгерта А. С., Харитонова Є. О. Одеса: Гельветика, 2020. С. 77-91.

[2] Про електронну комерцію: Закон України від 03.09.2015 р. URL: https://zakon.rada.gov.ua/laws/show/675-19

як «електронна торгівля», «електронний правочин», «електронний договір» тощо. Це певною мірою вплинуло на умови та порядок вчинення правочинів, визначення їх сторін, наслідки невиконання тощо, однак, практично, не змінило саме розуміння їхньої сутності. Аналіз же сформульованих понять дав можливість зробити висновок про те, що законодавець має на увазі правочини у традиційному його розумінні, оскільки змінюється лише характер спілкування сторін, спрощення вимог до оформлення правочинів тощо. Разом з тим, на нашу думку, мова йде не просто про електронну форму правочину, а про формування нової категорії, яка є наслідком формування інформатизації суспільства.

Таке забезпечення можливості в межах закону вчиняти правочини в електронній формі, без укладення паперових договорів, присутності сторін при його укладенні тощо є лише «перехідним» етапом та дає підґрунтя (основу) для формування правочинів «нового типу» (так званих «розумних» контрактів, які частіше позначаються терміном «смарт-контракти»[1]). Їх можна назвати «перспективними» правочинами, тобто такими, які можуть стати «звичайною справою» через 10-15 років.

Внаслідок поширення інформаційних технологій (зокрема, таких як блокчейн) та програм (таких як «смарт-контракт» тощо) та їхніх відчутних переваг ведеться мова не лише про удосконалення порядку укладення правочину, а про зміну самого розуміння його сутності. Тобто про існування нового типу правочинів, що формується в інформаційному суспільстві, до якого, на нашу думку, мають бути віднесені правочини, котрі сутнісно пов'язані з використанням інформаційних технологій. Із врахуванням цієї їх особливості вони можуть іменуватися «IT-правочини»[2].

Блокчейн, як інструмент реалізації різних важливих проєктів не лише в сфері бізнесу, але й державному регулюванні знаходиться на початку свого шляху. За твердженням розробників дана система виключає крадіжку, шахрайство, порушення майнових прав тощо. Факти, що зберігаються в блокчейн не можуть бути загублені.

---

[1] Терміни «смарт-контракт», «розумний контракт» є традиційними, однак тут мається на увазі будь-які правочини (як одно-, дво- та багатосторонні договори, які можуть вчинятися суботами цивільних правовідносин).

[2] Давидова І. В. Правочини та їх недійсність в інформаційному суспільстві: автореф. дис. … д-ра юрид. наук: 12.00.03. Одеса, 2018. С. 17.

Що ж стосується «смарт-контрактів», то це контракт на даних розподіленого реєстру блокчейн, де основою його реалізації є програмування з використанням принципу «якщо…, то….», тобто умова прямо визначена в контракті.[1]

Першим викликом, який суспільство намагалося подолати, стала коронавірусна хвороба. Це був виклик як для суспільства в цілому, так і для кожного окремо. Крім необхідності дотримуватися певних правил та обмежень, постраждала економіка багатьох країн світу, актуалізувалися питання співвідношення публічних та приватних інтересів, пріоритетність питань стосовно здоров'я, а не «роботи до виснаження», адже навіть «просто послаблений імунітет» міг спричинити, як наслідок, серйозне захворювання і навіть смерть.

Так, ст. 29 Закону України «Про захист населення від інфекційних хвороб», постановою Кабінету Міністрів України від 11 березня 2020 р. № 211 «Про запобігання поширенню на території України гострої респіраторної хвороби COVID-19, спричиненої коронавірусом SARS-CoV-2» з 12 березня 2020 р. до 22 травня 2020 р. було встановлено на всій території України карантин, який передбачав ряд обмежень та правил, які мають на меті запобігти поширенню даного захворювання. Зокрема, відповідно до Порядку проведення протиепідемічних заходів, пов'язаних із самоізоляцією осіб, який також затверджений 11 березня 2020 року, досить велика група людей підлягала самоізоляції, серед яких: особи, які мали контакт з пацієнтом з підтвердженим випадком COVID-19; особи, щодо яких є підозра на інфікування, або особи, які хворіють на COVID-19 в легкій формі та не потребують госпіталізації; особи, що дали згоду на самоізоляцію з використанням електронного сервісу «Дій вдома» Єдиного державного веб-порталу електронних послуг; особи, які досягли 60-річного віку (за деякими винятками). Також до цієї групи можна віднести і осіб, які не досягли 14 років, яким відповідно до аналізованої Постанови заборонено пересуватися без супроводу законних представників або повнолітніх родичів дитини. Отже, досить велика група осіб повинна була здійснювати покупки не виходячи з дому.

Виходом з ситуації тут стало більш активне використання можливостей інформаційних технологій при вчиненні правочинів, зокрема,

[1] Що таке Смарт-Контракт? URL: http://ethereum.net.ua/discussion/34/scho-take-smart-kontrakt

при купівлі товарів, де інтернет-магазини і служби доставки мали чи не найбільший попит. Крім того, звичайні крамниці, які не мали права працювати офлайн (наприклад, крамниці одягу, взуття тощо) і мали офіційний сайт «номінально», – перейшли в он-лайн простір та намагаються втримати своїх клієнтів.

Короновірус, звичайно, завдав багато шкоди людству, однак частково «підготував» нас до необхідності працювати та комунікувати онлайн. Виходом з ситуації при укладенні правочинів стало активне використання можливостей інформаційних технологій, зокрема, при купівлі товарів, де інтернет-магазини і служби доставки мали чи не найбільший попит. Крім того, звичайні крамниці, які не мали права працювати офлайн (наприклад, крамниці одягу, взуття тощо) і мали офіційний сайт «номінально», – перейшли в онлайн простір і намагалися максимально втримати своїх клієнтів.

Таким чином, із запровадженням обмежувальних заходів ми спостерігали ситуацію, коли звичні для нас (традиційні) договори трансформуються за допомогою запровадження інформаційних технологій в електронні договори, смарт-контракти тощо, які можуть укладатися сторонами без особистого контакту, паперових копій договорів, особистих (власноручних) підписів тощо. Це свого роду нова фаза розвитку, момент, який має відбутися не лише в сфері технічного забезпечення можливостей такого укладення правочинів, але й в свідомості кожної особи.

Враховуючи те, що учасниками цивільних правовідносин є фізичні та юридичні особи, а також держава Україна, Автономна Республіка Крим, територіальні громади, іноземні держави та інші суб'єкти публічного права, всі вони можуть бути сторонами договорів, у будь-якому сполученні, зокрема: між фізичними особами; між фізичними та юридичними особами; між юридичними особами; між фізичними особами та публічними утвореннями тощо.

Зазначимо, що розвиток інформаційного суспільства та інформаційних технологій, який зробив популярним укладення договорів он-лайн, має такі переваги, як швидкість, оперативний обмін інформацією, зручність зберігання, оброблення, відправлення документів тощо. В умовах необхідності віддаленої роботи він набув особливої актуальності, адже вчинення договорів за допомогою інформаційних технологій є не просто актуальним, а життєво необхідним для

суспільства, особливо для осіб, що перебувають на самоізоляції (за умови, коли мова йде про пандемію) або ж взагалі в іншому регіоні чи іншій країні (за умови, якщо ми говоримо про воєнний стан), належать до групи ризику, не мають можливості самостійно здійснити покупки тощо. Крім цього, внаслідок обмежень необхідний товар (непродовольчого призначення, в який входить великий перелік нагально необхідних речей) може бути доступним лише в інтернет-магазині. Тому аналіз правової природи, сутності електронних договорів, смарт-контрактів, їх особливостей є дуже актуальним. Знов таки, не всі регіони нині можуть отримати бажаний товар, адже не всі поштові відділення працюють і не на всіх складах є відповідні товари. Також у контексті воєнного стану ми стали свідками того, що логістична проблема є набагато більшою та глибшою, аніж можна було собі уявити.

Як уже було зазначено вище, законодавець виділяє як традиційне поняття «договір», що закріплене в ЦК України, так і поняття «електронний договір». Оферта має містити істотні умови, передбачені законодавством для відповідного договору, і виражати намір особи, яка її зробила, вважати себе зобов'язаною у разі її прийняття. Важливими тут є як «традиційні» так і «особливі» умови дійсності відповідного договору.

В умовах введення воєнного стану та проведення активних бойових дій на території України вчинення електронного правочину, а також можливість його виконання або ж вчинення необхідних дій для уточнення умов тощо має важливе практичне значення, а іноді це єдина можливість захистити права та інтереси осіб в умовах що склалися. Саме практична значущість та необхідність вчинення відповідних дій у «віддаленому» форматі є забезпеченням можливості продовження життя в тому руслі, що було до 24го лютого 2022 року (наскільки це можливо).

Відзначаючи специфіку електронних договорів, і враховуючи те, що важливим етапом укладення будь-якого договору є його підписання, зазначимо, що при укладенні договорів у цифровій (електронній) площині важливе значення має питання щодо ідентифікації особи. Під такою ідентифікацією законодавець розуміє процедуру використання ідентифікаційних даних особи з документів, створених на матеріальних носіях, та/або електронних даних, в результаті

виконання якої забезпечується однозначне встановлення фізичної, юридичної особи або представника юридичної особи, де ідентифікаційними даними особи є унікальний набір даних, який дає змогу однозначно встановити фізичну, юридичну особу або представника юридичної особи[1]. Враховуючи особливості ІТ середовища, будь-яка правова дія в електронній площині не може обійтися без ідентифікації.

Закон України «Про електронні довірчі послуги» (ст. 15) визначає, що схема електронної ідентифікації повинна встановлювати високий, середній або низький рівні довіри до засобів електронної ідентифікації, що використовуються в них. Нині генерування електронного підпису може зайняти декілька хвилин, що досить зручно та позитивно впливає на швидкість вчинення відповідних юридичних дій. Така ситуація дала можливість розширити перелік ситуацій, де може бути застосовано електронний підпис. Наприклад, в освітньому процесі така можливість використовується під час укладення договору про надання освітніх послуг, прийняття заліків та іспитів у здобувачів вищої освіти, подачі за загальний розгляд свого дисертаційного дослідження майбутнім доктором філософії тощо. Особливо важливим ідентифікація викладачів, які здійснюють навчальний процес в умовах воєнного стану далеко від дому, не мають фізичної можливості знаходитися в закладі освіти, де вони працюють. Це дає можливість не припиняти надання освітніх послуг, не втрачати як викладачів (яким необхідно мати заробіток та можливість кормити свою сім'ю), так і здобувачів освіти.

Отже, навіть якщо особа фізично не знаходиться на території України, вона може продовжувати працювати, навчатися, бути активним учасником цивільно-правових відносин, укладати договори та виконувати їх тощо.

Разом з тим, не можна забувати й про недоліки цифровізації, зокрема, можливість зламу системи, отримання доступу злочинцями, шахраями тощо до «закритої» інформації. Така ситуація мала місце і при роботі з Єдиним державним веб-порталом електронних послуг «Дія» (стався витік персональних даних і їх відкриття для публічного ознайомлення). Маємо надію на те, що розвиток технологій та збіль-

[1] Про електронні довірчі послуги: Закон України від 05.10.2017 р. № 2155-VIII. URL: https://zakon.rada.gov.ua/laws/show/2155-19

шення спеціалістів в галузі кібербезпеки буде позитивно впливати на рівень захисту інформації, в тому числі, персональних даних.

Отже, «в центрі» будь-яких суспільних (а отже, і цивільних) відносин є приватні особи, суб'єкти приватного права, учасники цивільних відносин, що має враховуватися при формуванні норм і правил приватного (цивільного) права, які визначають взаємини членів суспільства одне з одним і з державою, як суб'єктом приватних відносин. Дані питання не втрачають своєї актуальності і в умовах воєнного стану (війни). Зокрема, на практиці виникає чимало проблем в даному напрямку. Якщо ж говорити більш конкретно, зокрема, стосовно вчинення та виконання правочинів в даних умовах, то необхідно зазначити, що досить велика кількість зобов'язань не виконуються в строк або ж не виконуються взагалі. Також постає питання про суб'єктний склад укладених правочинів. Адже Україна впродовж війни, яка триває вже більше півроку, втратила багато людей, кожен з яких мав свої приватно-правові зобов'язання, і не завжди є фізична можливість (знаходження в іншій країні, в регіонах активних бойових дій, в полоні тощо) та юридичне обґрунтування (доведення правонаступництва, представлення законних інтересів тощо) виконати зобов'язання. Звичайно, війна це форс-мажорна обставина, що позитивно вплине на результат більш пізнього виконання зобов'язань та не буде мати негативних наслідків у виглядів додаткових штрафних санкцій, однак глобально ситуація досить складна. Тут є і проблеми вчинення нових правочинів, наприклад, заповітів, дарування, договорів купівлі-продажу нерухомості тощо. Аналіз обмежень, які мали місце з початку війни в зазначених сферах, звичайно, є обґрунтованими з позиції публічного управління та прагнення держави захистити учасників цивільно-правових відносин від дій зловмисників (як то продаж нерухомості є неможливим без доступу до відповідних реєстрів; робота нотаріуса (в деяких випадках) є неможливою без входження його у спеціальний перелік нотаріусів, якими в умовах воєнного стану вчиняються нотаріальні дії щодо цінного майна[1] або ж якщо в даному регіоні ведуться бойові дії (внаслідок чого припинено доступ до єдиних та державних реєстрів) тощо).

[1] Мін'юстом затверджено перелік нотаріусів, якими в умовах воєнного стану вчиняються нотаріальні дії щодо цінного майна. URL: https://www.kmu.gov.ua/news/minyustom-zatverdzheno-perelik-notariusiv-yakimi-v-umovah-voyennogo-stanu-vchinyayutsya-notarialni-diyi-shchodo-cinnogo-majna

Підбиваючи підсумок можна впевнено стверджувати, що використання інформаційно-телекомунікаційних систем для вчинення правочинів розширює можливості як фізичних осіб, зокрема, дає можливість здійснювати необхідні дії, які забезпечують виникнення та припинення цивільних правовідносин, так і ФОП й юридичних осіб, зокрема, допомагає працювати та отримувати прибуток; все це в сукупності дає нам надію на забезпечення більш-менш нормального ритму життя особи в умовах воєнного стану та можливості захистити її цивільні права.

Підводячи підсумок необхідно зазначити, що у сучасних умовах збройного конфлікту та гібридних загроз, коли існує високий ризик втручання ворога в документообіг – як паперовий, так і традиційний електронний, – технологія блокчейн набуває особливої значущості. Її децентралізована, захищена від підробок і втручань структура забезпечує збереження достовірності юридично значущих дій навіть в умовах окупації, на тимчасово непідконтрольних територіях або в «сірій зоні». Це робить блокчейн ефективним інструментом для укладення договорів у критичних ситуаціях, коли традиційні форми правового оформлення втрачають надійність. Впровадження цієї технології може стати запорукою стабільності цивільно-правових відносин у періоди надзвичайної загрози.

Ключові слова: цивільне право, цивільні правовідносини, правочин, договір, ІТ-право, інформаційні технології, інформаційне суспільство, цифрова доба, гібридна війна, воєнний стан, соціальні мережі, смарт-контракт, блокчейн, штучний інтелект, відповідальність.

Розділ 10

ПОРУШЕННЯ ПРАВ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ В МЕРЕЖІ ІНТЕРНЕТ ПІД ЧАС ГІБРІДНОЇ АГРЕСІЇ В УМОВАХ ВОЄННОГО СТАНУ

DOI

Наталія Бааджи
кандидатка юридичних наук, доцента

У сучасному світі, що стрімко розвивається під впливом глобалізації, розвитку інформаційно-комунікаційних технологій (ІКТ) і постійних трансформаційних процесів, питання захисту прав інтелектуальної власності набуває особливої актуальності. Наразі саме інтелектуальна діяльність є рушійною силою соціально-економічного розвитку, як на національному, так і на міжнародному рівні. Однак, розвиток інтелектуальної сфери призводить до зростання кількості і урізноманітнення видів порушень. Це, в першу чергу, є наслідком недостатньої правової свідомості та ігнорування права власності на інтелектуальні продукти, технологічні новації [1]. Інтелектуальна власність є важливою складовою ВВП країни, а відтак, потребує відповідного рівня охорони і захисту.

Сьогодні масштаби правопорушень у сфері інтелектуальної власності зростають в усьому світі, особливо у сфері авторського права і суміжних прав. Як свідчить світова практика, шкода від цих порушень сягає астрономічних цифр. Окремо слід звернути увагу на збільшення і урізноманітнення таких порушень в Інтернеті.

Глобалізаційні процеси сприяють поширенню інноваційних рішень і створенню нових цифрових продуктів, що потребують ефективного правового захисту. Виклики, пов'язані з кіберзлочинністю, інформаційними війнами та неконтрольованим, не-

[1] Бошицький Ю. Л. Деякі організаційно-правові аспекти удосконалення правової охорони інтелектуальної власності в сучасній Україні. *Часопис Київського університету права.* 2020. № 3.; Колісник А. С. Сучасні проблеми захисту прав інтелектуальної власності (на основі судової практики). *Науковий вісник Ужгородського університету*: серія: Право. 2023.Т. 1. Вип. 78.С. 192-197.

правомірним розповсюдженням інтелектуальних ресурсів, вимагають розробки сучасних підходів до забезпечення правової охорони інтелектуальної власності. В умовах глобалізації та розвитку інформаційних технологій порушення прав інтелектуальної власності набувають транскордонного характеру, а цифровізація економіки вимагає посилення захисту цифрових активів. Саме питанням боротьби з порушеннями прав інтелектуальної власності в глобальній мережі Інтернет була присвячена 16 сесія Консультативного комітету ВОІВ, яка відбулась в Женеві 31січня-2 лютого 2024 року[1].

Означена проблема стає ще більш гострою в умовах воєнного стану, в якому Україна знаходиться внаслідок зовнішньої агресії рф з 2022 року[2]. Війна є кризовим явищем, яке вимагає адаптації правових механізмів до нових реалій, що повинно бути спрямоване, зокрема, на забезпечення балансу між захистом прав інтелектуальної власності та потребами суспільства в умовах війни.

Воєнні конфлікти не лише забирають у людей життя і майбутнє, завдають шкоди економіці, інфраструктурі та соціальній сфері, але й створюють загрози для правового регулювання інтелектуальної власності. У таких умовах порушення авторських прав, незаконне використання об'єктів патентного права та брендів стає частішим, ускладнюючи забезпечення належного рівня їхнього захисту.

Об'єкти інтелектуальної власності відіграють ключову роль у виробництві товарів та послуг, особливо в умовах воєнного часу, коли активно розвивається оборонна сфера. Створення нових видів озброєння, комп'ютерних програм, патріотичних пісень та творів мистецтва генерує нові об'єкти авторських прав та суміжних прав і підкреслює важливість захисту інтелектуальної власності для економіки та оборони України[3].

---

[1] Боротьба з порушеннями прав інтелектуальної власності в Інтернеті. Огляд матеріалів до засідання Консультативного комітету Всесвітньої організації інтелектуальної власнсоті із захисту прав / IP OFFECE. Липень 2024. URL: https://nipo.gov.ua/wp-content/uploads/2024/07/porushennia IP prav v interneti.pdf

[2] Про введення воєнного стану в Україні: Указ Президента України від 24 лютого 2022 року№ 64/2022. URL: https://www.president.gov.ua/documents/642022-41397

[3] Єрофєєнко Л. Правовий аналіз законодавства щодо захисту прав інтелектуальної власності під час дії воєнного стану. URL: Приватно-правові та публічно-правові відносини: проблеми теорії та практики: матеріали III Міжнар. конф.(м. Кропивницький, 2023). С. 210-214.

Людські життя та руйнування міст є першочерговими проблемами в умовах гібридної війни, разом з тим, ігнорування росією міжнародних норм інтелектуальної власності є ще одним проявом її зневаги до міжнародного права і потребують дзеркального реагування.

За час війни в Україні зменшилася кількість заявок на реєстрацію об'єктів інтелектуальної власності. Загалом повномасштабне вторгнення хоч і спричинила зменшення заявок до українського IP-офісу, але воно не стало критичним. Так, якщо у 2021 році на винаходи було подано 3390 заявки, то у 2022-му їх кількість зменшилася лише до 2758, збільшуючись в подальшому до 2911 у 2023 р[1]. Фактично така ж хвилеподібна тенденція характерна і для заявок на інші об'єкти промислової власності. Разом з тим, статистика перших місяців 2025 року є дещо негативною у порівнянні з відповідними місяцями 2024 року[2].

Як зазначила О. Орлюк, «IP в умовах війни – це надзвичайно важлива сфера, адже мова не лише про бренд «Україна», а й про наше економічне виживання зараз, і про наше процвітання в майбутньому»[3].

Можливість відстоювати власні інтереси, права та свободи є фундаментальною характеристикою правової держави. Відповідно до цивільного законодавства України, кожен громадянин має право на захист своїх прав у разі їх порушення, невизнання або оспорювання. Охорона прав інтелектуальної власності забезпечується різними механізмами та процедурами, передбаченими як національним законодавством, так і міжнародними нормами. Одним із ключових способів захисту є притягнення порушників до відповідальності.

---

[1] Барбашин С. Аспекти захисту інтелектуальної власності в Україні під час війни. URL: https://unba.org.ua/publications/9042-aspekti-zahistu-intelektual-noi-vlasnosti-v-ukraini-pid-chas-vijni.html; Інтелектуальна власність в цифрах. Показники діяльності у сфері інтелектуальної власності за 2023 рік. URL:https://nipo.gov.ua/wp-content/uploads/2025/01/IP-in-Figures-2023-web 1-.pdf

[2] Показники надходження та розгляду заявок і реєстрації об'єктів промислової власності за лютий 2025 року. URL: https://nipo.gov.ua/wp-content/uploads/2025/03/February-2025- UKRNOIVI-statistics-UA-web.pdf ; Показники надходження та розгляду заявок і реєстрації об'єктів промислової власності за січень 2025 року. URL: https://nipo.gov.ua/wp-content/uploads/2025/02/January-2025- UKRNOIVI-statistics-UA-web.pdf

[3] Орлюк О. Інтелектуальна власність в умовах війни – це надзвичайно важливо. URL: https://ukrainky.com.ua/olena-orlyuk-intelektualna-vlasnist-v-umovah-vijny-cze-nadzvychajno-vazhlyvo/

Конституція України, у ст. 41 закріплює право кожного «володіти, користуватися і розпоряджатися своєю власністю, результатами своєї інтелектуальної, творчої діяльності»[1]. Конституція України гарантує кожному «свободу літературної, художньої, наукової і технічної творчості, захист інтелектуальної власності, їхніх авторських прав, моральних і матеріальних інтересів, що виникають у зв'язку з різними видами інтелектуальної діяльності»[9].

Необхідність охорони і захисту прав інтелектуальної власності підтверджується наявністю міжнародних нормативно-правових актів, які закріплюють низку стандартів у цій сфері. Серед таких варто назвати Угоду про торговельні аспекти прав інтелектуальної власності (Угода ТРІПС) від 15.04.1994 р., Бернську конвенцію про охорону літературних і художніх творів від 24.07.1971 р., Паризьку конвенцію про охорону промислової власності від 20.03.1883 р. Перелічені документи виокремлюють мінімальні вимоги до правової охорони інтелектуальної власності, а Угода ТРІПС встановлює справедливі й рівні для всіх процедури захисту прав, які не є необґрунтовано обтяжливими, складними або затратними, а також не обмежуються в часі для прийняття дій.

До ключових міжнародних та правових актів щодо захисту авторського права в Інтернеті відносять Інтернет-договори ВОІВ (1996) (Договір ВОІВ про авторське право (WIPO Copyright Treaty, WCT) та Договір ВОІВ про виконання і фонограми (WIPO Performances and Phonograms Treaty), Директиви ЄС щодо авторського права (Директива 2000/31/ЄС («Директива про електронну комерцію»), ухвалена 8 червня 2000 року, яка регулює правові аспекти надання інформаційних послуг у цифровому середовищі; Директива 2019/790/ЄС, прийнята 17 квітня 2019 року, яка регулює авторське право на Єдиному цифровому ринку та вносить зміни до попередніх директив (96/9/ЄС та 2001/29/ЄС), а також Digital Millennium Copyright Act (DMCA, 1998) (американський закон, що посилює захист авторських прав у цифрову епоху, зокрема регулює відповідальність інтернет-провайдерів і боротьбу з обхідними технологіями захисту контенту.

До національних нормативно-правових актів, які регламентують охорону і захист прав інтелектуальної власності відносяться, зокре-

[1] Конституція України від 28.06.1996 № 254к/96-ВР. URL: https://zakon.rada.gov.ua/laws/card/254%D0%BA/96- %D0%B2%D1%80

ма: Конституція України, Цивільний кодекс України, Кримінальний кодекс України, Кодекс України про адміністративні правопорушення, Господарський кодекс України (до втрати чинності у 2025), «Про захист від недобросовісної конкуренції», «Про авторське право і суміжні права», «Про охорону прав на винаходи і корисні моделі», «Про охорону прав на промислові зразки», «Про охорону прав на знаки для товарів і послуг», «Про охорону прав на сорти рослин» тощо.

Станом на 2025 рік, українське законодавство щодо захисту прав інтелектуальної власності (ІВ) в Інтернеті зазнало суттєвих змін, спрямованих на адаптацію до цифрової епохи та гармонізацію з європейськими стандартами. Так, оновлений Закон України «Про авторське право і суміжні права» враховує сучасні виклики цифрового середовища, зокрема: розширення прав та обов'язків інтернет-провайдерів щодо запобігання порушенням ІВ; визначення процедур блокування доступу до нелегального контенту; впровадження механізмів «notice and takedown» для оперативного реагування на порушення. Закон «Про електронну комерцію» **в**изначає правові засади для електронних транзакцій та містить положення щодо захисту ІВ в онлайн- торгівлі.

Слід зазначити, що Україна активно співпрацює з Всесвітньою організацією інтелектуальної власності (ВОІВ) та іншими міжнародними інституціями для вдосконалення механізмів захисту ІВ в Інтернеті.

Хоча законодавство містить чимало норм, спрямованих на захист інтелектуальної власності, на практиці це не завжди ефективно. Судова практика та дані про притягнення до відповідальності показують, що порушення прав інтелектуальної власності залишаються поширеним явищем.

Статистика Касаційного господарського суду у складі Верховного Суду (КГС ВС) ілюструє, «що протягом 2022 року на розгляд КГС ВС надійшло на 63,4% менше звернень з ІР-спорів, ніж у 2021-му. Тоді як у 2023 році, порівняно з показниками 2022-го, збільшилася кількість розглянутих КГС ВС справу сфері інтелектуальної власності на 19,1% (за даними статистики КГС ВС 2023 року)»[1].

[1] Ярошевська Я. Розвиток судової ІР-практики в умовах війни URL: https://yur- gazeta.com/publications/ practice/zahist-intelektualnoyi-vlasnosti-avtorske-pravo/rozvitok-sudovoyi-ippraktiki-v- umovah-viyni.html

Серед актуальних проблем захисту прав інтелектуальної власності в Україні виділяються питання реєстрації торговельних марок і знаків, а також дотримання цих прав у медіапросторі, зокрема в Інтернеті. Попри наявні заходи щодо законного поширення творів та інших об'єктів інтелектуальної власності, вони не завжди ефективні через відсутність належного контролю. Навіть механізми модерації веб-сайтів і соціальних мереж, які частково обмежують доступ до контенту, що порушує права інтелектуальної власності, не можуть повністю гарантувати їх дотримання. З кожним роком ризики порушень лише зростають, і навіть офіційна реєстрація об'єкта інтелектуальної власності не забезпечує його повного захисту[1]

Відтак можна стверджувати, що дослідження проблеми порушення прав інтелектуальної власності в мережі Інтернет в умовах гібридної війни має не лише теоретичне, але й практичне значення для забезпечення національної безпеки, економічного розвитку та міжнародної інтеграції України.

На актуальність окресленої проблематики вказує і тематика форуму, що проходив у межах Тижня інтелектуальної власності 2024, присвяченого World IP Day 2024, який відзначався під егідою Всесвітньої організації інтелектуальної власності – «Від моніторингу до захисту: інструменти права інтелектуальної власності»[2].

Слід зазначити, що український IP офіс оперативно відреагував на російську збройну агресію, зупинивши провадження експертизи заявок, здійснення реєстрації та розпоряджання правами. Одночасно з цими практичними заходами розпочалась робота з формування правового поля для недопущення набуття та розпоряджання російськими IP правами в Україні[3]. На базі IP офісу сьогодні працює Центр спостереження за порушеннями прав інтелектуальної власності[4] завдання якого націлені на об'єднання правоохоронних органів,

[1] Колісник А. С. Сучасні проблеми захисту прав інтелектуальної власності (на основі судової практики). *Науковий вісник Ужгородського університету*: серія: Право. 2023.Т. 1. Вип. 78.С. 192-197.

[2] Від моніторингу до захисту: інструменти права інтелектуальної власності. URL: https:// supreme. court.gov.ua/ supreme/pres-centr/news/1596771/

[3] Санкції проти агресора в дії: IP відомства країн ЄС більше не приймають заявки від росіян. URL: https://nipo.gov.ua/sanktsii-proty-ahresora/

[4] Центр спостереження з питань порушень прав інтелектуальної власності: для чого створено і як працюватиме новий майданчик IP офісу. URL: https://nipo.gov.ua/ukr-tsentr-sposterezhennia-porushen-ip-prav/

держави й тих, хто володіє правами з метою забезпечення якісного, сучасного та належного захисту прав інтелектуальної власності[1].

У 2022 році «росія формально легалізувала порушення IP прав іноземних правовласників з країн, які висловили солідарність Україні та запровадили санкційні та інші обмежувальні заходи проти росії. За вже усталеними традиціями росією було сформульовано список так званих «недружніх» країн, до яких росія віднесла країни-члени Європейського Союзу, Велику Британію, Канаду, США, Японію та багато інших»[2].

«Після цього росія запровадила цілу низку обмежень для правовласників з цих країн в IP сфері, зокрема: дозволила російським юридичним та фізичним особам не виплачувати компенсації за використання винаходів, корисних моделей та промислових зразків; обмежила можливості іноземних правовласників збирати ліцензійні платежі за більшістю видів IP прав; відмовляла у судовому захисті тощо.

Весь світ побачив цілу низку кричущих прикладів експропріації всесвітньо відомих брендів та їх бізнес-практик, нелегальний прокат та демонстрацію кінематографічних творів з «недружніх» країн тощо»[3].

Повномасштабна війна в Україні наочно демонструє, що країна проходить надзвичайно складне випробування, проте робить це гідно та впевнено, крок за кроком. Україна протистоїть ворогу не лише на полі бою, а й у всіх сферах життя, зокрема в цифровому просторі. Кількість кібератак під час війни зросла утричі, поряд із масованими мережевими атаками, поширенням фейків та інформаційними маніпуляціями з боку країни-агресора. Війна створила серйозні виклики для всіх аспектів суспільного життя, зокрема й для сфери інтелектуальної власності. Безумовно, подолати ці труднощі було б неможливо без міжнародної підтримки.

Так, Міжнародна коаліція по боротьбі з підробками (IACC) у своєму зверненні до USTR зазначила: «Загальна депріоритизація захисту прав інтелектуальної власності російським урядом призвели до ство-

[1] Моніторинг порушень і боротьба з контрафактом: День IP захисту під час IP Week URL: https://nipo.gov.ua/ip-week-24-ip-zakhyst/

[2] Санкції проти агресора в дії: IP відомства країн ЄС більше не приймають заявки від росіян. URL: https://nipo.gov.ua/sanktsii-proty-ahresora/

[3] Хід Володимира Путіна завдати шкоди компаніям у ворожих країнах. URL: https://www.infobae.com/ua/2022/03/19/vladimir-putins-move-to-harm-companies-in-enemy-countries/

рення більш сприятливого середовища для розповсюдження контрафактної продукції та піратства, що, ймовірно, негативно впливатиме на правовласників протягом багатьох років, і навіть після завершення війни»[1].

У червні 2024 року Рада Європейського Союзу затвердила 14-й пакет економічних та індивідуальних обмежувальних заходів, спрямованих на протидію легалізації порушень прав інтелектуальної власності в Російській Федерації. Метою цих заходів є зниження конкурентних переваг російської промисловості та обмеження її доходів, які використовуються для ведення незаконної та неспровокованої агресивної війни проти України.

Ці санкції охоплюють ключові сектори російської економіки, зокрема енергетику, фінанси та торгівлю, а також спрямовані на ускладнення шляхів обходу існуючих обмежень. Новий пакет санкцій також запроваджує обмеження щодо прийому заявок на реєстрацію інтелектуальної власності в ЄС від російських громадян, резидентів РФ, юридичних осіб та установ. Це спрямовано на компенсацію дій російського уряду та судів, які незаконно позбавляють власників інтелектуальної власності ЄС їхніх прав у Росії.

Регламент Ради (ЄС) 2024/1745 від 24 червня 2024 року передбачає[2]:

- заборону для національних та регіональних IP-офісів ЄС приймати заявки від зазначених осіб, навіть якщо такі особи є лише частиною групи заявників, без необхідності формального винесення рішення про відмову;
- обмеження на прийом заяв чи клопотань у процесі реєстрації щодо всіх об'єктів інтелектуальної власності;
- надання IP-офісам права запитувати додаткову інформацію у заявників.

Крім того, країни-члени ЄС та сам Союз зобов'язалися вживати заходів для того, щоб Всесвітня організація інтелектуальної власності (ВОІВ) не приймала нових заявок від таких осіб.

---

[1] Там само.

[2] Council Regulation (EU) 2024/1745 of 24 June 2024 amending Regulation (EU) No 833/2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine. ST/8282/2024/REV1.OJ L, 2024/1745, 24.6.2024, ELI: http://data.europa.eu/eli/reg/2024/1745/oj

Своєю чергою, рішенням РНБО України від 20 листопада 2023 року «Про застосування секторальних спеціальних економічних та інших обмежувальних заходів (санкцій) до Російської Федерації та Республіки Білорусь в оборонно-промисловій сфері» від 22.11.2023 № 3489 IX), заборонено: «передачу резидентам і резидентами російської федерації та республіки білорусь технологій прав на об'єкти права інтелектуальної власності; здійснення резидентами російської федерації та республіки білорусь дій з одержання охоронних документів, здійснення інших дій, пов'язаних з охороною прав на об'єкти інтелектуальної власності (винахоДи, корисні моделі, промислові зразки, компонування напівпровідникових виробів, торговельні марки, географічні зазначення, сорти рослин, об'єкти авторського права і суміжних прав), крім дій щодо продовження строку чинності прав інтелектуальної власності та продовження строку дії охоронних документів; реєстрацію і акредитацію організацій колективного управління, засновниками яких є резиденти російської федерації та республіки білорусь»[1].

Україна послідовно протидіє російській пропаганді та спробам узаконити тимчасову окупацію частини своєї території на міжнародних майданчиках, зокрема у ВОІВ. З 2014 року залишається актуальною проблема некоректного зазначення адрес заявників із тимчасово окупованих територій України як російських у міжнародних системах реєстрації прав інтелектуальної власності (РСТ, Мадридська та Гаазька системи).

Нещодавно у цьому питанні було досягнуто значного прогресу завдяки рішенню Асамблеї ВОІВ на 65-й серії засідань держав-членів від 15 липня 2024 року[2]. Це рішення, зокрема, зобов'язує Міжнародне бюро ВОІВ вживати заходів для забезпечення відповідності публікацій на ресурсах і платформах організації принципам суверенітету, незалежності та територіальної цілісності України в межах її міжнародно визнаних кордонів.

---

[1] Про застосування секторальних спеціальних економічних та інших обмежувальних заходів (санкцій) до Російської Федерації та Республіки Білорусь в оборонно-промисловій сфері: рішення РНБО від 20 листопада 2023 р. URL: https://zakon.rada.gov.ua/laws/show/n0045525-23#Text

[2] Рішення Генасамблеї: ВОІВ продовжить підтримувати Україну у відновленні та відбудові IP екосистеми, інноваційного та креативного секторів. URL: https://nipo.gov.ua/wipo-ga-65-pidtrymka-ukrainy/

Ще одним важливим напрямом міжнародної боротьби стало блокування впровадження російської мови у міжнародні системи реєстрації прав інтелектуальної власності ВОІВ (зокрема Мадридську та Гаазьку системи), скорочення фінансування проєктів ВОІВ у рф та ініціювання закриття її зовнішнього офісу в москві[1].

«Введення воєнного стану 24 лютого 2022 року, надання Україні статусу кандидата у члени Європейського Союзу 23 червня 2022-го, визначення 8 листопада 2022 року Українського національного офісу інтелектуальної власності та інновацій (УКРНОІВІ) суб ‘ єктом, що виконує функції НОІВ, прийняття відповідних змін до законодавства України для його гармонізації із законодавством ЄС і подолання наслідків військової агресії стали важливими кроками у перший рік війни»[2]

13 квітня 2022 року набув чинності Закон України 2174-IX від 01.04.2022 року «Про захист інтересів осіб у сфері інтелектуальної власності під час дії воєнного стану, введеного у зв’язку із збройною агресією Російської Федерації проти України»[3]. Основна мета законодавчих змін полягає в тому, щоб захистити права інтелектуальної власності під час воєнного стану, коли діють обмеження прав і свобод громадян і запроваджені обмеження для юридичних осіб. Закон передбачає зупинення строків, пов’язаних з охороною прав інтелектуальної власності, та надає можливість продовжити дію охоронних документів протягом 90 днів після скасування воєнного стану без додаткових зборів. Права залишаються чинними, і їх можна поновити у звичайному порядку після війни. Закон визначає, що на період воєнного стану зупиняються строки, пов’язані з набуттям прав, поданням заперечень, оскарженням рішень та поновленням пропущених строків. «Призупинення перебігу встановлених законом строків розпочалося 24 лютого 2022 року і триватиме до скасування правового режиму воєнного стану. Зупинено строки, зокрема, на виконання

---

1 Санкції проти агресора в дії: ІР відомства країн ЄС більше не приймають заявки від росіян. URL: https://nipo.gov.ua/sanktsii-proty-ahresora/

2 Ярошевська Я. Розвиток судової ІР-практики в умовах війни URL: https://yur-gazeta.com/publications/practice/zahist-intelektualnoyi-vlasnosti-avtorske-pravo/rozvitok-sudovoyi-ippraktiki-v- umovah-viyni.html

3 Про захист інтересів осіб у сфері інтелектуальної власності під час дії воєнного стану, введеного у зв’язку із збройною агресією Російської Федерації проти України: Закон України від 01.04.2022 р. № 2174-IX: URL: https://zakon.rada.gov.ua/laws/show/2174-20#

таких дій: подання заперечення проти заявки або дії про міжнародну реєстрацію в Україні, поновлення прострочених строків, оскарження рішення ІР-офісу за заявкою в суді або до апеляційної палати, подання заяви про визнання недійсними прав на винахід, сплата мита. По суті призупинення строку розглядається як надання додаткових правових гарантій для бізнесу та створення необхідних умов для збереження наявних інвестицій»[1].

Попри те, що ухвалення цього Закону стало важливим кроком для захисту прав інтелектуальної власності під час війни, він має суттєві недоліки, які потребують виправлення. Зокрема, закон не передбачає механізмів відновлення прав після закінчення воєнних дій, не розв'язує питання пріоритетів, не визначає наслідки включення патентних документів до рівня техніки заявок, права на які були втрачені через війну, та не встановлює порядок вирішення конфліктів між відновленими та чинними правами, включаючи процедури розгляду заперечень Національним органом інтелектуальної власності, судові позови, заяви Антимонопольного комітету, а також дії митних і правоохоронних органів. Крім того, не врегульовано питання представництва інтересів клієнтів, чиї повірені не можуть виконувати свої обов'язки через воєнні обставини.[2]

Недостатній захист майнових прав інтелектуальної власності, що закінчуються під час воєнного стану, є ще однією проблемою. Хоча закон продовжує їх дію до наступного дня після скасування воєнного стану, цього часу недостатньо для належного продовження, що може призвести до втрати або несанкціонованого використання цих прав.[3]

---

[1] Барбашин С. Аспекти захисту інтелектуальної власності в Україні під час війни. URL: https://unba.org.ua/publications/9042-aspekti-zahistu-intelektual-noi-vlasnosti-v-ukraini-pid-chas-vijni.html

[2] Дмитришин В. С. Особливості набуття та захист прав інтелектуальної власності в умовах військової агресії. *Європейський вибір України, розвиток науки та національна безпека в реаліях масштабної військової агресії та глобальних викликів XXI століття*: у 2 т.: матеріали Міжнар. наук.-практ. конф. м. Одеса, 17 червня 2022 р. Одеса: Видавничий дім «Гельветика», 2022. Т 2. С. 741-745.

[3] Шикір Д. О. Аналіз Закону України «Про захист інтересів осіб у сфері інтелектуальної власності під час дії воєнного стану, введеного у зв'язку із збройною агресією Російської Федерації проти України» в контексті захисту прав інтелектуальної власності в умовах війни. *Створення, охорона, захист і комерціалізація об'єктів прав інтелектуальної власності:* матеріали V Всеукраїнської науково-практичної конференції з міжнародною участю, м. Київ, 26 квітня 2022 р. Київ: КПІ ім. Ігоря Сікорського, 2022. С. 219-223.

У зв'язку з уточненням позиції удосконалення механізму захисту прав інтелектуальної власності, 20.03.2023 року Верховною Радою було прийнято Закон «Про внесення змін до деяких законодавчих актів України щодо посилення захисту прав інтелектуальної власності»[1]. Згідно з цим Законом, до Цивільного кодексу України внесено зміни, що стосуються механізмів захисту прав інтелектуальної власності. Зокрема, додано положення, яке дозволяє замінити традиційні способи захисту разовим грошовим стягненням у випадках, коли порушення було ненавмисним і без ознак недбалості. Розмір такого стягнення визначає суд, беручи за основу суму винагороди, яка могла б бути сплачена за законне використання спірного об'єкта інтелектуальної власності, і яка є справедливою для позивача.

Крім того, відповідно до змін у Цивільному процесуальному кодексі, суд може за клопотанням позивача вимагати інформацію про походження та шляхи розповсюдження товарів чи послуг, що потенційно порушують права інтелектуальної власності. Таке клопотання має обґрунтовувати необхідність надання виключно тієї інформації, яка стосується походження, розповсюдження та осіб, причетних до виробництва, реалізації чи торгівлі відповідними товарами або послугами.

Саме під час війни було прийнято нову редакцію Закону «Про авторське право і суміжні права»[2]. Він був ухвалений Верховною Радою 1 грудня 2022 року і набрав чинності з 1 січня 2023 року.

Навесні 2023 року були розглянуті питання щодо обмеження використання патріотичної тематики при реєстрації торговельних марок та в рекламі. Відповідний проект Закону було зареєстровано у ВР за № 9128 [3]. «Ним пропонується заборонити використання в маркетингових цілях назв, пов'язаних із військовими діями, військовими подіями, населеними пунктами і місцями, які стали символами героїзму.

[1] Про внесення змін до деяких законодавчих актів України щодо посилення захисту прав інтелектуальної власності: Закон України від 20 березня 2023 р. URL: https://zakon.rada.gov.ua/laws/show/2974-20#Text

[2] Про авторське право і суміжні права: Закон України від 01.12.2022 № 2811-IX URL: https://zakon.rada. gov.ua/laws/show/2811 -20#Text

[3] Проект Закону про внесення змін до деяких законів України щодо обмеження використання патріотичної тематики при реєстрації торговельних марок та в рекламі: законопроект № 9128 від 30 березня 2023 р. URL: https://itd.rada.gov.ua/biUInfo/Bills/Card/41592

Крім того, назви військових частин, назви, які відтворюють офіційне вітання ЗСУ, виробників і видів озброєння»[1].

У зв'язку з повномасштабною війною, Україна прийняла закон, що забороняє пропаганду російського нацизму та символів вторгнення. Закон № 2265-IX, прийнятий 22 травня 2022 року[2], ввів в українське право визначення «держава-терорист» та заборонив використання символіки, що асоціюється з російською агресією. Це включає літери «Z» та «V», а також емблеми російських збройних сил. Заборона поширюється на використання цієї символіки в більшості публічних матеріалів, включаючи інтернет та соціальні мережі, а також на об'єкти авторського права, створені після початку повномасштабного вторгнення, за винятком матеріалів, що мають на меті протидію агресії.

Також, слід відзначити прийняття Верховною Радою України Закону України «Про внесення змін до деяких законів України щодо підтримки національного музичного продукту та обмеження публічного використання музичного продукту держави-агресора» від 19 червня 2022 року № 2310-IX[3]. Вищевказаний Закон набув чинності 7 жовтня 2022 року. В основному зміни стосуються сфери телебачення, радіомовлення та культури. Наприклад, в ЗУ «Про культуру» було внесено зміни щодо заборони на території України публічного виконання, публічного показу, публічної демонстрації, публічного сповіщення фонограм, відеограм та музичних кліпів, які: «містять зафіксоване виконання музичного недраматичного твору з текстом, здійснене співаком (співачкою), який є або був у будь-який період після 1991 року громадянином держави, визнаної Верховною Радою України державою-агресором, за винятком колишніх громадян дер-

---

[1] Барбашин С. Аспекти захисту інтелектуальної власності в Україні під час війни. URL: https://unba.org.ua/publications/9042-aspekti-zahistu-intelektual-noi-vlasnosti-v-ukraini-pid-chas-vijni.html

[2] Про заборону пропаганди російського нацистського тоталітарного режиму, збройної агресії Російської Федерації як держави-терориста проти України, символіки воєнного вторгнення російського нацистського тоталітарного режиму в Україну: Закон України від 22.05.2022 № 2265-IX. URL: https://zakon.rada.gov.Ua/laws/show/2265-20#Text Барбашин С. Аспекти захисту інтелектуальної власності в Україні під час війни. URL: https://unba.org.ua/publications/9042-aspekti-zahistu-intelektual-noi-vlasnosti-v- ukraini-pid-chas-vijni.html

[3] Про внесення змін до деяких законів України щодо підтримки національного музичного продукту та обмеження публічного використання музичного продукту держави-агресора: Закон України від 19 червня 2022 року № 2310-IX. URL: https://zakon.rada.gov.ua/laws/show/2310-20#Text

жави-агресора, які є або на момент смерті були громадянами України і не мають (не мали на момент смерті) громадянства держави-агресора, та/або вироблені фізичною особою та/або юридичною особою, яка на момент їх оприлюднення була, відповідно, громадянином або зареєстрована в державі, яку в будь-який час визнано державою-агресором»[1]

Сьогодні національні та міжнародні заявки проходять процес реєстрації без суттєвих змін під час воєнного стану. Однак ІР-офіс України не проводить заходи щодо компаній, пов'язаних із країнами-агресорами.

З огляду на існуючу ситуацію, дослідження взаємозв'язку між порушеннями прав інтелектуальної власності в мережі Інтернет та стратегією гібридної війни має критичне значення для формування ефективної системи протидії, мінімізації загрози національній безпеці та збереження інтелектуального потенціалу України в умовах триваючого гібридного протистояння.

Правопорушення визначається як суспільно небезпечне діяння, що порушує норми права. У цивільному праві це діяння завдає шкоди майновим та особистим немайновим правам. Склад цивільного правопорушення утворюється тріадою: протиправна поведінка, шкода, причинний зв'язок, та вина. Разом з тим, у правовій доктрині існує позиція, що не слід дотримуватись традиційних постулатів, і не вважати склад правопорушення єдиною підставою відповідальності. Пропонується зосередити увагу на факті порушення суб'єктивного цивільного права як підставі відповідальності.

Порушення особистих немайнових прав інтелектуальної власності відбувається, коли дії особи суперечать закону, завдаючи шкоди особистим благам творця. Проте, якщо посягання вдалося запобігти, шкода може бути відсутня.

У юридичній науці немає чіткого визначення правопорушення у сфері інтелектуальної власності. Існуючі поняття не завжди ефективні. Р. Б. Шишка пропонує порушенням права інтелектуальної власності вважати «таке діяння, яке передбачене як таке нормою права, але призводить до негативних для потерпілої особи наслідків і можливості застосування способів і форм захисту суб'єктивного права чи охоронюваного інтересу. Деякі вчені вважають, що підставою від-

[1] Там само.

повідальності має бути сам факт порушення права, а не лише склад правопорушення»[1].

За визначенням О. А. Підопригори, і за визначенням законодавця (ст. 431 ЦК України) правопорушення визначається як будь-яке посягання на особисті немайнові та майнові права автора, що завдає шкоди його честі та репутації автора.

Закон України «Про охорону прав на винаходи і корисні моделі»[2] (ч. 1 ст. 34) визначає порушенням прав володільця патенту будь-яке посягання на права, що випливають з державної реєстрації патенту. Закон України «Про охорону прав на промислові зразки»[3] (ч. 1 ст. 26) визначає порушенням «прав власника зареєстрованого або незареєстрованого промислового зразка будь- яке посягання на права власника зареєстрованого промислового зразка, передбачені частиною другою статті 20 цього Закону, або будь-яке посягання на права власника незареєстрованого промислового зразка, передбачені частиною дев'ятою статті 20 цього Закону». Подібне визначення міститься у Законі України «Про охорону прав на знаки для товарів і послуг» (ст. 20), у Законі України «Про охорону прав на компонування напівпровідникових виробів». У Законі України «Про правову охорону географічних зазначень», зазначено що «порушення прав, що випливають з реєстрації географічного зазначення є, будь-яке посягання на права, що випливають з реєстрації географічного зазначення»[4]. В Законі України «Про охорону прав на сорти рослин» порушенням особистих немайнових прав інтелектуальної власності на сорт рослин є привласнення авторства (ст. 53).

Найбільш повний перелік порушень особистих немайнових та/або майнових авторських і суміжних прав розкривається у Законі України «Про авторське право і суміжні права»[5]. Дії, які в Україні вважаються порушеннями авторського права визначає ст. 53 Закону.

---

[1] Шишка Р. Б. Охорона права інтелектуальної власності у цивільному праві України: дис.... д-ра юрид. наук. Харків, 2002. 386 с.

[2] Про охорону прав на винаходи і корисні моделі: Закон України від 15.12.1993 № 3687-XII. URL: https://zakon.rada.gov.Ua/laws/show/3687-12#Text

[3] Про охорону прав на промислові зразки: Закон України від 15.12. 1993 № 3688-XII. URL: https://zakon.rada.gov.ua/laws/show/3688-12#Text

[4] Про правову охорону географічних зазначень: Закон України від 16.06.1999 № 752-XIV. URL: https://zakon.rada.gov.ua/laws/show/752-14#Text

[5] Про авторське право і суміжні права: Закон України від 01.12.2022 № 2811-IX URL: https://zakon.rada. gov.ua/laws/show/2811 -20#Text

Відповідно до Договору ВОІВ про авторське право порушеннями є: «будь-які дії для свідомого обходу технічних засобів захисту авторського права, зокрема виготовлення, розповсюдження, ввезення з метою розповсюдження і застосування засобів для такого обходу; підробка, зміна чи вилучення інформації, зокрема в електронній формі, про управління правами без дозволу суб'єктів авторського права чи особи, яка здійснює таке управління; розповсюдження, ввезення на митну територію України з метою розповсюдження, публічне сповіщення про об'єкти авторського права, з яких без дозволу суб'єктів авторського права вилучили чи змінили інформацію про управління правами, зокрема в електронній формі»[1]

Незважаючи на війну, Україна активно працює над захистом авторських прав в Інтернеті як для українських, так і для іноземних правовласників.

Мережа Інтернет є відкритою інформаційною системою, що представлена сукупністю мереж, служб і каналів для обробки і передачі інформації, локальних комп'ютерних мереж, мереж мобільної телефонії. Слід погодитись з С. П. Позняковим і Т. В. Маньгорою, що «Інтернет в цілому не є суб'єктом права, оскільки він не представляє собою міжнародну організацію, юридичну особу чи будь-яку іншу організовану структуру. Інтернет також не є об'єктом права, оскільки в ньому немає єдиного конкретного власника, а також відсутній суб'єкт, що контролює значну частину цієї мережі. Крім того, Інтернет не може бути розглянутий як засіб масової інформації, оскільки власник інформаційного ресурсу не здійснює активних дій з доставки інформації споживачеві»[2]

Визначення поняття «мережа Інтернет» міститься у Законі України «Про електронні комунікації», згідно зі ст. 1 якого вона є «глобальною електронно комунікаційною мережею, що призначена для передачі даних та складається з фізично та логічно взаємоз'єднаних окремих електронних комунікаційних мереж, взаємодія яких базується на використанні єдиного адресного простору та на використанні інтернет-протоколів, визначених міжнародними стан-

[1] Договір Всесвітньої організації інтелектуальної власності про авторське право, прийнятий Дипломатичною конференцією 20 грудня 1996 року URL: https://zakon.rada.gov.ua/laws/show/995_770#Text

[2] Позняков С. П., Маньгора Т. В. До проблеми захисту права інтелектуальної власності в мережі інтернет. *Наукові інновації та передові технології.* 2024. № 3. С.660-670.

дартами»[1]. Іншими словами Інтернет можна розглядати як засіб комунікації між людьми.

Правопорушення у сфері інтелектуальної власності в мережі Інтернет охоплюють такі дії, як порушення авторських прав (незаконне копіювання, поширення або використання захищених матеріалів – текстів, фотографій, відео, музики тощо – без згоди автора чи правовласника), незаконне завантаження, використання або розповсюдження програмного забезпечення, захищеного авторським правом, без відповідного дозволу, а також плагіат і крадіжку контенту (використання інтелектуальних продуктів, таких як статті, блоги, відео тощо, без належного посилання або дозволу автора). До цих порушень також належать неправомірне використання торговельних марок, зокрема в доменних іменах чи інших контекстах, що може вводити в оману споживачів, а також розробка шкідливого програмного забезпечення або технічних засобів для обходу систем захисту авторських прав чи інших механізмів охорони інтелектуальної власності.[2]

Основною перешкодою для ефективного правового захисту та притягнення винних до відповідальності є складність встановлення факту правопорушення. Відтак, ключовими завданнями у процесі фіксації порушення авторського права є: ідентифікація власника вебресурсу, на якому відбулося порушення; встановлення особи, яка вчинила правопорушення; визначення процедури фіксації такого порушення. У більшості випадків ідентифікувати власника вебресурсу або безпосереднього правопорушника в Інтернеті майже неможливо. Це зумовлено тим, що під час реєстрації власник вебресурсу може вказати недостовірні або вигадані дані, оскільки законодавство не регулює їх перевірку. Крім того, особа, яка вчинила правопорушення, могла використовувати IP-адресу, що їй не належить. Сучасні програми та застосунки дозволяють легко змінювати IP-адресу, проте законодавство не містить відповідних норм щодо їх використання, а також не передбачає відповідальності за їх застосування[3]

Прийняття нового Закону України «Про авторське право і суміжні права», який регламентує порядок припинення порушень

[1] Про електронні комунікації: Закон України від 16.12.2020 № 1089-IXURL: https://zakon.rada.gov. Ua/laws/show/1089-20#Text

[2] Там само.

[3] Солончук І. В. Мельник В. В. Проблема захисту авторського права в Інтернеті. Пра*вова позиція.* 2022. № 3. С. 41-45.

авторських і суміжних прав у мережі Інтернет (ст. 56), а також запровадження адміністративної відповідальності за недотримання встановлених правил щодо такого припинення (ст. 164-17 Кодексу України про адміністративні правопорушення) є важливим кроком у боротьбі з порушеннями авторських прав в онлайн-просторі. Попри наявність певних недоліків, цей механізм правового захисту, з урахуванням міжнародного досвіду, має потенціал для подальшого вдосконалення. У зв'язку з цим наукові дослідження, присвячені захисту авторських прав в Інтернеті, залишаються актуальними.

Слід зазначити, що до найбільш поширених порушень авторських прав в мережі інтернет сьогодні відносять інтернет-піратство; поширення контенту, захищеного авторським правом користувачами з використанням файлообмінних мереж (зокрема, мереж типу peer-to-peer); завантаження та поширення авторських матеріалів у соцмережах; незаконне використання об'єктів авторського права через стрімінгові сервіси[1].

З розвитком високошвидкісного інтернету, стрімінгових сервісів та цифрового контенту незаконне розповсюдження фільмів, музики, програмного забезпечення та книг стало масовим явищем у всьому світі. Проблема інтернет-піратства є актуальною наразі як на глобальному рівні, так і в Україні. Попри жорсткі заходи з боку урядів і технологічних компаній, піратські сайти знаходять нові способи обходу блокувань, а користувачі продовжують шукати безкоштовні альтернативи офіційному контенту. Зокрема, зростання популярності VPN та анонімних мереж ускладнює боротьбу з піратством.

В Україні проблема інтернет-піратства стоїть особливо гостро. На «високий рівень піратства і контрафакції, недостатність узгоджених заходів і ефективної інфраструктури з попередження та боротьби з даними явищами» вказано в Стратегічному плані розвитку Державної організації «Український національний офіс інтелектуальної власності та інновацій» на 2024-2028 рр[2]. За оцінками міжнародних організацій, країна довгий час входила до списку *держав із високим*

[1] https://activelex.com/wp-content/uploads/2024/02/presentation vebinar final updated.pdf

[2] Стратегічному плані розвитку на 2024-2028 рр. URL: https://nipo.gov.ua/wp-content/uploads/2024/04/Stratehichnyyi_plan_rozvytku_UKRNOIVI_2024-2028-web.pdf

рівнем порушень авторських прав[1]*. «Серед 50 найбільш відвідуваних в Україні ресурсів на початок грудня 2024 року було аж вісім піратських і жоДного легального»*[2].

Єдиним міжнародним документом, що містить визначення терміна «піратство», є Угода про торговельні аспекти прав інтелектуальної власності (TRIPS) Всесвітньої торговельної організації (WTO). Згідно з Приміткою 14 до Статті 51 цієї Угоди, під «товарами, що порушують авторські права» розуміються будь-які копії, виготовлені без дозволу правовласника або уповноваженої ним особи в країні виробництва. Такі товари створені на основі оригінального виробу і є порушенням авторських чи суміжних прав у країні, куди вони імпортуються

В законодавстві України визначення Інтернет-піратства наведене в Законі України «Про авторське право і суміжні права» (документ 2811-IX, редакція від 15.04.2023, підстава – 2974-IX), згідно з яким в ст. 53 «Підстави для захисту авторського права і суміжних прав» зазначено, що Інтернет- піратство – це незаконне використання об'єктів авторського права та/або об'єктів суміжних прав із застосуванням мережі Інтернет.

Сербін Д. справедливо наголошує на серйозних негативних наслідках інтернет-піратства, і з цим важко не погодитися[3]. Передусім, піратство фактично є крадіжкою, оскільки воно позбавляє авторів та розробників заслуженої винагороди за їхню працю. Творці контенту інвестують час, кошти та зусилля у створення продуктів, а пірати без дозволу розповсюджують їх, порушуючи права інтелектуальної власності.

Крім того, піратські файли часто містять віруси та шкідливий код, що становить серйозну загрозу для кібербезпеки. Такі продукти можуть не лише пошкодити пристрої користувачів, а й

---

[1] Щеглюк С. Д. Особливості тінізації сфери креативних послуг в Україні: напрями її подолання Аналітична записка URL: https://ird.gov.ua/irdp/e20210301.pdf; 2021 Special 301 Report. Office of the United States Trade Representative. URL: https://ustr.gov/sites/default/files/files/reports/2021/2021%20Special%20301% 20Report%20(final).pdf ; Thomas Buckley T. Streaming Pirates Are Hollywood's New Villains. URL: https://www.bloomberg.com/news/articles/2024-01-24/streaming-service-costs-drive-new-era-of-hollywood- piracy

[2] На рівні «цифрового Сомалі»: статистика інтернет-піратства в Україні. URL: https://svoboda.te.ua/na-rivni- czyfrovogo-somali-statystyka-internet-piratstva-v-ukrayini/

[3] Сербін Д. Штрафи за піратство в Україні: зміни у 2023 році. URL: https://yur- gazeta.com/publications/practice/zahist-intelektualnoyi-vlasnosti-avtorske-pravo/shtrafi-za-piratstvo-v-ukrayini- zmini-u-2023-roci.html

використовувати їх у шахрайських схемах. До того ж, піратські ресурси нерідко монетизуються за рахунок прихованої реклами або співпраці зі зловмисниками, що лише підсилює ризики для користувачів.

Ще одним небезпечним аспектом є збір особистих даних без відома користувача. Завантажуючи нелегальний контент, люди часто не усвідомлюють, що він може містити модифікації, які відстежують їхню активність або навіть отримують доступ до конфіденційної інформації.

Нарешті, піратство завдає удару по креативних індустріях та компаніях, що займаються створенням контенту. Якщо прибутки виробників падають через нелегальне розповсюдження їхньої продукції, це може призвести до скорочення інвестицій у нові проєкти та втрати робочих місць.

Таким чином, піратство – це не просто безкоштовний доступ до контенту, а комплексна проблема, яка шкодить і авторам, і користувачам, і економіці загалом.

Слід зазначити, що Україна стала однією з перших країн, яка використовує захищену онлайн-платформу для виявлення сайтів та додатків, що порушують авторські права. Це також важливий крок на шляху до євроінтеграції[1]. Україна приєдналася до міжнародної платформи WIPO ALERT, де країни обмінюються інформацією про сайти, що порушують права інтелектуальної власності. Міністерство економіки України (Мінекономіки) затвердило порядок формування національного переліку таких сайтів (наказ від 03 лютого 2024 р. № 2945). Платформа WIPO ALERT, яку адмініструє Всесвітня організація інтелектуальної власності (ВОІВ), дозволяє країнам- учасницям обмінюватися даними про сайти та мобільні додатки, що підозрюються в порушенні прав інтелектуальної власності. Завдяки співпраці Мінекономіки з ВОІВ, правовласники можуть подавати заявки до IP офісу для включення сайтів-порушників до національного переліку[2]. Наразі Міністерство економіки України з 10 березня 2025 року запустило оновлену процедуру розміщення національного переліку

[1] Дзіс С. Реєстр вебсайтів, що порушують авторське право: зрада чи перемога? URL: https://sdm- partaers.com/novyny/statti/register-of-infringing-websites/

[2] Україна розширила інструменти захисту авторських прав в інтернет-просторі URL: https://me.gov.ua/News/Detail?lang=uk-UA&id=9a03f906-731f-4288-a0a6- 4b45fb-c1e192&title=UkrainaRozshirilaInstrumentiZakhistuAvtorskikhPravVInternetprostori

вебсайтів, які порушують права інтелектуальної влісності на платформі WIPO ALERT[1].

Варто відмітити також, що відповідно до змін, внесених до Закону України «Про рекламу» наразі вважається адміністративним правопорушенням розміщення рекламних оголошень та інтеграцій на сайтах, внесених в реєстр WIPO ALERT. Окрім того, інформація з реєстру надається операторам платіжних систем (Visa, MasterCard, PayPal), щоб вони уникали співпраці з власниками цих майданчиків.

Наразі у багатьох розвинених країнах діють суворі покарання не лише за розповсюдження, а й за споживання піратського контенту. Так, у Японії незаконне завантаження фільмів або музики може призвести до двох років ув'язнення. В Італії користувачі нелегального контенту ризикують отримати штраф до 5000 євро. У Німеччині ж навіть спроба завантажити піратську продукцію вважається рівнозначною її розповсюдженню: перше порушення коштуватиме 155 євро, а повторне – вже близько 1000 євро.

Треба відмітити, що навесні 2023 року користувачі супутникових терміналів Starlink в Україні почали отримувати попередження за завантаження й поширення неліцензійних фільмів і серіалів. При цьому попереджувальна інформація сповіщала, що повторне порушення авторського права може призвести до повного блокування доступу термінала до мережі[2].

Таким чином, можна стверджувати про розширення кола суб'єктів правопорушень щодо інтернет-піратства за рахунок користувачів контенту, що при закріпленні на рівні законодавчої норми може виявитися дієвим засобом боротьби з порушенням авторських прав в мережі Інтернет.

Разом з тим, наразі незважаючи на посилення законодавчих ініціатив та блокування піратських ресурсів, доступ до нелегального контенту залишається простим і привабливим для багатьох користувачів, а інтернет-піратство – одним із ключових видів порушень авторських прав у цифрову еру. Це не лише завдає збитків правовлас-

[1] Центр спостереження з питань порушень прав інтелектуальної власності: для чого створено і як працюватиме новий майданчик IP офісу. URL: https://nipo.gov.ua/ukr-tsentr-sposterezhennia-porushen-ip-prav/

[2] На рівні «цифрового Сомалі»: статистика інтернет-піратства в Україні. URL: https://svoboda.te.ua/na-rivni- czyfrovogo-somali-statystyka-internet-piratstva-v-ukrayini/

никам, а й гальмує розвиток креативних індустрій та створює загрози для кібербезпеки користувачів.

Гібридна війна, яку веде росія проти України, поєднує військові, політичні, економічні та інформаційні методи впливу. У такій війні інформаційна складова має особливе значення, адже маніпулювання даними, дезінформація та викривлення реальності є ефективними інструментами ведення бойових дій у цифровому просторі. Водночас соціальні мережі стають головним майданчиком для поширення інформації, що призводить до масових порушень прав інтелектуальної власності.

Під час гібридних конфліктів відбувається масове використання чужого контенту без дозволу для поширення дезінформації та пропаганди. Зловмисники перекручують оригінальний зміст, видають його за власний або приписують авторство іншим джерелам. Поширеним є розповсюдження інформаційних продуктів (інфографік, документальних матеріалів, звітів) без посилання на першоджерело.

Соціальні мережі дозволяють миттєво поширювати контент, що ускладнює контроль за дотриманням авторських прав у ситуації інформаційного протистояння.

Використання вкраденого контенту може бути частиною спланованих операцій з метою підриву довіри до авторитетних джерел інформації або створення хибних наративів. Соціальні мережі широко використовуються для створення і поширення фейкових новин, що базуються на викрадених або видозмінених матеріалах. Російські пропагандистські ресурси систематично змінюють першоджерело інформації, видаючи український контент за власний або навпаки, приписуючи Україні дії, яких вона не вчиняла.

В умовах війни спостерігається масштабне використання українських торговельних марок та логотипів без згоди правовласників. Це може включати: творення підроблених акаунтів, що видають себе за офіційні сторінки українських державних структур або компаній; використання символіки українських брендів у пропагандистських матеріалах або в комерційних цілях без дозволу.

Збільшилася кількість випадків незаконного поширення українських книг, музики, фільмів та іншого контенту, особливо на тлі міжнародного інтересу до України. Пропагандистські ресурси можуть

поширювати такі матеріали без дозволу правовласників, зокрема з метою маніпулювання суспільною думкою.

У хаотичному інформаційному просторі воєнного часу важко своєчасно виявляти та реагувати на всі випадки копіювання контенту без дозволу. Часто автори контенту втрачають контроль над своїми творами, що призводить до фінансових збитків та ускладнює протидію дезінформації. Транскордонний характер соціальних мереж та різні юрисдикції ускладнюють захист авторських прав, особливо коли порушення відбуваються як частина гібридних операцій.

У контексті гібридної війни різноманітні заходи захисту прав інтелектуальної власності стикаються з низкою проблем: відсутність ефективного механізму блокування контенту, розміщеного на закордонних платформах (наприклад, російських або анонімних сайтах); обмежена можливість юридичного переслідування осіб, які знаходяться поза юрисдикцією України; недостатня співпраця соціальних мереж із державними органами щодо швидкого реагування на порушення.

Фактично «соціальні мережі змінили порядок взаємодії користувачів з об'єктами права інтелектуальної власності. Тому питання існування різних форм об'єктів інтелектуальної власності в мережі та різних форм суб'єктів, будь-то творець цього об'єкту чи користувач, а також особливості їх взаємодії в теперішніх умовах, є вкрай актуальними»[1]. Серед об'єктів права інтелектуальної власності частіше всього в соціальних мережах порушуються «права на літературні письмові твори публіцистичного, технічного, белетристичного, наукового або іншого характеру, фотографічні твори, музичні твори без тексту та з текстом і твори, що виконані способом, подібним до фотографії»[2]

Діяльність у соціальних мережах не може бути врегульована нормами лише однієї сфери права, це можуть бути норми, що регулюють суспільні відносини в таких сферах, як реклама, торгівля, захист даних, інтелектуальна власність тощо. Деякі аспекти діяльності соці-

[1] Канарик Ю. С. Захист прав інтелектуальної власності в соціальних мережах: окремі аспекти. *Юридичний науковий електронний журнал.* 2021. № 9. С. 68-71.

[2] Марущак Я. С. Порушення прав інтелектуальної власності у соціальних мережах Інтернету. *Актуальні проблеми захисту права власності*: матер. кругл. столу (м. Одеса,17 червня 2016 р.).Одеса, 2016. С. 87-88.

альних мереж регулюються не тільки правовими нормами, а й підпадають під вплив різноманітних моральних та етичних стандартів[1]

Всесвітньо відомі соціальні мережі сьогодні активно працюють над розробленням політик і дієвих механізмів захисту прав на об'єкти інтелектуальної власності. При цьому слід зазначити, що сучасна система захисту авторських прав значною мірою ґрунтується на Законі США про авторське право в цифрову епоху (*Digital Millennium Copyright Act*, DMCA). Одним із ключових принципів цього закону є концепція так званої «безпечної гавані» (*safe harbors*) для постачальників онлайн-послуг. Вона передбачає певні умови та дії, за яких провайдери звільняються від відповідальності за розміщений користувачами контент.

DMCA дозволяє правовласникам подавати онлайн-сервісам запити на видалення незаконно розміщених матеріалів (*DMCA takedown requests*). Якщо постачальник онлайн-послуг оперативно реагує на такі запити та видаляє контент, що порушує авторські права, він не несе відповідальності за його розміщення.

Так, Instagram активно протидіє порушенням авторських прав, застосовуючи автоматизовані системи для видалення нелегального контенту та блокування акаунтів. Щоб уникнути порушень, користувачам необхідно отримувати дозвіл на використання чужих матеріалів або правильно вказувати авторство. Це особливо актуально для музичного контенту, адже дозволяється використовувати лише треки з відкритим доступом або ті, на які є відповідна ліцензія. В іншому випадку відео може бути видалено, навіть якщо воно створене самим користувачем.

Facebook також серйозно ставиться до захисту авторських прав, пропонуючи інструменти для контролю за контентом. Правовласник або його представник може подати скаргу через спеціальну онлайн-форму, проте платформа рекомендує спочатку спробувати вирішити питання безпосередньо з порушником. У заяві необхідно вказати інформацію про правовласника, опис захищеного контенту та посилання на матеріал, що порушує авторські права. Facebook може видалити спірний контент, однак користувач має право оскаржити

[1] Ваксман Р. В. Окремі питання правового регулювання реклами в соціальних мережах. *Юридичний науковий електронний журнал.* 2024. № 11. С. 164-166. URL: http://www.lsej.org.ua/11_2024/38.pdf

це рішення. Виняток становлять матеріали, що використовуються в некомерційних цілях для критики, коментарів, новин, навчання або наукових досліджень.

Аналогічні правила діють і на YouTube. Система Content ID автоматично виявляє збіги з захищеним контентом та дозволяє правовласникам керувати його використанням. Якщо користувач вважаєте, що його права порушено, він може подати скаргу через спеціальну форму. Важливо пам'ятати, що YouTube може заблокувати обліковий запис за зловживання інструментами захисту, тому скаргу слід подавати лише при наявності вагомих підстав.

TikTok, популярна серед молоді платформа, активно розвиває систему ліцензування та дозвільних програм, що сприяє зростанню її аудиторії. Користувачі можуть створювати власний контент, використовуючи інтелектуальну власність компанії Bytedance, якій належать права на програмне забезпечення, графіку, аудіо та відео. Створені відео можна поширювати в інші соціальні мережі, такі як Facebook, Instagram, Twitter, YouTube, або через пряме посилання чи вбудовування. Однак деякі користувачі обмежують доступ до свого контенту, забороняючи збереження відео, використання звуків або створення дуетів. Незважаючи на водяний знак з ім'ям автора, поширення обмеженого контенту без дозволу є порушенням авторських прав. Згідно з умовами використання TikTok, контент, що порушує авторські права, може бути видалений, а обліковий запис – заблокований. У разі порушення авторських прав TikTok рекомендує зв'язатися з автором або подати скаргу[1]

Таким чином, порушення прав інтелектуальної власності в соціальних мережах набули особливої гостроти в умовах гібридної війни, коли інформація використовується як зброя. Масштабне незаконне використання контенту, маніпуляція авторством, піратство та порушення суміжних прав вимагають комплексного підходу до захисту цифрової власності. Вирішення цих проблем потребує оновлення законодавства, активної міжнародної співпраці та впровадження сучасних технологій для боротьби з інформаційними загрозами/ Особливу увагу варто приділити судовій практиці щодо порушення авторських прав в Інтернеті. Важливим аспектом таких справ є використання су-

[1] Моргун А. Захист авторських прав в соціальних мережах. URL: https://surl.li/dkqvfi

дами термінології, яка не закріплена в національному законодавстві України, але при цьому враховується під час розгляду справ.

Наприклад, у справі № 759/8347/23 Київський апеляційний суд роз'яснив[1], що Telegram-канал не можна прирівнювати до вебсайту чи вебсторінки, оскільки він за своєю природою не відповідає цим поняттям. Суд зазначив, що Telegram є месенджером, призначеним для обміну повідомленнями, з функцією наскрізного шифрування, відеодзвінків та передачі файлів. Таким чином, Telegram не може вважатися класичним вебресурсом, хоча і залишається платформою, де можливі порушення авторських прав.

Важливим висновком цього рішення є те, що якщо порушення авторських прав відбувається в месенджері (наприклад, у Telegram), відповідач не звільняється від відповідальності навіть за умови досудового врегулювання спору відповідно до ст. 56 Закону про авторське право. Це підтверджує, що правовласники мають шанс притягнути правопорушників до відповідальності та домогтися компенсації, навіть якщо порушення відбувається не на традиційних вебресурсах, а в цифрових комунікаційних середовищах.

В умовах воєнного стану недобросовісна конкуренція у сфері інтелектуальної власності становить серйозну загрозу для інновацій та економіки країни. Конкуренти можуть використовувати складну ситуацію для незаконного використання об'єктів права інтелектуальної власності інших компаній, що призведе до порушення прав та втрати доходів. Особливо небезпечним є використання воєнного стану для отримання конфіденційної інформації про інтелектуальну власність конкурентів. Це може призвести до крадіжки технологій та ідей, що завдасть значної шкоди інноваційним компаніям. Компанії повинні забезпечити надійний захист своїх інтелектуальних активів від кібератак та фізичного втручання. Також важливо посилити правовий захист інтелектуальної власності та контроль за її порушеннями[2].

У воєнний час недобросовісна конкуренція у сфері інтелектуальної власності може набувати таких форм: крадіжка інтелектуальної

---

[1] Постанова Київського апеляційного суду у справі № 759/8347/23 від 07 листопада 2023 р. URL: https://verdictum.ligazakon.net/document/115075175?q=

[2] Створення, охорона, захист і комерціалізація об'єктів права інтелектуальної власності: матеріали *VI Всеукраїнської науково-практичної конференції з міжнародною участю, присвяченої Міжнародному дню інтелектуальної власності.* (м. Київ, 26 квітня 2023 р.): ел. збірник. Київ: КПІ ім. Ігоря Сікорського, 2023. 321

власності; шпигунство та диверсії; підробка товарів; незаконне копіювання та розповсюдження; дезінформація; силове заволодіння технологіями. Судова практика показує, що найчастіше зустрічаються такі порушення[1]: неправомірне використання назв та поширення оманливої інформації; дискредитація конкурентів та заклики до їх бойкоту.

Нормативна база, що регулює питання недобросовісної конкуренції є досить розлогою та включає в себе, зокрема, такі нормативно-правові акти, як «Конституція України, Господарський кодекс України, Закон України «Про захист від недобросовісної конкуренції», Закон України «Про Антимонопольний комітет України», а також Паризьку конвенцію про охорону промислової власності, учасником якої, в тому числі, є Україна. Під захистом від недобросовісної конкуренції вважається врегульована законом діяльність держави, її компетентних органів і посадових осіб, які наділені відповідними повноваженнями»[2]. В реальному сучасному світі поняття недобросовісної конкуренції стало частиною боротьби за ринок. По суті, недобросовісна конкуренція – це все, що виходить за рамки здорового суперництва. Тобто будь-які конкурентні дії, що суперечать торговим та іншим чесним звичаям. Положення статті 4 Закону України «Про захист від недобросовісної конкуренції» передбачають можливість «здійснювати захист широкого кола об'єктів інтелектуальної власності від неправомірного використання (тобто без дозволу правовласника), зокрема таких, як: комерційне найменування, рекламні матеріали, торговельні марки та інші позначення, у тому разі, якщо таке неправомірне використання призвело чи може призвести до змішування з діяльністю правовласника (який раніше почав використовувати свої позначення)»[3].

У більшості випадків недобросовісна поведінка порушує як конкурентне законодавство, так і законодавство про інтелектуальну власність.

---

[1] Цуркан О. Спроба врегулювати питання права інтелектуальної власності на час війни призвела до проблем на фармринку. URL: https://www.legalalliance.com.ua/publikacii/sproba-vreguluvati-pitanna-prava-intelektualnoi-vlasnosti-na-cas-vijni-prizvela-do-problem-na-farmrinku/

[2] Швидка Т. І. Удосконалення законодавчого регулювання неправомірного використання ділової репутації суб'єкта господарювання. *Актуальні проблеми вітчизняної юриспруденції.* 2021. № 1. С. 60-64.

[3] Про захист від недобросовісної конкуренції: Закон України від 07.06.1996 № 236/96-ВР URL: https://zakon.rada.gov.ua/laws/card/236/96-%D0%B2%D1%80

Сьогодні, з огляду на розвиток суспільних відносин і технологій, випадків недобросовісної конкуренції значно більше, ніж передбачено чинним законодавством.

Коли порушення стосуються використання чужої ділової репутації, найбільше потерпають сумлінні виробники. Вони втрачають частину потенційних споживачів, яких переманюють недобросовісні конкуренти. Останні, не вкладаючи значних ресурсів, отримують перевагу за рахунок привласнення чужих досягнень і використання репутації інших компаній.

Переважна більшість порушень прав на торговельну марку пов'язані з протиправним використанням торговельної марки іншими особами не власниками цієї торговельної марки. До видів використання торговельної марки, науковці відносять: «нанесення торговельної марки на: будь-які товари, для яких торговельну марку було зареєстровано; упаковки, в яких ці товари зберігаються; вивіски, пов'язані з товаром; етикетки, нашивки, бирки тощо; зберігання таких товарів із зазначеним нанесенням торговельної марки з метою пропозиції до продажу; пропозиція товару до продажу з нанесеною торговельною маркою; продаж, експорт, імпорт товарів з нанесеною торговельною маркою; застосування торговельної марки під час пропозиції та надання послуг, для яких торговельну марку зареєстровано; застосування торговельної марки в діловій документації, у рекламі, у мережі Інтернет, у тому числі в доменних іменах»[1]. Торговельна марка вважається використаною, навіть якщо вона представлена у дещо зміненому вигляді, але при цьому зберігає свою основну унікальність. Іншими словами, використання окремих елементів зареєстрованої торгової марки також вважається її використанням.

Шимон С. І. звертає увагу на те, що наразі поширеним є застосування, зокрема, позначень торговельних марок у нетрадиційних формах у відповідних засобах мережі Інтернет: для оптимізації результатів пошуку у змісті сайту (HTML-коді) сторінки; у складі доменного імені; у якості гіперпосилання; у якості метатег; для створення та появи рекламних посилань різними засобами – за певних умов також може становити порушення прав на торговельну марку[2].

[1] Ткачук Г. В. Напрями вдосконалення законодавства України про реалізацію і захист прав на торговельні марки. *Форум права.* 2018. № 4. С. 95-101.

[2] . Шимон С. І. Актуальне дослідження правової охорони торговельних марок в Інтернет. *Часопис Київського університету права.* 2017. № 4. С. 319-320.

Іноді порушення прав власника торгової марки складно виявити. Тому суд може застосувати тимчасові заходи для збереження доказів порушення, наприклад: огляд приміщень, де можуть зберігатися товари з незаконним маркуванням; арешт та вилучення таких товарів; арешт рахунків та документів, що підтверджують порушення. У соціальних мережах порушенням вважається створення рекламних акаунтів з використанням торгової марки без відповідного дозволу або всупереч умовам ліцензійної угоди. Отже, незаконним використанням торговельних марок в Інтернеті є: використання торговельної марки способами, не передбаченими договором; продаж товарів низької якості під чужою торговою маркою[1].

Власник веб-сайту та власник веб-сторінки, де незаконно використовується торговельна марка, не завжди є однією і тією ж особою. Це впливає на визначення відповідальності. Наприклад, у соціальних мережах, таких як Facebook та Instagram, власником сайту є компанія Meta, а власником сторінки, де порушено право інтелектуальної власності, може бути будь-яка фізична або юридична особа. У такому випадку відповідальність несе власник сторінки, а не власник сайту. Виявлення незаконного використання торговельних марок в Інтернеті є складним завданням. Чинне законодавство недостатньо регулює ці питання. Крім того, потрібні знання не лише в галузі права, а й в ІТ, оскільки порушення часто здійснюються за допомогою сучасних технологій.

Незаконне використання торговельних марок в Інтернеті є цивільним правопорушенням, яке порушує права потерпілої особи. Це правопорушення є підставою для цивільної відповідальності. Неправомірне використання торговельної марки в мережі Інтернет – це цивільне правопорушення, яке характеризується протиправною поведінкою, «яка порушує норму права або умови укладеного між контрагентами договору; протиправними можуть бути не лише дії, а й бездіяльність»[2]. Незаконне використання торговельної марки в Інтернеті порушує норми Цивільного кодексу України, закону «Про охорону прав на знаки для товарів та послуг» або умови ліцензійного договору. Постраждала сторона може зазнати матеріальних та мо-

[1] Мінковський В. В. Проблематика розмежування правомірного та неправомірного використання торговельної марки в мережі Інтернет. *KELM*. 2022. № 1(45). С. 193-197.

[2] Заіка Ю. О. Українське цивільне право: навч. посіб. Київ: Істина, 2005. 312 с.

ральних збитків. При цьому матеріальні збитки включають реальні витрати та втрачену вигоду, а моральні – шкоду діловій репутації.

Для притягнення до відповідальності необхідно довести причинно-наслідковий зв'язок між незаконними діями та завданими збитками.

При цьому порушення може бути вчинене як навмисно, так і через необережність. Навмисне порушення передбачає усвідомлення незаконності дій та бажання або свідоме допущення шкідливих наслідків. Необережність – це завдання збитків через неусвідомлення їх шкідливості.

Незаконне використання торговельних марок в Інтернеті може здійснюватись, зокрема: на спеціально створених веб-сайтах для продажу підробок; на торгових онлайн-майданчиках; у соціальних мережах.

Так, веб-сайти складаються з видимої та технічної частин. Незаконне використання торговельної марки може відбуватися як у видимому (доменне ім'я), так і в технічному (мета-теги) аспектах. Отже, використання торгової марки в доменному імені та мета-тегах, таких як «title», «keywords», «description», «img», без дозволу є неправомірним[1]. Так, поняття «домену» наведено у статті 2 Закону України «Про електронні комунікації», відповідно до якої: «домен є частиною ієрархічного адресного простору мережі Інтернет, що має унікальну назву (доменне ім'я), яка її ідентифікує, обслуговується групою серверів доменних імен та адмініструється централізовано»[2]. У свою чергу, у розумінні статті 1 Закону України «Про охорону прав на знаки для товарів та послуг» «доменне ім'я є як ім'ям, яке використовується для адресації комп'ютерів і ресурсів в Інтернеті»[3].

---

[1] Як правильно прописати мета-теги Title та Description. URL: https://lanet.dick/yak-prawlno-propysaty-meta- tehy-title-i-description/; Булеца С. Б. Віртуальне майно у метавсесвіті як об'єкт цивільних прав. *Науковий вісник Ужгородського національного університету.* Серія: Право. 2022. Том 1. № 72. С. 126-133; Позова Д. Д. Деякі питання контрафакції в мережі Інтернет. *Актуальні проблеми захисту права власності*: матер. кругл. столу (м. Одеса,17 червня 2016 р.). За заг. ред. Є. О. Харитонова. Одеса: Фенікс, 2016. С. 71-74. Voitovych P., Bondarenko K., Ennan R., Havlovska A., Shliienko V. Objects of intellectual property rights created by artificial intelligence: international legal regulation. *Cuestiones Politicas.* Vol. 39. Iss. 68. Universidad del Zulia, 2021. P. 505-519.

[2] Про електронні комунікації: Закон України від 16.12.2020 р. № 1089-IX. URL: https://zakon.rada.gov.ua /laws/show/1089-20#Text

[3] Про охорону прав на знаки для товарів та послуг: Закон України від 15.12.1993 р. № 3689-XII. *Відомості Верховної Ради України.* 1994. № 7. Ст. 36. URL: https://zakon.rada.gov.Ua/laws/show/3689-12#Text

Таким чином, неправомірним використанням торговельної марки у доменному імені веб-сайту, буде вважатися: «застосування текстового позначення, яке складає частину торговельної марки або такого, яке можна сплутати з торговельною маркою у випадку відсутності у ліцензійному договорі дозволу на зазначене використання торговельної марки або ж у випадку використання за відсутності ліцензійного договору у спосіб, не передбачений частиною шостою статті 16 Закону України «Про охорону прав на знаки для товарів та послуг»[1].

Використання торговельної марки на веб-сайті вважається незаконним, якщо правовласник не випускав товари під цією маркою в обіг, а порушник продає товари з цією маркою без ліцензійної угоди. Потерпілою стороною може бути власник торгової марки або ліцензіат. Однак, довести незаконність складно через труднощі з ідентифікацією власника сайту, підтвердженням випуску товару в обіг та встановленням походження товару (оригінал чи підробка). Вирішення цих проблем вимагає часу та витрат, а іноді можливе лише через суд, за допомогою заходів забезпечення позову та доказів.

Важливо зазначити, що коли власник торгової марки випустив товар в обіг, а власник веб-сайту перепродає цей товар, то використання торгової марки буде законним, згідно з частиною шостою статті 16 Закону України «Про охорону прав на знаки для товарів та послуг». Для того, щоб притягнути до відповідальності за незаконне використання торгової марки на веб-сайті, необхідно встановити наявність таких складових правопорушення: протиправна поведінка; збитки; причинний зв'язок; вина.

Слід враховувати відмінність між умисним правопорушенням і правопорушенням з необережністю. Умисел – це усвідомлене порушення з бажанням або свідомим допущенням шкідливих наслідків (при наявності умислу порушник права інтелектуальної власності неправомірно розміщує торговельну марку у зовнішній та/або технічній стороні свого веб-сайту, передбачає можливі шкідливі наслідки таких дій та бажає їх настання (прямий умисел) або не бажає, однак свідомо припускає їх настання (непрямий умисел) Необережність – це порушення, яке призвело до збитків, але порушник не усвідомлював їх шкідливість (полягає у розміщенні торговельної марки

[1] Там само.

на веб- сайті порушника, що призвело до завдання збитків, шкідливість яких він не усвідомлював).

Наступним паразитичним способом використання торговельної марки в мережі Інтернет є використання її на торговельних майданчиках та маркетплейсах. Визначається, що «торговельний майданчик є комплексом матеріально-технічних засобів, який забезпечує користувачам рішення для участі у електронній комерції»[1]. Своєю чергою, дещо конкретніше визначає це поняття компанія Google у своєму сервісі Google Merchant Center, а саме як «платформа електронної комерції, на якій представлено товари або веб-сайти різних продавців у тому самому домені»[2]. Під маркетплейсом слід розуміти: «ресурс в мережі Інтернет, за допомогою якого була б можливість комунікувати з широким колом клієнтів, можливість здійснення он-лайн платежів, тощо»[3]. Проте, існує й дещо інша думка щодо визначення цього поняття як: «тип веб-сайтів електронної комерції, де інформацію про продукти або послуги надають треті сторони»[4]. Можна говорити про більш точне визначення у другому прикладі.

Торгові онлайн-майданчики та веб-сайти для продажу контрафактних товарів мають багато спільного, зокрема способи незаконного використання торговельних марок. Власниками торгових майданчиків зазвичай є юридичні особи, а власниками окремих оголошень – як юридичні, так і фізичні особи. Незаконне використання торговельних марок найчастіше відбувається в окремих оголошеннях, оскільки майданчики передбачають створення оголошень користувачами, які несуть за них відповідальність. Однак модерація оголошень не завжди відповідає вимогам законодавства, оскільки адміністрація майданчика не може перевірити наявність ліцензійних угод та інші обставини. З технічної точки зору, власник оголошення обмежений у виборі способів використання торгової марки, оскільки майданчик має свої правила.

---

[1] Що таке електронний торговельний майданчик. URL: https://smarttender.biz/terminy/view/elektronniy- torgovelniy-maydanchyk/

[2] Про торговельні майданчики. URL: https://support.google.com/merchants/answer/6363319?hl=uk

[3] Правові аспекти організації роботи маркетплейсів. URL: https://legalitgroup.com/pravovi-aspekty-marketplace/

[4] Маркетплейс. URL: https://uk.wikipedia.org/wiki/%D0%9C%D0%B0%D1%80%D0%BA%D0%B5%D1% 82%D0% %D0%BB%D0 %B5%D0%B9%D1%81

Різні майданчики можуть використовувати різні мета-теги, але деякі з них, наприклад «title» та «img», використовуються майже на всіх майданчиках. Це пов'язано з тим, що кожна сторінка має заголовок і зображення. Саме ці теги можуть містити назву та зображення торговельної марки.

Неправомірне використання торговельної марки на веб-сайті торговельного майданчика також є цивільним правопорушенням. При цьому протиправна поведінка полягає у вчиненні дій, що порушують норми чинного законодавства у галузі права інтелектуальної власності[1]. Незаконне використання торговельної марки на торгових онлайн-майданчиках може включати: розміщення текстового або графічного зображення торгової марки на сторінці оголошення; використання торгової марки всупереч умовам ліцензійної угоди. Збитки від такого порушення схожі на збитки від незаконного використання торгової марки на окремому веб-сайті, але можуть бути більшими. Це пов'язано з тим, що торгові майданчики залучають багато цільових користувачів, які шукають конкретні товари. Причинний зв'язок між незаконними діями та збитками доводиться так само, як і у випадку з окремим веб-сайтом. Наприклад, продаж підроблених товарів через оголошення з незаконним використанням торгової марки завдає шкоди репутації її власника. Вина порушника може бути як умисною, так і необережною, як і при порушенні на окремому веб-сайті.

Варто підкреслити, що ефективний захист прав інтелектуальної власності неможливий без активної участі національного бізнесу, зокрема маркетплейсів, які об'єднують продавців і покупців та мають дотримуватися принципів IP-культури. У липні 2024 року IP-офіс України розпочав співпрацю з OLX. UA, спрямовану на боротьбу з контрафактною продукцією, розробку сучасних механізмів захисту прав інтелектуальної власності в Інтернеті, аналіз ринку, а також проведення консультацій та просвітницьких заходів[2].

Крім того, обговорення проблем незаконного використання торговельних марок на маркетплейсах повинно відбуватися з урахуван-

[1] Харитонова О. І. Право інтелектуальної власності: підручник. Київ: Юрінком Інтер. 2023. 540 с.; Харитонова О. І. Правовідносини інтелектуальної власності, що виникають внаслідок створення результатів творчої діяльності (концептуальні засади): монографія. Одеса: Фенікс, 2011. 52 с.

[2] WIPO Alert, боротьба з піратством та контрафактом: про нові практики IP захисту на IP LET FORUM 2024 URL: https://nipo.gov.ua/ip-let-forum-2024-s3-1/

ням актуальних викликів, що стоять перед сферою інтелектуальної власності. Співпраця стейкхолдерів у цьому напрямку є важливим кроком до створення більш прозорого та безпечного ринку.

Крім того, важливо враховувати світовий довід вирішення означеного питання, зокрема Європейського суду. ЄС у рішенні від 22 грудня 2022 року, Christian Louboutin, C-148/21 та C-184/21, EU:C:2022:1016. «було роз'яснено, що оператор онлайн-майданчика може бути відповідальним за порушення прав на торговельну марку, якщо:

1) на онлайн-майданчику містяться також власні торгові пропозиції цього оператора;
2) сторонні продавці пропонують для продажу на цьому ринку без згоди власника цієї торговельної марки такі товари з цим знаком;
3) добре поінформований і розумно уважний користувач цього сайту встановить зв'язок між послугами цього оператора та спірним знаком, іншими словами, у такого користувача може скластися враження, що цей оператор сам займається рекламуванням від свого імені і за власний рахунок товарів, що неправомірно використовують знак»[1].

Ще одним випадком неправомірного використання торговельної марки у мережі Інтернет можна розглядати її «використання у соціальних мережах, які є веб-сайтом або іншою службою в мережі Інтернет, яка дозволяє користувачам створювати публічні або напівпублічні анкети (акаунти), складати списки користувачів, з якими вони мають зв'язок, та переглядати власний список зв'язків і списки інших користувачів»[2]. У соціальній мережі «Facebook» таке використання може розглядатися у вигляді текстових позначень та графічних зображень. Зокрема, текстове позначення може застосовуватись у назвах облікових записів (окремих сторінок або спільнот) чи у описі цих записів, а також у публікаціях, які користувачі можуть вільно створювати. У свою чергу, графічні зображення застосовуються у контенті, який створюється власником такої сторінки у вигляді зображень

[1] Соколова В. Чи має власник онлайн-майданчиків відповідати за продаж підробок? URL: https://yur-gazeta.com/publications/practice/zahist-intelektualnoyi-vlasnosti-avtorske-pravo/chi-mae-vlasnik- onlaynmaydanchikiv-vidpovidati-za-prodazh-pidrobok.html

[2] Прокопенко В. Правова природа сторінок у соціальних мережах. URL: https://yur- gazeta.com/publications/practice/zahist-intelektualnoyi-vlasnosti-avtorske-pravo/pravova-priroda-storinok-u- socialnih-merezhah.html

або відеоматеріалів, які містять у собі торговельну марку. Прикладом такого неправомірного використання може слугувати створення рекламного облікового запису у якому містяться текстові та графічні позначення торговельної марки, спосіб використання яких не регулюються ліцензійним договором, або не передбачені частиною шостою статті 16 Закону України «Про охорону прав на знаки для товарів та послуг». Окремої уваги заслуговує той факт, що відповідно до Умов надання послуг компанії **Meta**, користувач повинен володіти правами на інтелектуальну власність (авторськими правами або торговельними марками) на будь-який контент, який він створює та поширює. Водночас для користування послугами компанії необхідно надати певні юридичні дозволи (так звану «ліцензію») на використання цього контенту. Зокрема, «коли користувач поширює, публікує або завантажує контент, що є об'єктом прав на інтелектуальну власність, він надає компанії невиключну, безоплатну глобальну ліцензію з правом передавання й субліцензування на розміщення, використання, розповсюдження, змінення, виконання, копіювання, публічне виконання або показ, переклад користувацького контенту та створення похідних творів на його основі»[1].

Аналізуючи викладені положення Умов користування, постає питання щодо правомірності використання торговельної марки в соціальній мережі. Користувач Facebook може послуговуватися торговельною маркою на підставі договору або ж неправомірно використовувати її за відсутності ліцензійного договору та у спосіб, що не відповідає частині шостій статті 16 Закону України «Про охорону прав на знаки для товарів та послуг». Якщо торговельна марка використовується на підставі ліцензійного договору, правомірність такого використання залежатиме від наявності в договорі положень про субліцензування та згоди власника свідоцтва на торговельну марку на його надання. Тобто, якщо договір не містить положень про субліцензію або якщо правовласник не надає згоди на її видачу, викори-

[1] Умови надання послуг URL: https://uk-ua.facebook.com/legal/terms; Булеца С. Б. Право власності на об'єкти віртуальної власності. Розділ ІІІ. цивільне право і цивільний процес; сімейне право; міжнародне приватне право. *Аналітично-порівняльне правознавство.* 2023 С. 143-148; Кулініч О. О., Мазуренко С. В. Зображення, виконані з використанням програмного забезпечення, як об'єкт авторського права. *Правове життя сучасної України*: у 2 т.: матер. Міжнар. наук.-практ. конф. (м. Одеса, 17 трав. 2019 р.). Одеса: Гельветика, 2019. Т 2. С. 562-564.

стання торговельної марки компанією Meta вважатиметься неправомірним. В іншому випадку, коли використання торговельної марки здійснюється на підставі статті 16 Закону України «Про охорону прав на знаки для товарів та послуг», надання ліцензії відповідно до Умов користування є незаконним. Це пояснюється тим, що такий користувач соціальної мережі не має жодних законних прав на торговельну марку.

Ще однією не менш популярною соціальною мережею є «Instagram». У ній торговельна марка також може використовуватись як у текстовому так й у графічному вигляді. У текстовому вигляді вона може застосовуватись у назві рекламного облікового запису (аккаунту) або у описі рекламної публікації. У свою чергу, у графічному вигляді торговельна марка використовується у фото- та відео- публікаціях або у тимчасових фото- та відео- публікаціях (сторіс). Неправомірність такого використання має місце, коли користувач цієї соціальної мережі створює обліковий запис із застосуванням позначення торговельної марки а також застосовує її у публікаціях з метою отримання прибутку за відсутності договору та за наявності обставин, які підтверджують неправомірність дій у широкому сенсі цього поняття. Крім того, умови користування «Instagram» передбачають такі ж положення щодо надання користувачем безоплатної ліцензії на використання та поширення контенту як і у «Facebook», що може ставити під сумнів правомірність такого використання. Однак в умовах використання «Instagram» існує цікаве положення щодо використання торговельної марки цієї соціальної мережі. Так, відповідно до нього «Користувач не може змінювати, перекладати жодні продукти чи їх компоненти, створювати похідні продукти на їх основі або розбирати їх для подальшого відтворення, а також не може використовувати ім'я домену або URL-адресу у своєму імені користувача без попередньої письмової згоди компанії «Meta»»[80]. Таким чином, зазначені Умови використання захищають лише інтереси компанії-власника соціальної мережі та створюють середовище для неправомірного використання інших торговельних марок.

Використання торговельних марок у соціальних мережах, таких як Facebook та Instagram, створює унікальні виклики для захисту прав інтелектуальної власності. Зокрема, умови користування цих платформ дозволяють компанії Meta змінювати та створювати по-

хідні твори на основі користувацького контенту, що включає об'єкти інтелектуальної власності. Згідно з Законом України «Про охорону прав на знаки для товарів та послуг», такі змінені або похідні торговельні марки можуть не мати правової охорони. Це створює ризик збільшення випадків неправомірного використання змінених об'єктів інтелектуальної власності, що ускладнює захист прав власників, збільшує потенційні збитки та ускладнює притягнення порушників до відповідальності. Фактично, власник торговельної марки опиняється у складному становищі, оскільки закон не надає захисту зміненим об'єктам, що ставить під сумнів правомірність дій порушників та ускладнює процес притягнення їх до відповідальності.

Для вирішення означеної проблеми доцільним слід розглядати доповнення Закону України «Про охорону прав на знаки для товарів та послуг» положеннями, які б визнавали неправомірним використання змінених торговельних марок, що вводять споживачів в оману щодо якості та виробника товарів.

Таком чином, неправомірне використання торговельної марки в соціальних мережах включає: розміщення текстових або графічних позначень, що містять торговельну марку, з порушенням законодавства або умов ліцензійного договору: використання торговельної марки з порушенням статті 16 Закону України «Про охорону прав на знаки для товарів та послуг»; використання торговельної марки на підставі ліцензійного договору, який не передбачає її використання в Інтернеті; використання торговельної марки за ліцензійним договором, який не передбачає субліцензування, у випадках, коли соціальні мережі вимагають надання ліцензії на використання об'єктів інтелектуальної власності.

Протиправна поведінка в розглянутому випадку полягає в розміщенні торговельної марки з порушенням закону або договору, яка призводить до збитків володільця торгівельної марки, аналогічних збиткам від інших видів порушення прав інтелектуальної власності. При цьому має існувати доведений зв'язок між протиправною поведінкою та збитками. Вина в цьому виді правопорушіень може бути у формі умислу або необережності.

Війна, розв'язана Росією проти України, суттєво погіршує ситуацію з захистом прав на торговельні марки. Санкції, запроваджені проти агресора, стимулюють зростання випадків незаконного вико-

ристання торговельних марок в Інтернеті, як зареєстрованих в Україні, так і міжнародних.

Таким чином, можна підсумувати, що на сьогодні існує безліч способів незаконного використання торговельних марок в Інтернеті, включаючи веб- сайти, онлайн-платформи оголошень, соціальні мережі, месенджери. Для визначення правомірності використання торговельної марки необхідно враховувати широкий спектр обставин.

Важливим кроком для розвитку захисту прав ІВ, зокрема на торговельні марки, є визначення у судовій практиці загальних підходів до виникнення у позивачів прав на звернення з позовом за тих чи інших умов.

Останнім часом спостерігається зростання кількості судових позовів щодо порушення авторських прав компаніями, які розробляють генеративні моделі ШІ. З одного боку, медіакомпанії, зокрема *The New York Times*, оскаржують дії OpenAI та Microsoft, звинувачуючи їх у незаконному використанні контенту для навчання штучного інтелекту. З іншого боку, технологічні корпорації захищають своє право на інновації, наголошуючи, що ШІ відкриває нові можливості для творчості. Подібні суперечки тривають і в музичній та кіноіндустрії, а також у сфері стокової фотографії. За кожним таким позовом стоять фінансові претензії на мільярди доларів, що свідчить про вихід проблеми авторського права та ШІ за межі традиційного плагіату в текстах, охоплюючи інші галузі творчої діяльності.

Наприкінці 2023 року *The New York Times* подало до суду на Microsoft та OpenAI, звинувативши їх у порушенні авторських прав. Це перше велике американське медіа, яке офіційно висунуло такі претензії до розробників генеративного ШІ. У своєму позові газета не зазначає конкретної суми компенсації, однак стверджує, що завдані їй збитки сягають мільярдів доларів. Крім того, *The New York Times* вимагає заборонити компаніям використання її контенту та зобов'язати їх знищити набори даних, що містять її матеріали. Наразі справа перебуває на розгляді суду, і остаточне рішення ще не ухвалене. Проте медіа надало переконливі докази копіювання його контенту, що ускладнює завдання відповідачів щодо їх спростувань[1].

[1] Пилипів І., Матяш А. Війна за мільярди: проблема авторського права та ШІ вийшла за рамки звичайного плагіату. URL: https://epravda. com.ua/publications/2024/05/07/713178/

У всіх сферах, де штучний інтелект здатен генерувати матеріали, зростає кількість позовів, пов'язаних із плагіатом та неправомірним використанням творів. Це стосується зображень, музики, поезії, прозових текстів та іншого творчого контенту. Однак судові справи – лише частина ширшої тенденції. На глобальному рівні поки що відсутнє чітке законодавче регулювання таких питань, оскільки закони про авторське право та інтелектуальну власність у контексті ШІ перебувають на стадії розробки.

Наразі прецедентною слід розглядати угоду OpenAI з британським агентством *Financial Times,* яка дозволяє використовувати його матеріали для навчання ШІ-моделей. Для видання така співпраця сприятиме залученню нових читачів, оскільки ChatGPT включатиме посилання на *FT* у відповідях, заснованих на його контенті. Подібні домовленості OpenAI вже підписала з *Associated Press, Axel Springer, Le Monde* та *Prisa Media.*

Важливим чинником, що спонукає медіа до таких угод, є складне бізнес-середовище, в якому вони працюють. Хоча деталі фінансових домовленостей зазвичай не розголошуються, відомо, що відповідно до аналогічного договору з Google платформа *Reddit* щороку отримуватиме приблизно 60 мільйонів доларів[1].

Наразі в Україні роботу генеративних моделей частково регулює закон «Про авторське право і суміжні права», який сфокусований передусім на інтелектуальній діяльності людини. Проте в березні 2023 року в ньому з'явилася ст. 33 (sui-generis або права особливого роду) щодо неоригінальних об'єктів, згенерованих комп'ютером. Слід відмітити, що Україна стала одною з перших країн у світі, яка ввела таку статтю. Відповідна норма встановлює, що «суб'єктами права особливого роду на такі неоригінальні об'єкти є особи, яким належать майнові права на комп'ютерні програми (ШІ), або особи, що мають ліцензійні права на такі програми»[2]. Відповідно, права на контент, створений за допомогою AI, можуть належати розробникам мовних моделей або користувачам, які володіють підпискою чи ліцензією на користування системою.

---

[1] Там само.

[2] Про авторське право і суміжні права: Закон України від 01.12.2022 № 2811-IX URL: https://zakon.rada. gov.ua/laws/show/2811 -20#Text

Крім цього, правове регулювання використання штучного інтелекту в Україні частково здійснюється законами України «Про захист персональних даних», «Про захист прав споживачів», «Про електронні довірчі послуги» тощо.

Сьогодні в Україні ІР офіс вже має практику видачі свідоцтв про реєстрацію авторського права на твори, до яких включені зображення, що були створені за допомогою штучного інтелекту [1].

Штучний інтелект (ШІ) активно інтегрується в академічне середовище, змінюючи способи створення, обробки та поширення наукового контенту. Водночас це породжує важливі питання щодо охорони та захисту прав інтелектуальної власності (ІВ). З одного боку, ШІ сприяє покращенню академічної продуктивності та доступу до знань, з іншого – створює виклики, пов'язані з авторським правом, академічною доброчесністю та використанням даних.

Використання АІ в академічному середовищі має свої значні переваги, які пов'язані з автоматизацією досліджень і аналізу даних; захистом прав ІВ і виявленням плагіату; оцифруванням та збереженням наукової та культурної спадщини; оптимізацією наукових комунікацій.

Наразі АІ здатний швидко опрацьовувати великі обсяги наукової інформації, аналізувати публікації та виявляти тренди, що значно пришвидшує дослідницьку діяльність. Крім того, використання алгоритмів АІ дозволяє прогнозувати напрямки наукових новацій та аналізувати цитованість академічних текстів. Важливим компонентом у використанні АІ є і розвиток інструментів перевірки текстів на унікальність, яиявлення порушень авторських прав, зокрема, плагіату завдяки машинному навчанню та нейромережам. Автоматичне розпізнавання тексту (OCR) дозволяє зберігати та аналізувати старі рукописи, архівні документи, що сприяє їхньому захисту та поширенню в легальному просторі. Алгоритми АІ широко використовуються для автоматизованого перекладу та генерації анотацій, що сприяє міжнародному обміну знаннями, а також сприяють

[1] В Україні вперше зареєстровано авторське право на твори, до яких включені зображення, згенеровані ШІ. URL: https://nipo.gov.ua/ap-zobrazhennia-shi/; Вальчук Д. В. Авторське право штучного інтелекту: проблеми та шляхи вирішення. *Modern scientific journal.* 2024. № 3. С. 7-15. URL: https://joumals.indexcopemicus.com/api/file/viewbyfileid/2056038; Бойко Д. Авторські права і ШІ: межі добросовісного використання. URL:https://dc.org.ua/news/avtorski-prava-i-shi-mezhi-dobrosovisnogo- vykorystannya

відкритій науці шляхом класифікації та розподілу інформації в наукових репозитаріях.

Разом з тим варто варто пам'ятати про ризики, які несуть алгоротми AI для академічного середовища. Використання AI у наукових дослідженнях може спричиняти правопорушення, пов'язані з порушенням авторського права, плагіатом, незаконним використанням даних та академічною недоброчесністю. AI може генерувати неправдиві або неіснуючі джерела, що підриває довіру до наукових досліджень та спотворює академічну комунікацію. Важливим питанням постає питання ймовірність витоку конфіденційної наукової інформації при використанні AI для обробки закритих або неопублікованих досліджень.

Використання AI у науковій діяльності є неминучим, адже він значно розширює можливості наукової діяльності. Проте використання AI потребує вдосконалення правових механізмів захисту інтелектуальної власності. Важливо розробити чіткі норми щодо прав на AI-генерований контент, впровадити етичні стандарти для запобігання академічним зловживанням та посилити захист авторських прав у цифровому середовищі. Захист інтелектуальної власності в академічному середовищі повинен передбачати баланс між розвитком технологій та дотриманням правової етики. Законодавче врегулювання цього питання, а також підвищення рівня цифрової грамотності серед науковців та студентів, є ключовими кроками для мінімізації правопорушень у цій сфері.

Аналізуючи дослідження Г. О. Андрощука[1], можна відзначити, що штучний інтелект сьогодні активно використовується у різних сферах, таких як транспорт, телекомунікації, біологічні науки, медицина, персональні технології та безпека. Як багатофункціональна технологія, AI вже має значний вплив на економічні та соціальні процеси, змінюючи підходи до створення, виробництва та розподілу товарів і послуг, оформлення патентів, авторських прав тощо. Очікується, що цей вплив лише посилюватиметься в майбутньому.

Інтелектуальна власність (ІВ) і штучний інтелект мають багато точок перетину, оскільки ключовою метою політики у сфері ІВ є стимулювання інновацій та творчості в межах економічних і куль-

[1] Андрощук Г. О. Штучний інтелект і інтелектуальна власність: проблеми регулювання. URL: https://doi.org/10.32689/2617-9660-2021-2(14)- 58-78

турних систем. Традиційно системи ІВ слугували інструментом заохочення винахідницької та творчої діяльності, що раніше вважалося виключно людською здатністю. Однак швидкий розвиток ШІ як універсальної технології ставить під сумнів усталені підходи до охорони інтелектуальної власності, викликаючи необхідність перегляду існуючих правових норм.

Для багатьох країн світу штучний інтелект став ключовим елементом стратегічного розвитку, що зумовлює необхідність формування національних стратегій його впровадження та регулювання. Держави активно розробляють політику, спрямовану на розвиток ШІ-потенціалу, а також встановлюють правові механізми для його контролю. Водночас перед світовою спільнотою постають нові виклики, що потребують комплексного та глобального підходу до врегулювання правових аспектів, пов'язаних із використанням ШІ в економіці, культурі та інтелектуальній діяльності.

Підсумовуючи аналіз, слід зазначити, що полігібридні війни, створюючи «гібридні загрози» в усіх сферах життя людини і суспільства, порушують права та свободи людини, або перешкоджають реалізації останніх, що зумовлює необхідність пошуку «гібридних відповідей», зокрема з використанням правових (юридичних засобів /заходів). Головною ознакою такої війни є тещо вона є одночасно війною інформаційною, економічною, репутаційною, смисловою. На неї повинні працювати всі, хто має вплив на населення. Військові дії задають лише фон для більш масштабної війни в людському розумі[1].

Російські операції в Україні порівнюють із китайською концепцією війни без обмежень, що містить дуже багато невійськових інструментів. І одній, і другій «властиві однотипні елементи: інвестиції, купівля медіа, підтримка політичних партій, розвідувальне проникнення в європейські структури, встановлення зв'язків між релігійними інституціями, використання нерозв'язаних етнічних конфліктів, підтримка російських засобів інформації за кордоном (типу Russia Today), координовані кібератаки» [2].

[1] Магда Є. В. Гібридна війна: вижити і перемогти. Харків: Віват, 2015. С. 12. Почепцов Г. Гібридна війна: інформаційна складова. URL: //https://ms.detector.media/mediaanalitika/post/14501/2015-10-25-gibrydnaviyna- informatsiyna-skladova/

[2] Почепцов Г. Гібридна війна: інформаційна складова. URL: //https://ms.detector.media/mediaanalitika/post/14501/2015-10-25-gibrydnaviyna-informatsiyna-skladova/

Разом з тим, повномасштабна російська агресія виявила нагальну потребу в удосконаленні правового механізму, особливо в частині регулювання цивільних відносин та захисту прав в умовах воєнного стану. Війна вимагає ефективного правового регулювання, що базується на глибокому розумінні суспільних процесів та поєднанні приватно-правових і публічно-правових методів.

Сьогодні в правовому полі України здійснюється масштабна трансформація, обумовлена запровадженням воєнного стану. В надскладних умовах здійснюються дієві кроки спрямовані на максимальну охорону і захист прав громадян, зокрема і прав інтелектуальної власності.

Після початку війни у 2014 році цивільне законодавство не зазнало обмежень прав, тривали активні реформи цивільного законодавства для адаптації до права ЄС. Обмеження прав після повномасштабного вторгнення і введення воєнного стану у 2022 році загалом були мінімальними, а концепція адаптації національного законодавства до права ЄС збережена.

Концепція приватного права та механізми його реалізації можуть суттєво модифікуватись в умовах гібридної війни. Однак, поєднання заходів заохочення та примусу є оптимальним. Комунікація між владою та суспільством є невід'ємною частиною ефективної боротьби з викликами гібридної війни, зокрема у сфері інтелектуальної власності.

Війна, яка триває в Україні, завдає значних економічних збитків, що стимулює нелегальне виробництво та розповсюдження контрафактної продукції, яка може становити загрозу національній безпеці, особливо в таких сферах, як фармацевтика, оборона та харчова промисловість. Вона стимулює кіберзлочинність, включаючи піратство, крадіжку даних та інші порушення. Крім того, використання об'єктів інтелектуальної власності в інформаційній війні також вимагає адекватного правового захисту. Застосування заходів кібербезпеки може обмежувати право на інформацію, особливо в транскордонному контексті. Для вирішення цієї колізії необхідно використовувати «гібридні» (приватно-публічні) заходи, що поєднують захист права на інформацію з вимогами кібербезпеки.

Наразі основні правопорушення у сфері інтелектуальної власності в мережі Інтернет включають незаконне копіювання, поширення та

використання захищених матеріалів без згоди правовласника. Значні ризики становить нелегальне завантаження та розповсюдження програмного забезпечення, захищеного авторським правом, що порушує права розробників. При цьому поширеними проблемами залишаються плагіат і крадіжка контенту (статті, блоги, відео тощо) без належного посилання або дозволу автора. Варто відмітити, що неправомірне використання торговельних марок, зокрема в доменних іменах, може вводити споживачів в оману та спричиняти фінансові втрати для власників брендів. Сьогодні потребує ефективного правового реагування розробка та використання шкідливого ПЗ для обходу систем захисту авторських прав, яка загрожує безпеці цифрового простору.

Як позитивний крок слід розглядати підписання меморандумів ВС України з ВОІВ. Ці ініціативи спрямовані на підвищення кваліфікації суддів та впровадження світового судового досвіду й підходів у практику вирішення спорів в Україні. Документи передбачають співпрацю у розробленні та реалізації програми безперервної освіти суддів з питань інтелектуальної власності, а також наповнення Бази судових рішень **WIPO Lex-Judgments**, створеної ВОІВ. У межах цієї взаємодії до бази вже внесено шість рішень Верховного Суду України у сфері інтелектуальної власності. Зазначена База забезпечує доступ до найважливіших судових рішень судів різних країн світу (понад 200 юрисдикцій) з автоматичним перекладом. Безумовно отримана можливість стане позитивним кроком з огляду на необхідність аналізу існуючих правопорушень у сфері інтелектуальної власності на сучасному етапі, вдосконалення механізму захисту об'єктів інтелектуальної власності та підвищення кваліфікації суддів в IP-сфері.

Ключові слова: інтелектуальна власність, порушення прав інтелектуальної власності, порушення в Інтернеті, воєнний стан, гібридна війна, порушення авторських прав, кіберзлочинність, інформаційні війни, захист авторських прав в Інтернеті, інтернет-піратство, соціальні мережі, торговельні марки, недобросовісна конкуренція, штучний інтелект.

Розділ 11

КІБЕРЗАГРОЗИ У ГІБРИДНІЙ КІБЕРВІЙНІ: ДІЯ І ПРОТИДІЯ

DOI

Євген Харитонов
доктор юридичних наук, професор,
член-кореспондент НАПрН України

Олена Харитонова
докторка юридичних наук, професорка,
членкиня-кореспондент НАПрН України

Попередні зауваження

«Віртуалізація» суспільства супроводжується зростанням значення кіберзброї та штучного інтелекту в гібридній війні.

Одним з чинників цього було те, що кіберзброя потенційно є не тільки руйнівною силою у «воєнній» війні, а й засобом тиску в позірно мирний час. Генерал Джеймс Картрайт, котрий у 2004 році очолив Стратегічне командування США в Омасі (яке відповідає за ядерний арсенал держави), думав використати її для «перезапуску дипломатії», тобто, щоб змусити іншу країну усвідомити, що в неї немає іншого вибору, окрім як погодитися на переговори».[1]

Нам здається доречним згадати влучне та емоційно забарвлене зауваження щодо «буденності» кібервійни Девіда Е. Сенгера: «Так хотілось би думати, наче кібервійна якось відрізняється від інших конфліктів, наче вона розгортається собі десь у хмарах окремо від того, що відбувається на землі. Коли держави створювали військово-повітряні сили, то міркували так само: повітряні бої – це одне, а перестрілка в окопах – інше. Аж під час Другої світової війни утвердилася концепція «єдиного бойового простору», що охоплює повітря, землю та море. У деяких краї-

[1] Сенгер, Девід Е. Досконала зброя. Війна, саботаж і страх у кіберепоху. С. 44.

нах світу до цього вже додають і кіберпростір. Просто це важче помітити».[1]

Книга Д. Сенгера, де міститься це висловлювання, була видана у США відносно недавно – у 2018 році.[2] Але за час, що минув після її видання, здається, практично не залишилось країн, котрі так чи інакше не переконались би у слушності цього зауваження. Чимало зусиль до цього доклала росія, щодо агресії якої проти України Д. Сенгер зазначив: «У битві за територію України та душі її мешканців традиційна війна й кібервійна не просто доповнювали одна одну. Вони, немов стрічка Мебіуса, відображають конфлікт XXI століття, гладко раз у раз перетікаючи з поверхні на поверхню. Путін продемонстрував світові, наскільки ефективна така стратегія «гібридної війни…».[3]

Інформаційній гібридній війни, зокрема, правовим проблемам, що при цьому виникають, ми плануємо присвятити спеціальне дослідження (власне, окремі питання цієї проблематики ми вже розглядали у 2016-2018 рр.[4], але відтоді минуло чимало часу і багато що змінилося).

---

1 Сенгер, Девід Е. Досконала зброя. Війна, саботаж і страх у кіберепоху. Пер. з англ. Вікторія Дєдик: фах.ред.укр.вид Олександр Дєдик і Олег Фешовець. Львів: Астролябія, 2022. С. 227.

2 Sanger, David E. The Perfect Weapon: War, Sabotage and Fear in the Cyber Agt. New York : Crown Publishing Group, 2018.

3 Сенгер, Девід Е. Досконала зброя. С. 227.

4 Information security and IT law in conditions of integration processes: [Collective monograph]. Edited by O. Kharytonova, E. Kharytonov. Riga: Izdevnieciba Baltija Publishing, 2017. 213 p.; Харитонов Є. О. Інформаційна безпека з погляду цивілістики. *Цивільне право та інформаційна безпека в умовах інтеграційних процесів :* мат. кругл. столу (3 червня 2017 р., м. Одеса). Збірник матеріалів Міжнародного Конгресу «Правові проблеми державно-правового партнерства в умовах євроінтеграції», присвяченого 20-річчю Національного університету «Одеська юридична академія» (м. Одеса, 2-4 червня 2017 р.). Одеса: Юрид. Літ., 2017. С. 64-68; Харитонов Є. О., Харитонова О. І. Проблеми правового регулювання в ІТ-сфері в умовах інформаційної війни. *Проблеми відновлення конституційного ладу в Україні:* Матеріали міжнародної науково-практичної конференції. м. Київ. 19-20 травня 2017 р. Київ: Таврійський національний університет ім. В. І. Вернадського. 2017. С.159-163; Харитонов Є. О., Харитонова О. І. Проблеми відшкодування майнової шкоди у сфері використання інформаційних технологій. *Спогади про Людину, Вченого, Цивіліста (до 90-річчя від Дня народження професора Діни Василівни Бобрової)*; за заг. ред. Р. О. Стефанчука. К.: АртЕк, 2019. С. 275-287; Харитонов Є. О. COVID-19 та проблеми інформаційної безпеки. *Цивілістичні проблеми інформаційної безпеки в умовах COVID-19* : матеріали Всеукр. круглого столу, Одеса, 21 червня 2021 р. За заг. ред. Є. О. Харитонова, І. В. Давидової. Одеса : Фенікс, 2021. С. 5-9; Kharytonov E., Kharytonova O., Tolmachevska Y., Fasii B., Tkalych M. Information Security and Means of Its Legal Support. Amazonia Investiga, 8(19). P. 255-265.

Разом із тим, у цій книзі ми означимо низку основних проблем, що торкаються концепту приватного права в умовах інформаційної гібридної війни і застосування кіберзброї у традиційній «воєнній» війні.

Кібервійна, кіберзагрози та супутні терміно-поняття

Почнемо з визначення основних понять (конструктів) та категорій, що найчастіше зустрічаються/ використовуються у публікаціях, присвячених гібридній війні в інформаційній сфері (зазвичай іменується просто «інформаційною війною»).

На нашу думку, найбільш поширеними концептами і конструктами тут є: інформаційна війна, кібервійна, кіберзагрози, кібератаки, кіберзброя, кіберпростір, штучний інтелект та ін. Отже далі визначимося щодо достатньо усталеного розуміння цих категорій, скориставшись для цього довідковим виданням «Стратегічні комунікації» (і подаючи визначення у скороченому вигляді).

«Інформаційна війна» є родовим поняттям щодо усіх інших видів протиборства у інформаційній сфері, зокрема, тих, що відбуваються у кіберпросторі). Відтак кібервійну визначають як різновид інформаційної війни у кіберпросторі.[1]

Кіберзагроза характеризується як «дестабілізуючий чинник негативного впливу на об'єкт інформаційної безпеки шляхом використання технологічних можливостей кіберпростору, спрямованих на порушення конфіденційності, цілісності, авторства, спостережності та доступності інформації; загроза застосування деструктивних інформаційно-психологічних впливів на свідомість та психічний стан населення».[2] (Найбільш поширеною загрозою є кібератака – або ж – атака інформаційно-телекомунікаційної системи – цілеспрямований вплив на уразливі елементи такої системи з метою порушення доступності, цілісності та конфіденційності інформації, блокування роботи та виведення з ладу системи або її елементів; форма боротьби в телекомунікаційних системах[3]).

[1] Попова Т. В., Ліпкан В. А. Стратегічні комунікації. С. 189.
[2] Попова Т. В., Ліпкан В. А. Стратегічні комунікації. С. 189-190.
[3] Попова Т. В., Ліпкан В. А. Стратегічні комунікації. С. 35.

Як випливає з такого розуміння кіберзагроз, невід'ємною частиною їхньої характеристики є категорії «кіберзброя» і «кіберпростір».

Кіберзброя розуміється як різновид інформаційної зброї, головними елементами якої є інформація та інформаційні технології, способи і засоби інформаційного впливу й захисту віл нього, призначені для ведення інформаційної боротьби у кіберпросторі.[1]

Кіберпростір, навіть на рівні елементарних характеристик має кілька значень: 1. Електроне інформаційне середовище, утворене організованою сукупністю взаємопоєднаних за єдиними принципами та правилами інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем. 2. Середовище існування та розповсюдження інформації, створюване кіберінфраструктурою. 3. Середовище, створюване інформаційними системами, об'єднаними у локальні або глобальні комп'ютерні мережі або реалізованими на окремих комп'ютерах та інших пристроях. 4. Уявне середовище, в якому за допомогою комп'ютерних мереж циркулює цифрова інформація.[2]

Відповідно до такого розуміння цих категорій визначається поняття кіберзахисту, котрий розглядається, як: 1. Сукупність методів і заходів організаційного, нормативно-правового та технічного характеру, спрямованих на забезпечення кібербезпеки. 2. Реалізація у кіберпросторі комплексу організаційних, нормативно-правових, технічних та інших заходів для запобігання кібератакам та забезпечення кібербезпеки,[3] котра, у свою чергу, розуміється як «стан захищеності кіберпростору від кібератак, за якого забезпечується його сталий розвиток, а також своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз функціонуванню його елементів».[4]

Як зазначалося, усі згадані поняття досить чітко пов'язані з концептом «кіберпростір», котрий виступає і тлом, і кваліфікуючою ознакою кібервійни, кіберзагроз тощо.

Разом із тим, деяку непевність у цю загалом чітку систему понять додають кілька терміно-понять, у яких фігурує термін «кібернетичний» (кібернетична загроза, кібернетична зброя, кібернетичний захист, кібернетичний потенціал та ін.).

---

1 Попова Т. В., Ліпкан В. А. Стратегічні комунікації. С. 190.
2 Попова Т. В., Ліпкан В. А. Стратегічні комунікації. С. 191.
3 Попова Т. В., Ліпкан В. А. Стратегічні комунікації. С. 190.
4 Попова Т. В., Ліпкан В. А. Стратегічні комунікації. С. 189.

Зокрема, «кібернетична загроза» визначається як наміри, дії або явища, що створюють небезпеку інтересам людини, суспільства та держави шляхом інформаційного впливу на соціальні об'єкти, інформаційну інфраструктуру та інформаційні ресурси в кібернетичному просторі.[1]

Оскільки визначення поняття «кібернетичного простору» відсутнє, виникає питання, чи є це поняття тотожним поняттю «кіберпростір»?

Лише у одному випадку – «кібернетична безпека (кібербезпека)» шляхом вживання одночасно (в дужках) обох термінів – міститься натяк на те, що їх можна розцінювати як тотожні.

Утім, далі це поняття (з уточненням у дужках) визначається інакше, ніж «кібербезпека»: якщо «кібербезпека» – це стан захищеності кіберпростору від кібератак, за якого забезпечується його сталий розвиток, а також своєчасне виявлення, запобігання і нейтралізація реальних та потенційних функціонуванню його елементів, то «кібернетична безпека (кібербезпека)» – це стан захищеності в кіберпросторі життєво важливих інтересів людини і громадянина, суспільства та держави.[2]

Звісно, можна сказати, що «стан захищеності кіберпростору від кібератак» це також одночасно є і «стан захищеності в кіберпросторі інтересів людини і громадянина, суспільства та держави». Однак перше визначення є вужчим , ніж друге, оскільки загрози інтересам можуть бути не тільки від кібератак, але й від інших чинників, зокрема, від самого кіберпростору, його інфраструктури, котра охоплює не тільки сукупність інформаційно-телекомунікаційних систем тощо, але й організаційні структури, які забезпечують їхнє функціонування.

З цих міркувань здається доцільним відмовитись від «роздвоєння» терміно-поняття «кібербезпека» (а так сам від усіх терміно-понять, похідних від тих, що утворені шляхом приєднання до базового слова додатку «кібер…»). В іншому разі можна спрогнозувати високу вірогідність плутанини у нормативних актах та документах, які будуть регулювати відносини у «кіберпросторі» (чи у «кіберсфері»).

---

[1] Попова Т. В., Ліпкан В. А. Стратегічні комунікації. С. 191.

[2] Попова Т. В., Ліпкан В. А. Стратегічні комунікації. Порівн.: С. 189-191.

Проблема стримування кіберзагроз

У попередньому фрагменті цього розділу йшлося про проблеми регулювання використання кіберзброї «внутрішнім» законодавством країни, яке встановлює правила використання ШІ суб'єктами цивільних відносин у певній державі.

Однак ще більш важливим було б встановлення правил використання кіберзброї учасниками збройного конфлікту (звісно за умови дотримання ними цих правил). Бо, як гарно зауважив Девід Сенгер: «У кіберепоху ми ще не віднайшли балансу сил з головними супротивниками (яким була гарантія взаємного знищення в ядерну епоху) і, мабуть, не віднайдемо. Кіберзброя повністю відрізняється від ядерної, і поки що наслідки її застосування порівняно незначні. Однак думати так далі означає припустити, що ми зрозуміли руйнівну силу створених нами технологій і зможемо з нею упоратися. Як засвідчує історія, це надто ризиковане переконання».[1] І далі додає: «Під час Холодної війни ми хоч непросто, але навчилися жити з усвідомленням того, що ядерна зброя Радянського Союзу та Китаю націлена на нас. Не існувало ідеального захисту. Так само нам доведеться призвичаїтись жити у світі постійних кіберконфліктів».[2]

Враховуючи, що згадана праця Девіда Сенгера, як на наш погляд, наразі є не тільки найбільш цікавим і змістовним дослідженням застосування кіберзброї у сучасному світі, але й найбільш конструктивним зібранням авторських пропозицій щодо врегулювання проблем використання такої зброї, розглянемо далі можливість впровадження їх у практику долання викликів у кіберсекторі гібридної війни.

Зауважимо, що Д. Сенгер констатує існування істотних труднощів у досягненні міждержавних домовленостей про стримування кіберзагрози. Він згадує підхід Кіберкомандування США, який передбачав ледь не щоденні рейди у тил супротивника з метою виявити загрози раніше, ніж вони доберуться до американських комп'ютерних мереж – «перенести бойові дії на територію ворога», і зазначає, що це спроба використати досвід ведення антитерористичних операцій.

---

[1] Сенгер, Девід Е. Досконала зброя. Війна, саботаж і страх у кіберепоху. Пер. з англ. Вікторія Дєдик: фах. ред. укр. вид Олександр Дєдик і Олег Фешовець. Львів: Астролябія, 2022. С. 413.

[2] Сенгер, Девід Е. Досконала зброя. С.419.

«Але проблема в тім, що коли інші країни приймуть таку саму стратегію, а вони неодмінно це зроблять, – то різко зросте ймовірність того, що кібератаки переростуть у звичайні бойові дії або навіть у щось страшніше», – вважає він, а відтак пропонує визнати безглуздість наміру йти у напад без належної оборони (усунути вразливості у мережах). «Усе ускладнює та обставина, що головні цілі атак належать приватним особам. Зважаючи на те, наскільки складним є інтернет, уряд не може регулювати діяльність банків, телекомунікаційних і газових копаній, Google і Facebook у царині їхньої власної кібербезпеки. Усі системи кардинально відрізняються одна від одної. Однак час дивитися на все реально. Уряд не допоможе захистити американські установи, окрім хіба що найважливіших електромереж, системи для голосування, систем водопостачання та каналізації, фінансової системи та ядерної зброї.[1]

Оскільки можливості урядів інших держав, зокрема України, також не долають цю планку, особливого значення набуває врегулювання проблеми на «позадержавному» рівні.

Ми свідомо вживаємо тут термін «позадержавний», усвідомлюючи його некоректність, але бажаючи наголосити на важливій домінанті концепції Девіда Сенгера, котрий вважає, що «Класичні угоди з контролю над озброєнням не спрацюють: переговори щодо них ведуться роками, а процес ратифікації ще довший. Зважаючи на блискавичні темпи технологічних змін у кіберсфері, такі угоди застаріли б, ще й не набувши чинності». Тому він пропонує звернутися до інших способів досягнути мети, хоча кожен має значні недоліки.

На його думку, найцікавішим способом є Цифрова женевська конвенція (Digital Geneva Convention – ініціатива 34-х великих ІТ-компаній, які запропонували укласти конвенцію про вироблення загальних правил поведінки у кіберпросторі), у якій поки що перед ведуть компанії, а не країни. Значну роль тут відіграє Президент Microsoft Бред Сміт, котрий прагне створити модель кіберугоди між компаніями, яка б ґрунтувалася на конвенціях, що регулювали традиційне ведення війни й вдосконалювалися понад сотню років.

Утім, Девід Сенгер вважає, що «аналогію з кіберпростором провести важко. Женевські конвенції діють під час війни. Якщо ми сподіваємось створити подібний перелік правил для кібервиміру, то мусимо

[1] Сенгер, Девід Е. Досконала зброя. С. 420-421.

визначити стандарти мирного часу. І ці стандарти мають поширюватися на компанії так само, як на країни, оскільки Google, Microsoft, Facebook, Cisco творять кіберпростір, у якому розгортаються світові кіберконфлікти».

Далі коротко розглянемо, які рішення пропонуються у цьому проєкті цифрової Женевської конвенції,[1] використовуючи також кваліфікований коментар Хайді Творк (Heidi Tworek) (у адаптованому перекладі її статті для Wired).

Як вважає Хайді Творк, Microsoft, очевидно, бажає продемонструвати вміння вчитися на прикладах з історії і саме тому посилається на Женевські конвенції. Країни G7 також висловилися за необхідність затвердити універсальні норми поведінки в кіберпросторі на державному рівні. Рішення боротися з правовим онлайн-нігілізмом похвальне, однак та сама історія доводить, що одні лише міжнародні домовленості не захистять від кіберзлочинів. Найбільші шанси на успіх матимемо, якщо учасники ринку добровільно запровадять певні стандарти для галузі.

Компанія Microsoft озвучила три головні складові міжнародної співпраці для запобігання онлайн-війни:

1) держави, що підтримають цифрову Женевську конвенцію, повинні відмовитися від проведення та санкціонування кібератак;

2) держави підпишуть Технологічну угоду, в якій затвердять основи поведінки для захисту громадян в інтернеті;

3) розслідування атак та виявлення суб'єктів порушення домовленостей довірять нейтральній неурядовій організації, яка, втім, не матиме повноважень для примусу виконувати правила.

Всі ці компоненти необхідні для того, щоб споживачі довіряли технологіям, – переконані в Microsoft.

Крім Женевських конвенцій щодо ведення війни зразками для наслідування у галузі регулювання телекомунікацій слугував також Міжнародний телеграфний союз (International Telegraph Union, ITU), який розпочав роботу 1860-х і відповідав за електричний телеграфний зв'язок між країнами. З розвитком радіо, супутникового зв'язку, телебачення та інтернету з'являлися все нові відомства, що регулювали правила комунікації.

[1] Прогнімак К. Microsoft має рацію: нам потрібна цифрова Женевська конвенція. 13 травня 2017. URL: https://www.imena.ua/blog/microsoft-digital-geneva-convention/

Хайді Творк, дослідивши вплив досвід регулювання, виокремила 2 головних факти: 1) країнам вдавалося узгоджувати та дотримуватися лише технічних стандартів, але не стандартів регулювання контенту; 2) добровільні домовленості ІТ-компаній є життєво важливими для успішного захисту громадян.

Так, століття тому керівні органи країн світу об'єдналися щоб врегулювати радіо, запобігти перешкодам та розподілити роботу в частотах. В 1920-х роках європейці та американці сперечалися, чи спектр має розподілятися по країнам, чи по типу користувача. Американські радіокомпанії підтримували ідею виділення спектру для трансляції по типу використання. В 1927 році на Вашингтонській профільній конференції було прийняте рішення підтримувати американський підхід, а не європейський – тамтешні компанії пропонували призначати окремі формати використання спектру для кожної держави. Перемовини засвідчили, що комерційні радіокомпанії, коли діють об'єднано, можуть значно впливати на міжнародні домовленості.

Сьогодні важко уявити, як розвивалася би радіомережа та телекомунікації в цілому, якби на міжнародному рівні була прийнята схема, запропонована європейцями. Але затверджені параметри дозволили радіозв'язку вільно розвиватися, а ефір став незамінним супутником життя мільйонів людей по всьому світу.

Уряди країн вже мають гарну традицію узгодження технологічних вимог і стандартів, які сприяють інтеграції, розповсюдженню комунікаційної інфраструктури. Проте коли йдеться про абстрактніші поняття, такі як свобода висловлювань та вільного поширення інформації державам важче досягти згоди. Міжнародні угоди, досягнуті в Атлантік-Сіті (США) в 1947 році до сих пір звільняють передавачів зв'язку від обов'язку транслювати повідомлення, які класифікуються як такі, що загрожують державній безпеці, громадському порядку або суспільній моралі. Це означає, що будь-які дані можна цензурувати, якщо вони будуть визнані небезпечними, відповідно до наведеної характеристики.

Щоб бути успішною, цифрова міжнародна конвенція повинна фокусуватися на технологічних аспектах, встановлювати реальні інструменти для недопущення злочинного втручання в роботу систем. Якщо ж в документі йтиметься про розмиті поняття, які в кожній

країні визначають по-своєму, такий проєкт буде недієвим. Так само, як 90 років тому представники галузі запропонували уряду встановити стандарти використання зв'язку, так і сьогодні ІТ-компанії мають об'єднати зусилля для визначення стандартів цифрової безпеки.

Компанії і раніше співпрацювали, наприклад, під час т.з. процесу добровільного встановлення стандартів, консенсусу. Вперше концепцію застосувала Міжнародна електротехнічна комісія, створена в 1906 році. Це мало вирішальне значення для розвитку інженерії, обчислювальної техніки та комп'ютеризації. Єдині стандарти почали використовувати і приватні організації, такі як Інститут інженерів з електротехніки та електроніки, а пізніше – Консорціум Всесвітньої павутини, заснований самим Тімом Барнерсом-Лі.

Із запропонованих Microsoft пунктів найбільший резонанс для широкого загалу становить Технологічна угода. Довіра до авторів проекту має основне значення, щоб суспільство сприйняло ініціативу серйозно. Нещодавнє дослідження Pew Research виявило, що американці вважають корпоративний ІТ-сектор більш компетентним в питання захисту персональних даних та протистояння іноземним хакерам, аніж державні установи. Отже, міжнародні норми безпеки від компаній матимуть підтримку користувачів, а от ініціатива від правоохоронців чи урядовців – буде провальною.

В Microsoft наголошують, що їх цифрова конвенція досі в процесі розробки. Звернувшись до архівів історії, автори проекту можуть дослідити, які моделі найкраще підходять для регулювання комунікаційних технологій, а які краще не застосовувати, адже в минулому вони виявилися неефективними. Очевидно, що для успіху провідні компанії повинні брати участь в створенні майбутньої Технологічної угоди.

Історія не може передбачати майбутнє, але вона допоможе спрогнозувати, які методи регулювання суспільно-важливих відносин будуть дієвішими. У випадку з встановленням міжнародних правил онлайн-безпеки, Microsoft слід продовжувати агітувати за цей проект та залучати інші компанії. Врешті, маємо шанс отримати справді якісний та ефективний інструмент.

Спираючись на викладені вище засади, навесні 2018 року близько тридцяти компаній, зокрема Microsoft, Facebook та Intel погодили «підставові принципи». Зокрема, підписанти зобов'язалися не допо-

магати жодному уряду, навіть уряду США, проводити атаки проти «безневинного цивільного населення та підприємств з жодної точки світу». Компанії також пообіцяли допомогти будь-якій країні, що стане жертвою таких атак, незалежно від того, чи ведуть їх зі «злочинними, а чи з геополітичними» намірами.

«Справу започатковано, – зазначив Д. Сенгер, – але цього недостатньо, бо жодна китайська, російська або іранська компанія не підписали первинного договору, – зазначає він далі. Так само окремі гіганти технологічного світу, зокрема Google та Amazon усе ще розриваються між бажанням співпрацювати зі Збройними силами США і небажанням обурювати своїх клієнтів. Формулювання угоди залишало простір для маневрів: компанії могли приєднуватися до атак проти терористичних формувань або урядів, що утискують своїх громадян. Не згадувалося також про підтримку демократії або прав людини, а це означає, що якщо Apple з часом приєднається до угоди, то не буде покарана за рішення поступитися Пекіну й зберігати дані про китайських користувачів на серверах, розташованих у Китаї»[1].

Як наголошує Бред Сміт, «потрібно ухвалити закони, які вимагали б поваги до певних принципів у всьому світі. Зокрема, уряди мусять утримуватися від атак на найважливішу інфраструктуру як у мирний час, так і під час бойових дій, і навіть тоді, коли незрозуміло, в якому саме часі ми живемо»[2].

На думку Девіда Сенгера, «… з часом ці принципи зробили світ гуманнішим. … Тепер, як і після винайдення літака та атомної бомби годилося б ширше замислитися над тим, де шукати безпеку.

Ясно, що не в безкінечних перегонах кіберозброєнь, де перемоги над ворогами минущі, а найвища ціль – здолати захист іншої країни або вивести з ладу її підприємства. Слід пам'ятати, що ми створили ці технології, щоб збагатилося наше суспільство й наше життя, а не для того, щоб мати ще один спосіб занурити супротивника в пітьму. Добра новина полягає в тому, що ми створили ці технології, тож можемо і контролювати їх, якщо тільки зосередимося на тому, як впоратися з ризиками. Це спрацювало в інших вимірах, тож може спрацювати і в кіберпросторі», вважає він.[3]

---

1 Сенгер, Девід Е. Досконала зброя. С. 427-428

2 Очевидно йдеться про гібридну війну, але без використання цього терміну

3 Сенгер, Девід Е. Досконала зброя. С. 428

Кібербезпека: проблема національного законодавства

Протилежне «кіберзагрозі», але пов'язане з ним поняття «кібербезпека» визначається як стан захищеності кіберпростору від кібератак, за якого забезпечується його сталий розвиток, а також своєчасне виявлення, запобігання і нейтралізація реальних та потенційних функціонуванню його елементів»[1].

«Кібербезпека» відповідно до положень Закону України «Про основні засади забезпечення кібербезпеки України» є захищеністю життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі.[2]

Оскільки кібервійна є видом інформаційної війни, враховуємо також положення Стратегії інформаційної безпеки, затвердженої Указом Президента України від 28 грудня 2021 року № 685/2021, де інформаційна безпека України розглядається як складова частина національної безпеки України, стан захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації, існує ефективна система захисту і протидії нанесенню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом.[3]

---

1 Попова Т. В., Ліпкан В. А. Стратегічні комунікації. Словник. С. 189.

2 Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 р. *Відомості Верховної Ради.* 2017. № 45. Ст. 403. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

3 Стратегія інформаційної безпеки, затверджена Указом президента України від 28 грудня 2021 року № 685/2021. URL.: https://zakon.rada.gov.ua/laws/show/685/2021#Text

У тому ж документі інформаційна загроза характеризується як потенційно або реально негативні явища, тенденції і чинники інформаційного впливу на людину, суспільство і державу, що застосовуються в інформаційній сфері з метою унеможливлення чи ускладнення реалізації національних інтересів та збереження національних цінностей України і можуть прямо чи опосередковано завдати шкоди інтересам держави, її національній безпеці та обороні. Кіберзагроза у вже згадуваному Законі України «Про основні засади забезпечення кібербезпеки України» визначається як наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об'єктів.

Зауважимо, що ці два поняття мають багато спільного, однак останнє має відчутне публічне забарвлення.

Стратегія національної безпеки України сучасними загрозами для національної безпеки України в інформаційній сфері визначила: 1) стрімкі технологічні зміни та зростання ролі інформаційних технологій у всіх сферах суспільного життя; 2) застосування росією інформаційної «зброї» у поєднанні з енергетичною для зміцнення позицій у Європі, її намагання впливати на внутрішню ситуацію у європейських державах, підживлення триваючих конфліктів, збільшення військової присутності у Східній Європі; 3) продовження російською федерацією гібридної війни проти України шляхом системного застосування інформаційно-психологічних, кібернетичних, політичних, економічних і воєнних засобів для відновлення свого впливу на неї; 4) внутрішню і зовнішню деструктивну пропаганду, що розпалює ворожнечу, провокує конфлікти, підриває суспільну єдність, використовуючи суспільні суперечності в умовах відсутності цілісної інформаційної політики держави, слабкості системи стратегічних комунікацій; 5) недостатню ефективність державних органів, що ускладнює вироблення і реалізацію державою ефективної політики (зокрема в інформаційній сфері), є джерелом загроз незалежності України, її суверенітету і демократії; 6) посилення загроз для критичної інформаційної інфраструктури, пов'язаних із погіршенням її технічного стану, відсутністю інвестицій в її оновлення та розвиток, несанкціонованим втручанням у її

функціонування, зокрема фізичним і кібернетичним, триваючими бойовими діями, а також тимчасовою окупацією частини території України.

Фактичні загрози інформаційній безпеці мають правове значення і у випадках, коли вони не згадані у законодавчих актах.

Експерти поміж головних видів загроз кібербезпеці зазвичай називають:

Фішинг. Наразі атаки соціальної інженерії здійснюються не просто у формі електронних листів, а на настільних комп'ютерах і мобільних пристроях за допомогою голосових дзвінків, текстових повідомлень та соціальних мереж.

Програмне забезпечення-вимагач. Під час атаки програмного забезпечення-вимагача кіберзлочинець встановлює частину зловмисного програмного забезпечення на комп'ютер або сервер, котре шифрує конфіденційну інформацію, яку знаходить. Потім зловмисник вимагає викуп,

Атаки ботнетів. Ботнети використовуються для запуску атак типу «відмова в обслуговуванні» (DoS) або розподілених атак «відмова в обслуговуванні» (DDoS).

Хмарні експлойти. Як і в інших експлойтах, хакери часто мають намір використовувати заражені корпоративні хмарні ресурси для викрадення даних або видобутку криптовалюти.

Атаки, пов'язані з роботою з дому. Оскільки гігієна домашньої безпеки користувачів зазвичай не така ретельна, як на рівні підприємства, це відкриває двері для атак, спрямованих на незахищені мережі Wi-Fi, паролі, які легко зламати, і навіть фізичну крадіжку таких пристроїв, як ноутбуки та смартфони.

Атаки на національну державу. Вважається, що резонансна атака SolarWinds, яка сталася в 2020 році, була ініційована російською розвідкою. Під час атаки кіберзлочинці впровадили бекдори в мережі десятків міжнародних компаній і державних установ, які надали їм постійний доступ протягом майже року, перш ніж їх виявили. Це актуалізувало необхідність стратегій проактивної протидії цим складним операціям кібершпигунства.

Як зазначають Т. Обіход та П. Біленчук, «аналіз кібератак за 2022 рік дає змогу зробити висновок, що найпоширенішим вектором атак залишається крадіжка облікових даних (19%), потім фішинг (16%), не-

правильно налаштована хмара (15%) і вразливості стороннього програмного забезпечення (13%)».[1]

Закон визначає кібератаки як спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту.[2]

Після повномасштабного вторгнення росії в Україну кількість кібератак на державні інформаційні системи та об'єкти критичної інформаційної інфраструктури України зросла втричі. 90% атак здійснюють військові хакери рф та білорусі, діяльність яких фінансується владою. Основна ціль російських хакерів – цивільна інфраструктура. Вони намагаються завдати якомога більше шкоди звичайним людям шляхом як ракетних та інших обстрілів, так і кібератак.[3]

Разом із тим, очікування щодо російських кіберзагроз виявились перебільшеними. Як зазначає Н. Баловсяк, у міру загострення напруженості між Росією та Україною багато людей очікували, що конфлікт буде посилюватись на кіберфронті. Причому про це говорили й закордонні експерти. Департамент внутрішньої безпеки США оприлюднив попередження щодо необхідності бути готовим до російських кібератак, схожі заяви робив також Національний центр кібербезпеки Великобританії. Багато експертів були впевнені в тому, що

[1] Правове і наукове забезпечення кібербезпеки України. П. Біленчук, Т. Обіход, URL: Думка експерта – LexInform: Правові та юридичні новини, юридична практика, коментарі (https://lexinform.com.ua/dumka-eksperta/pravove-i-naukove-zabezpechennya-kiberbezpeky-ukrayiny-chastyna-2/?

[2] Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 р. *Відомості Верховної Ради.* 2017. № 45. Ст. 403. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

[3] Вимоги до захисту інформації в інформаційних системах у воєнний час: роз'яснення Держспецзв'язку | Кабінет Міністрів України (kmu.gov.ua)

Росія підтримає свій військовий наступ руйнівними кібератаками. Тим більше, що протягом останніх декількох років напади на критичну інфраструктуру зачепили багато країн світу і їх можна було розглядати, як певну підготовку до кібервійни під час війни традиційної.

Однак з початку війни не спостерігалося хоча б якоїсь більш-менш серйозної атаки на українські ресурси, що породжує припущення ніби в останні роки Росія лише похвалялась своєю кіберспроможністю, а сама натомість займалась розробкою менш дорогої, менш ефективної кіберзброї, яка завдає меншої шкоди і від якої значно легше захищатись. І «хоча виключати кібератаки з боку Росії у майбутньому не варто, але все менше сумнівів в тому, що наявність у Росії кібернетичного «вундерваффе» є ні чим іншим, аніж витвором пропаганди», – підсумовує Н. Баловсяк.[1]

Хоча кіберзагрози з боку росії можуть з'являтися з різних напрямів (через російське програмне забезпечення,[2] камери вуличного спостереження в містах країн, які вона атакує, тощо), але найбільш зручним для їхнього проникнення каналом є соціальні мережі, популярність яких істотно зросла за роки пандемії. Найпопулярніші соціальні мережі налічують мільйони користувачів. Люди зустрічаються в інтернеті для спілкування, діляться досвідом, емоціями або новинами, розміщують свої фотографії та залишають коментарі. Соціальні мережі розширили можливості людей користуватися правом на свободу вираження поглядів та отримувати і поширювати великий обсяг інформації.[3] Разом із тим, соціальні мережі також значно спростили роботу спецслужб з вербування людей. Якщо раніше співробітники спецслужб змушені були безпосередньо контактувати з тими людьми, які могли б бути корисними, то з появою соціальних мереж вербувальники вивчають людину за профілем у соцмережі: дізнаються про її погляди, цінності, психологічні особливості, місце роботи,

[1] Баловсяк Н. Чи має Росія кібернетичну суперзброю? 22 Березня 2022. Чи має Росія кібернетичну суперзброю? – Український тиждень (tyzhden.ua)

[2] Марія Галелюка. 14 червня, 2024. Чотири міфи про незамінність російського софту. URL: https://biz.nv.ua/ukr/markets/andriy-dligach-ukrajini-neobhidno-zaluchiti-4-5-mln-dodatkovih-pracivnikiv-za-5-rokiv-50427142.html; США заборонили використання програмного забезпечення Kaspersky через загрозу нацбезпеці. Ростислав Вонс. 1 червня 2024. URL: https://glavcom.ua/techno/telecom/ssha-zaboronili-vikoristannja-prohramnoho-zabezpechennja-kaspersky-cherez-zahrozu-natsbezpetsi-1006295.html

[3] Що загрожує персональній інформації та правам користувачів у соціальних мережах: пояснення юриста – Українська Гельсінська спілка з прав людини (helsinki.org.ua)

можливості використання тощо. Визначається інтерес для вербування. Якщо результат позитивний, то далі вивчається психологічний профіль людини. За допомогою комп'ютерних програм можна аналізувати з точки зору психолінгвістики психотип людини. Детальний профіль у соцмережах дозволяє створити реальний психологічний профіль людини, за яким можна підібрати вербувальні підходи до потенційної жертви.[1]

У травні 2017 року указом Президента України було введено в дію рішення РНБО про блокування в Україні доступу до російських соціальних мереж «ВКонтакте», «Одноклассники», ресурсів Yandex, Mail.ru, а також про заборону використання бухгалтерського програмного продукту «1С». Пізніше відповідні списки було розширено, а дію санкцій продовжено.[2]

Після блокування в Україні доступу до російських соціальних мереж ситуація дещо покращилася, але повномасштабне вторгнення загострило її знову.

Наразі досить активно обговорюються питання блокування Телеграм.

Утім політика стосовно заборон чи блокування соціальних мереж виглядає досить непослідовною, у кожному разі, такою, що часто-густо визначається, якщо й не меркантильними, то прагматичними міркуваннями.[3]

Скажімо, перед виборами Президента США Дональд Трамп створив сторінку в соцмережі TikTok, який він намагався заборонити за час своєї президентської каденції. Про створення свого акаунту на платформі він заявив у TikTok, перше відео на акаунті Трампа уже подивилися понад 19 мільйонів осіб, а на його сторінку підписалися

---

1 Артур Гор ВКонтакте заборонили, загрози залишились: як українців обманюють у мережі. URL: https://apostrophe.ua/ua/article/society/2017-06-01/vkontakte-zapretili-ugrozyi-ostalis-kak-ukraintsev-obmanyivayut-i-verbuyut-v-seti/12599

2 https://www.unian.ua/politics/zaboroni-rosiyskih-saytiv-ta-socmerezh-v-ukrajini-rnbo-shvalila-prodovzhennya-blokuvannya-novini-ukrajina-10995161.html

3 Telegram отримав список «проблемних» каналів від української влади – ЗМІ. Ростислав Вонс. 4 березня 2024. URL: https://glavcom.ua/techno/telecom/telegram-otrimav-spisok-problemnikh-kanaliv-vid-ukrajinskoji-vladi-zmi-989165.html; Івженко М. Які гроші обертаються в українському сегменті Telegram і чи можна його заблокувати — розбір NV . 30 квітня 2024. URL: https://biz.nv.ua/ukr/tech/blokuvannya-telegram-yak-pracyuye-biznes-kudi-ydut-groshi-chi-mozhna-blokuvati-chogo-ochikuvati-ukrajini-50414108.html?utm_medium=push&utm_source=gravitec

майже 1 мільйон осіб. За інформацією Politico, рішення приєднатися до TikTok було спробою Трампа достукатися до потенційних виборців напередодні листопадових виборів. У виданні зазначають, що це сталося саме тоді, коли застосунку загрожує потенційна заборона у США, якщо він не вийде з-під контролю свого китайського власника ByteDance.[1]

Можна вважати це специфічною особливістю соцмереж (платформ), котрі як кожна зброя, може бути повернута у будь-який бік.

Після початку повномасштабного російського вторгнення в Україні також значно зросла кількість випадків кібершахрайства. Про це повідомили учасники спільного прес-брифінгу РНБО, НБУ та «Київстар», який пройшов у Нацбанку 15 лютого 2023 року. Найпопулярнішим методом кібершахраїв під час війни став фішинг – збір персональної інформації громадян, у тому числі необхідної для доступу до фінансових акаунтів і облікових записів.[2]

У залежності від джерел їхнього походження доцільно розрізняти публічні та приватні кіберзагрози.

Перші походять від суб'єктів публічних відносин – держав та їхніх фігурантів. Найчастіше мають місце у процесі застосування різних форм кібер /інформаційної війни, операцій спецслужб агресора тощо

Другі мають джерелом протиправну діяльність приватних осіб, якими найчастіше є хакери, пірати, шахраї різного ґатунку, полем діяльності котрих є кіберпростір.

Врахування названих та інших відмінностей має значення при визначені заходів кібербезпеки.

Заходи кібербезпеки

У залежності від виду і джерел походження кіберзагрози для її попередження та ліквідації наслідків державою можуть бути використані різноманітні профілактичні, організаційні та правові засоби, нормативним підґрунтям визначення яких є Доктрина інформаційної

[1] Трамп створив акаунт у TikTok, хоча раніше намагався заборонити цю соцмережу. 2 червня 2024. URL: https://nv.ua/ukr/world/geopolitics/tramp-stvoriv-akaunt-u-tiktok-hocha-ranishe-namagavsya-zaboroniti-cyu-socmerezhu-50423863.html

[2] Бабенко М. Фейки, фішинг, крадіжка грошей із карт: у кібершахрайства в Україні російське коріння. URL: Кіберзлочини під час війни. Що таке і як працює фішинг (focus.ua)

безпеки України, яка була ухвалена у грудні 2016 р. РНБО і введена в дію 25 лютого 2017 р. Указом Президента України. Ї хоча деякі експерти вважають, що Доктрина це лише декларація,[1] однак слід визнати, що вона встановила достатньо чіткі орієнтири діяльності у цій галузі. Доповнив Доктрину Закон України «Про основні засади забезпечення кібербезпеки України», який визначив основні шляхи функціонування національної системи кібербезпеки. Відповідно до його положень, функціонування національної системи кібербезпеки забезпечується шляхом: 1) формування та оперативної адаптації державної політики у сфері кібербезпеки, кіберзахисту з урахуванням наявних або потенційних ризиків, впровадження кращих практик та досягнення сумісності з відповідними стандартами Європейського Союзу та НАТО; 2) запровадження нормативно-правового регулювання у сфері кібербезпеки, кіберзахисту з урахуванням ризик-орієнтованого підходу, чіткого розподілу ролей, завдань, функцій та відповідальності публічного сектору, операторів критичної інфраструктури та власників або розпорядників об'єктів критичної інформаційної інфраструктури, а також галузевої специфіки, гармонізації практик та стандартів з Європейським Союзом та НАТО; *{Пункт 3 частини третьої статті 8 виключено на підставі Закону № 4336-IX від 27.03.2025};* 4) запровадження заходів стимулювання розвитку та конкурентоспроможності індустрії послуг та продуктів у сфері кібербезпеки в Україні; 5) залучення експертного потенціалу приватного сектору, наукових установ, професійних та громадських об'єднань до розроблення проектів щодо стратегічного планування, державної політики, проектів нормативно-правових актів, нормативних документів, стандартів та методичних рекомендацій у сфері кібербезпеки; 6) систематичного проведення навчань з питань кіберзахисту для осіб, які в межах своєї компетенції безпосередньо здійснюють заходи з кіберзахисту в органах державної влади, органах місцевого самоврядування, що є власниками або розпорядниками інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або службова інформація та інформація, що становить державну таємницю, об'єктів критичної інфраструктури, об'єктів критичної інформацій-

[1] Доктрина інформаційної безпеки України – це лише декларація – експерти. URL: https://www.radiosvoboda.org/a/28336852.html

ної інфраструктури; 7) функціонування системи оцінювання стану кіберзахисту в органах державної влади, державних органах, органах місцевого самоврядування, державних підприємствах, господарських товариствах, 50 і більше відсотків акцій (часток) яких належать державі, державних наукових установах та закладах вищої освіти, щодо об'єктів критичної інфраструктури, об'єктів критичної інформаційної інфраструктури; 8) розвитку мережі команд реагування на кіберінциденти, кіберзагрози на національному, галузевому та регіональному рівнях, у тому числі із залученням приватних команд реагування; 9) розвитку та вдосконалення системи технічного і криптографічного захисту інформації; 11) створення та забезпечення функціонування Національної електронної комунікаційної мережі; 12) функціонування національної системи реагування на кіберінциденти, кібератаки, кіберзагрози та національної системи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози; 13) впровадження єдиної (універсальної) системи індикаторів кіберзагроз з урахуванням міжнародних стандартів з питань кібербезпеки та кіберзахисту; 14) підготовки фахівців освітньо-кваліфікаційних рівнів бакалавра і магістра за державним замовленням в обсязі, необхідному для задоволення потреб державного сектору економіки, а також за небюджетні кошти, у тому числі для підвищення кваліфікації та проведення обов'язкової періодичної атестації (переатестації) персоналу, відповідального за забезпечення кібербезпеки об'єктів критичної інфраструктури, з урахуванням міжнародних стандартів; 15) впровадження організаційно-технічної моделі кіберзахисту національної системи кібербезпеки; 16) встановлення вимог (правил, настанов) щодо безпечного використання мережі Інтернет та надання електронних послуг державними органами; 17) застосування інструментів та механізмів державно-приватної взаємодії для виконання завдань у сфері кібербезпеки, включаючи, але не обмежуючись, функціонування національної системи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози, заходи кіберзахисту та захисту інформації; запровадження загальної системи або індивідуальних програм моніторингу, аналізу, координації дій, у тому числі під час реагування на кіберінциденти; усунення наслідків, здійснення заходів з відновлення; організації та здійснення заходів з підготовки кадрів, підвищення рівня знань і навичок, проведення навчань, розроблення та реалізації

освітніх і просвітницьких програм; здійснення досліджень та нових розробок; забезпечення функціонування центрів кібербезпеки та їхніх сервісів; розроблення програмних документів та нормативно-правових актів у сфері кібербезпеки, а також для вирішення інших завдань у сфері кібербезпеки, що можуть бути вирішені шляхом державно-приватної взаємодії; 18) періодичного проведення огляду національної системи кібербезпеки, розроблення індикаторів стану кібербезпеки; 19) стратегічного планування та програмно-цільового забезпечення у сфері розвитку електронних комунікацій, інформаційних технологій, захисту інформації та кіберзахисту; 20) розвитку міжнародного співробітництва у сфері кібербезпеки, підтримки міжнародних ініціатив у сфері кібербезпеки, що відповідають національним інтересам України, поглиблення співпраці України з Європейським Союзом та НАТО з метою посилення спроможності України у сфері кібербезпеки, участі у заходах із зміцнення довіри при використанні кіберпростору, що проводяться під егідою Організації з безпеки і співробітництва в Європі; 21) здійснення оперативно-розшукових, розвідувальних, контррозвідувальних та інших заходів, спрямованих на запобігання, виявлення, припинення та розкриття кримінальних правопорушень проти миру і безпеки людства, які вчиняються з використанням кіберпростору, розслідування, переслідування, оперативного реагування та протидії кіберзлочинності, розвідувально-підривній, терористичній та іншій діяльності у кіберпросторі, що завдає шкоди інтересам України, використанню мережі Інтернет у воєнних цілях; 22) здійснення воєнно-політичних, військово-технічних та інших заходів для розширення можливостей Воєнної організації держави, сектору безпеки і оборони з використанням кіберпростору, створення і розвитку сил, засобів та інструментів можливої відповіді на агресію у кіберпросторі, яка може застосовуватися як засіб стримування воєнних конфліктів та загроз з використанням кіберпростору; 23) обмеження участі у заходах із забезпечення інформаційної безпеки та кібербезпеки будь-яких суб'єктів господарювання, які перебувають під контролем держави, визнаної Верховною Радою України державою-агресором, або держав та осіб, стосовно яких діють спеціальні економічні та інші обмежувальні заходи (санкції), прийняті на національному або міжнародному рівні внаслідок агресії щодо України, а також обмеження використання продукції,

технологій та послуг таких суб'єктів для забезпечення технічного та криптографічного захисту державних інформаційних ресурсів, посилення державного контролю в цій сфері; 24) розвитку системи контррозвідувального забезпечення кібербезпеки, призначеної для запобігання, своєчасного виявлення та протидії зовнішнім і внутрішнім загрозам безпеці України з використанням кіберпростору; усунення умов, що їм сприяють, та причин їх виникнення; 25) проведення розвідувальних заходів із виявлення та протидії загрозам національній безпеці України у кіберпросторі, виявлення інших подій і обставин, що стосуються сфери кібербезпеки; 26) планування витрат та фінансування органами державної влади, державними органами, органами місцевого самоврядування, операторами критичної інфраструктури, власниками або розпорядниками об'єктів критичної інформаційної інфраструктури заходів кіберзахисту, передбачених законодавством; 27) проведення інструктажів та систематичних тренінгів щодо кібергігієни для членів уряду України, народних депутатів України, працівників патронатних служб, депутатів місцевих рад, державних службовців, військовослужбовців, працівників органів державної влади та державних органів, керівників та працівників державних підприємств, установ та організацій, систематичність та порядок проведення яких встановлюються Кабінетом Міністрів України. [1]

Критики стверджують, що для вирішення проблеми кібернетичного захисту населення таких заходів, як блокування небезпечних сайтів, недостатньо. В інформаційну епоху вирішення будь-яких проблем – це не заборони, а навчання та підвищення рівня грамотності населення. Для досягнення цієї мети повинні працювати література, кінематограф, у доступній і популярній формі розповідаючи людям як вірно діяти. При цьому прищеплювати інформаційну гігієну необхідно на етапі початкової школи та навчання у вузі.[2]

Перед тим, як оцінювати слушність такої позиції, маємо спростувати несправедливість закидів щодо неефективності блокування взагалі. Як зазначав В. Горбулін, «При, як декому здається, «смішних»

[1] Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 р. *Відомості Верховної Ради. 2*017. № 45. Ст. 403. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

[2] Гор А. ВКонтакте заборонили, загрози залишились: як українців обманюють у мережі. URL: https://apostrophe.ua/ua/article/society/2017-06-01/vkontakte-zapretili-ugrozyi-ostalis-kak-ukraintsev-obmanyivayut-i-verbuyut-v-seti/12599

контрдіях, ці кроки України приносять цілком відчутні втрати агресорові, змушуючи його збиватися з ритму, відволікатися на чимдалі нові й нові незручності. Заборона соцмереж – прекрасний приклад. Безперечно, при певних технічних навичках заборони можна спробувати обійти (до речі кажучи, механізми обходу часто надаються структурами, близькими до ФСБ). Але важливо, наприклад, зазначити, що відразу після запровадження заборони на роботу «Яндексу» в Україні його акції впали на 3,3%. А це недоплачені податки в російський бюджет, а отже – трохи менше грошей на російський оборонпром або фінансування сепаратистів. Не кажучи вже про різке скорочення цільової аудиторії для латентного «промивання мізків».[1]

Що стосується інформаційної гігієни взагалі, то, визнаючи її важливість та слушність критики недостатньо активної діяльності держави у цій галузі, слід зауважити, що помилкою були б надмірні сподівання на ефективність виховної та просвітницької діяльності. По-перше, тому, що йдеться про тривалий процес виховання, результати якого стануть помітними, у кращому разі, за кілька років, тоді як ситуація, що наразі склалася у галузі інформаційної безпеки, потребує швидкого поліпшення. По-друге, тому, що наївними виглядають сподівання на достатність підвищення рівня «інформаційно-безпекової грамотності» населення, починаючи з «початкової школи та навчання у вузі» на тому тлі, що в інформаційному суспільстві види і характер кіберзагроз стрімко змінюються. Втім, як докорінно має змінитися, на думку експертів у сфері ІТ, і сам характер освіти майбутнього.[2] Те, чому навчать у «початковій школі», навряд, чи буде актуальним для вирішення проблеми асекурації кібербезпеки на момент її закінчення (крім випадків, коли йдеться про загальні засади співжиття у суспільстві, дотримання загальних правил безпеки взагалі та інформаційної безпеки, зокрема).

Враховуючи зазначене, «інформаційну гігієну» можна визнати чинником формування правосвідомості, умовою ефективності застосування правових засобів, поміж яких важливе місце займають засоби публічно-правового впливу, котрі активно використовують, навіть, європейські демократичні держави.

[1] Горбуліін В. «Цінності суспільства» і «гібридний мир»: криза моделі захисту. *Деркало тижня.* 2017. Вип. 24.

[2] Усе рухне у відносно короткий проміжок часу. Інтерв'ю з ІТ-експертом Ігорем Новіковим. Країна. 2017. 15 червня. С. 20.

Оцінюючи з таких позицій ситуацію у цій галузі, зазначимо, що вирішення проблеми кіберзагроз потребує врахування двох аспектів: законодавчого та правозастосовчого.

Що стосується першого з них, то тут вже є Закони України «Про захист інформації в інформаційно-комунікаційних системах»[1], «Про основні засади забезпечення кібербезпеки України». Крім того, експерти з кібербезпеки, відзначаючи певний прогрес ставлення до кібербезпеки з боку держави (вироблена стратегія кібербезпеки, при РНБО існує координаційний центр тощо, говорять про необхідність прийняття закону про відповідальність хакерів, котрі зараз почуваються безпечно.

Повномасштабна війна в Україні, порушення всіх норм міжнародного права призвели до того, що міжнародні норми просто перестали діяти. Як приклад, Міжнародний комітет Червоного Хреста (МКЧХ) вперше опублікував правила для цивільних хакерів, які беруть участь у конфліктах. Наглядовий орган попереджає, що після вторгнення Росії в Україну до патріотичних кіберугруповань приєднується безпрецедентна кількість людей. Нові правила включають заборону на атаки на лікарні, неконтрольоване поширення хакерських інструментів і загрози, які тероризують цивільне населення. ІТ-армія України, яка в телеграмі налічує 160 000 учасників, також атакує державні служби, такі як залізниці та банки.

Її представник сказав BBC News, що вони ще не вирішили, чи застосовувати правила МКЧХ. Група вже заборонила атаки на медичні цілі – але вплив на цивільне населення є неминучим, бо «дотримання правил може поставити одну сторону в невигідне становище».

Тим часом представник групи Anonymous Sudan, яка останніми місяцями почала атакувати технологічні компанії та державні служби, які, на їхню думку, критикують Судан чи іслам, сказав BBC News, що нові правила «нежиттєздатні і що їх порушення заради інтересів групи неминуче».

А один із високопосадових членів групи Anonymous розповів BBC News, що вони «завжди працювали на базі кількох принципів, зокрема правил, озвучених МКЧХ», але тепер втратили віру в цю організацію і не будуть дотримуватись її нових правил.[2]

---

[1] Про захист інформації в інф... | від 05.07.1994 № 80/94-ВР (rada.gov.ua)

[2] Джо Тайді У світі вперше запровадили правила для хакерів: чи будуть виконувати їх українці під час війни? – BBC News Україна

У ситуації, що склалася, як зазначив Єгор Аушев – CEO CyberUnit Technologies, – Україна має стати центром спротиву, оскільки отримала під час війни величезний досвід і має використовувати його не тільки для підвищення своєї кіберстійкості, але й для побудови відомої у світі експертизи.

З початку війни наша держава зазнала численних кібератак, які спрямовані на суб'єкти інфраструктури різних типів власності – державні, корпоративні, приватні тощо. За 2023 рік CERT-UA опрацювала 2543 кіберінциденти – це на 15,9% більше ніж за 2022 рік, коли вторгнення рф в Україну супроводжувалось величезною кількістю атак. Найбільше ворожі хакери атакували уряд та урядові організації, місцеві органи влади та сектор безпеки та оборони. Численні кібератаки на фінансові установи, критичну інфраструктуру, енергетичний сектор, телекомунікації стали нормою та продовжують завдавати шкоди державі та приватному бізнесу.

До прикладу, згадаємо масовану атаку на Київстар, яка загрожувала не лише телекомунікаційним системам України, але й вказала на новий рівень кіберагресії рф. Якби атака повною мірою досягла своїх цілей у руйнуванні критичної інфраструктури, то понад сто тисяч об'єктів в Україні могли б зазнати значних, а інколи критичних, наслідків.

Україна визнає загрози кібербезпеки як важливий аспект національної безпеки. Запровадження ефективних механізмів захисту від кібератак, підвищення кіберсвідомості людей та ефективна координація усіх суб'єктів кібербезпеки є пріоритетами.

На думку Аушев,а потрібен не тільки захист на локальному рівні, а й на глобальному, де потрібно створювати глобальні спільні групи реагування на міждержавному рівні, оскільки протистояння в кіберпросторі тепер виходить за рамки національних кордонів, особливо в умовах війн та конфліктів у різних куточках світу. Країни, що володіють розвинутими кібервійськовими програмами, такі як росія, Північна Корея та Іран, можуть фінансувати та використовувати хакерські угруповання як інструмент впливу на свої стратегічні цілі, а також крадіжки коштів та персональних даних, шантажу тощо.

У цьому контексті світового протистояння Україна має всі шанси стати центром спротиву, який об'єднає західні країни в кіберкоаліцію задля протистояння загрозам у кіберпросторі, шляхом розробки

спільних ефективних інструментів кіберстримування та зміною політики кіберзахисту світу. І єдине, що для цього потрібно, це усвідомлення важливості всіма учасниками процесу та об'єднання навколо його драйверів, якими сьогодні є представники української професійної спільноти, держава та бізнес.[1]

Висновки

Реалізація завдань усунення кіберзагроз, на наш погляд, можлива двома шляхами:

Перший – це домовленості між активними суб'єктами кіберпростору, як це передбачає проєкт цифрової Женевської конвенції.[2] Але головною проблемою тут є необмежена добровільність дотримання державами і компаніями, які не приєдналися. Тому здається доцільним другий шлях: використання жорстких заходів державами, які протистоять агресії, зокрема тих, заходів, що їх застосовує Україна, з обґрунтуванням виправданості застосування блокування, використання цільових програм, антихакерських об'єднань протягом війни і у оборонних цілях.

Оскільки досягнення кібербезпеки припускає застосування певних обмежень та заходів державного примусу, неминуче виникає колізія використання згаданих заходів здійснення та права на інформацію, яка має транскордонний характер.

При вирішенні цієї колізії, на наш погляд, слід виходити з необхідності поєднання реалізації права на інформацію із врахуванням вимог кібербезпеки.

Пам'ятаючи, що право на інформацію проголошене Конституцією України і набуло практичного наповнення у Законі про інформацію, разом із тим, враховуємо, що ст. 2 цього Закону встановлює основні принципи інформаційних відносин: гарантованість права на інформацію; відкритість, доступність інформації, свобода обміну інформацією; достовірність і повнота інформації; свобода вираження

[1] Україна має стати центром спротиву: Як використати унікальність нашого досвіду з подолання кібератак. 16 березня 2024. URL: https://biz.nv.ua/ukr/experts/novi-kiberataki-vid-rf-yak-reaguvati-ukrajini-ta-do-chogo-nam-vsim-gotuvatisya-50401148.html

[2] Прогнімак К. Microsoft права: нам потрібна цифрова Женевська конвенція. 13 травня 2017. URL: https://www.imena.ua/blog/microsoft-digital-geneva-convention/

поглядів і переконань; правомірність одержання, використання, поширення, зберігання та захисту інформації, ст. 3 – передбачає певні зобов'язання держави у цій галузі, а ст. 7 – передбачає низку гарантій такого права..[1]

Разом із тим, до основних напрямків державної інформаційної політики Закон про інформацію відносить забезпечення інформаційної безпеки України, а вимогою до реалізації права на інформацію є те, що вона не повинна порушувати громадські, політичні, економічні, соціальні, духовні, екологічні та інші права, свободи і законні інтереси інших громадян, права та інтереси юридичних осіб.

Із врахуванням цих вимог право на інформацію може бути обмежене законом в інтересах національної безпеки, територіальної цілісності або громадського порядку, з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя.

Крім того, неприпустимим є зловживання правом на інформацію (ст. 28 Закону про інформацію). Ця заборона має практичним результатом те, що інформація не може бути використана для закликів до повалення конституційного ладу, порушення територіальної цілісності України, пропаганди війни, насильства, жорстокості, розпалювання міжетнічної, расової, релігійної ворожнечі, вчинення терористичних актів, посягання на права і свободи людини. Недотримання цієї вимоги має наслідком відмову у захисті права на інформацію, а у випадках, передбачених законом, тягне настання юридичної відповідальності.

Обмеження публічної інформації має місце під час війни. Тут важливо не допустити маніпуляцій стосовно того, яка інформація може бути обмежена. Є інформація, вільний обіг якої є важливим для демократичної держави. Вважається, що в усіх випадках і незалежно від обставин суспільний інтерес в поширенні такої інформації буде переважати шкоду від її оприлюднення. Відкритість цієї інформації прямо передбачається законом України «Про доступ до публічної ін-

[1] Роз'яснення Міністерства України від 3 травня 2012 р. «Право на доступ до інформації як елемент правового статусу особи». URL:ttp://zakon2.rada.gov.ua/laws/show/n0012323-12

формації» (Закон № 2939-VI).[1] Перелік безумовно відкритої інформації закріплений у Законі України «Про інформацію».[2] Понад десять галузевих законів забороняють обмежувати доступ до окремих категорій інформації.

Зауважимо також, що обмеження права на інформацію з міркувань інформаційної безпеки є досить поширеним явищем, котре відповідає загальним засадам реалізації прав особи і не порушує права людини. Не суперечить таке тлумачення і позиціям з відповідної категорії справ Європейського Суду з прав людини.[3]

Активне і досить ефективне використання кібератак у гібридних війнах ставить під сумнів спроможність ідеї самовпорядкування ІТ-сфери на сучасному етапі її розвитку. Можливо, це стане реальністю після того як штучний інтелект стане дужчим інтелекту людського і сформує свій ідеальний віртуальний світ.

Наразі загрози інформаційній безпеці не подолати лише за допомогою технічних засобів, оскільки останні можуть впливати лише на технічну складову ІТ-сфери, залишаючи поза увагою «соціальний елемент» яким є учасники відносин, що виникають у ІТ-сфері (у тому числі, програмісти, провайдери, користувачі тощо). Це не можна визнати виправданим, оскільки на даному етапі розвитку ІТ саме соціальний елемент є головним чинником порушення інформаційної безпеки. У пошуках впливу на цю складову ІТ-сфери маємо удосконалювати засоби впливу на людський чинник як джерело загроз інформаційній безпеці.

Ключові слова: інформаційні технології, інформаційна війна, право на інформацію, інформаційна безпека, колізія інтересів, кіберпростір, кібервійна, кіберзагрози, протидія кіберзагрозам, хакери, соціальні мережі, блокування.

[1] Закон України «Про доступ до публічної інформації». *Відомості Верховної Ради України.* 2011. № 32. Ст. 314.

[2] Закон України «Про інформацію». *Відомості Верховної Ради України.* 1992. № 48. Ст. 650. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text

[3] http://cedem.org.ua/analytics/pravo-na-dostup-do-informatsiyi-evolyutsiya-pidhodiv-yevropejskogo-sudu-z-prav-lyudyny/

Розділ 12

ЕТИКО-ЮРИДИЧНІ АСПЕКТИ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В МЕРЕЖІ ІНТЕРНЕТ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

DOI

Олександр Омельчук
кандидат юридичних наук, доцент

Формування інформаційного суспільства в Україні напряму пов'язане з розвитком та широким впровадженням цифрових технологій. Тотальна діджиталізація суспільного та особистого життя на даний момент об'єктивується як елемент чинної реальності, а отже актуалізуються для вивчення питання правового регулювання сучасної сфери інформаційних відносин та захисту прав та інтересів (як приватних, так і суспільних) в даній сфері.

На сьогодні перспективи використання ШІ викликають інтерес не лише в експериментальних та прикладних технічних галузях, соціальній та економічній сфері. Людство працює над удосконаленням технологій та вирішенням філософських питань стосовно ШІ, держави та міжнародні організації мізкують над іншими проблемними питаннями – про встановлення юридичної природи ШІ так про результати його діяльності, а також про те, чи може він бути застосованим у правових та організаційних аспектах використання нематеріальних активів.

Як слушно відмічає О. С. Котуха, неконтрольоване та беззастережне втручання у «цифровий світ», а також в життя людей за його допомогою може спричинити серйозні порушення прав і свобод людини та громадянина, порушення особистих кордонів, руйнування звичних підвалин життя населення, втрату звичаїв тощо.[1]

[1] Котуха О. С., Попов Д. І. Штучний інтелект та права людини: проблеми цифровізації права на сучасному етапі розвитку електронної держави. *Вісник Львівського торговельно-економічного університету.* 2024. № 15. С. 22.

Вітчизняні дослідники проблем правового регулювання штучного інтелекту також вказують на проблему ризиків дезінформації, зумовлених поширенням ШІ (приклади останньої можуть з'являтися у текстах, згенерованих за допомогою ШІ), а, поряд з цим, і на проблему потенційного збільшення кількості випадків порушення авторського права.[1]

На сьогоднішній день ШІ вже може обробляти велику кількість даних та навчатися, щоб вирішувати задачі, генерувати текст, фото, відео, аудіо, код, інформацію та її сукупність. ШІ вже зараз здатний аналізувати дані, змішувати їх і генерувати на їхній основі новий та неповторний результат.[2]

За прогнозами експертів найближчим часом ШІ перейде від узагальнених продуктів до рішень, орієнтованих на розв'язання конкретних завдань. Окрім того, ШІ проникатиме в різні сфери життя й бізнесу – від зміни клімату до охорони здоров'я. [3] Більшість людей не усвідомлюють, що вже зараз використовують технології штучного інтелекту у щоденному житті, в освіті та медицині, комунікаціях та соціальній сфері, економіці та юридичній сфері.[4]

О. Косілова та Х. Солодовнікова, аналізуючи наявні застереження щодо використання ШІ, приходять до висновку, що людство не просто на порозі відкриття «надрозуму», а й може просто вже опинитися перед обличчям загрози, яка полягає в жорсткій конкуренції між людиною та штучним інтелектом, і останній стрімко завойовує усі сфери буття людини, що, на думку вченого, є серйозною загрозою основоположним правам людини. Саме тому обумовлюється необхідність відповідного всебічного захисту людини, в тому числі й юридично-правового.[5]

---

[1] Пертів О. Штучний інтелект та авторське право. Центр демократії та верховенства права. 2023. URL: https://cedem.org.ua/analytics/shtuchnyi-intelekt-avtorske-pravo/

[2] Спесивцева О. Право sui generis: як штучний інтелект адаптує під себе авторське право? *Юридична газета.* 2024. URL: https://yur-gazeta.com/publications/practice/informaciyne-pravo-telekomunikaciyi/pravo-sui-generis-yak-shtuchniy-intelekt-adaptue-pid-sebe-avtorske-pravo.html

[3] Баловсяк Н. Прикладний штучний інтелект і заборона соцмереж для дітей. Чого чекати від 2025-го технологічного. *Український тиждень.* 2024. URL: https://tyzhden.ua/prykladnyj-shtuchnyj-intelekt-i-zaborona-sotsmerezh-dlia-ditej-choho-chekaty-vid-2025-ho-tekhnolohichnoho/

[4] Живцова Л. І. Штучний інтелект: сутність та перспективи розвитку. *Український журнал будівництва та архітектури.* 2023. № 3. С. 67-71.

[5] Косілова О. І., Солодовнікова Х. К. Права і свободи людини і громадянина V. S. Штучний інтелект: проблемні аспекти. *Інформація і право.* 2020. № 4(35). URL: http://bulletin.kpi.ua/index.php/2616-6798/article/view/221218

Для ефективного досягнення результатів даного дослідження важливим є формування коректного розуміння понять нейромережа та штучний інтелект, а також визначення природи «використання» останніх в мережі Інтернет.

Сучасна концепція штучного інтелекту (ШІ) – це сукупність наукових дисциплін і методів, призначених для обробки даних та вирішення складних обчислювальних завдань.[1]

О. А Баранов відзначає, що відсутність консенсусної дефініції терміну «штучний інтелект» хвилює практично всіх представників філософських, гуманітарних, технічних та інших наук. В той же час для представників правової науки ця проблема набуває особливо гострих форм, тому що даний термін не є спеціально-юридичним, має універсальний характер та має бути однаково зрозумілим для представників будь-яких політичних, наукових та бізнесових кіл, верств населення, сфер соціального життя тощо.[2]

В сучасному цивільному законодавстві неодноразово згадується штучний інтелект. В той же час, термін «штучний інтелект» є досить новим для українського законодавства, що створює проблеми з чітким правовим визначенням та регулюванням цього поняття.

Відповідно до Концепції розвитку штучного інтелекту в Україні, Окрім цього затвердженої Кабінетом Міністрів України розпорядженням № 1556-р від 02 грудня 2020 р. штучний інтелект – це організована сукупність інформаційних технологій, із застосуванням якої можливо виконувати складні комплексні завдання шляхом використання системи наукових методів досліджень і алгоритмів обробки інформації, отриманої або самостійно створеної під час роботи, а також створювати та використовувати власні бази знань, моделі прийняття рішень, алгоритми роботи з інформацією та визначати способи досягнення поставлених завдань.[3]

---

[1] Фоміна Н. Чи можуть твори, створені за допомогою ШІ, розраховувати на авторське право. *Юридична газета.* 2023. № 11–12 (769–770). URL: https://yur-gazeta.com/publications/practice/zahist-intelektualnoyi-vlasnosti-avtorske-pravo/chi-mozhut-tvori-stvoreni-za-dopomogoyu-shi-rozrahovuvati-na-avtorske-pravo.html

[2] Баранов О. А. Визначення терміну «штучний інтелект». *Інформація і право.* 2023. № 1(44). С. 33.

[3] Про схвалення Концепції розвитку штучного інтелекту в Україні: Розпорядження Кабінету Міністрів України; Концепція від 02.12.2020 № 1556-р. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text

Штучний інтелект представляє собою технологію, що дозволяє комп'ютерним системам виконувати завдання, які зазвичай потребують людського інтелекту, такі як розпізнавання мови, розуміння текстів, аналіз даних та прийняття рішень. Штучний інтелект широко застосовується у всіх галузях, включаючи літературу, мистецтво та інші творчі напрямки. Він є передовою галуззю розвитку технологій і має значний вплив на різні аспекти життя.[1]

В юридичній науці штучний інтелект визначають як певну сукупність методів, способів, засобів та технологій, насамперед, комп'ютерних, що імітує (моделює) когнітивні функції, які мають критерії, характеристики та показники еквівалентні критеріям, характеристикам та показникам відповідних когнітивних функцій людини. Згадування у дефініції комп'ютерних технологій не впливає на основний сенс розуміння штучного інтелекту та не обмежує можливість його застосування в рамках інших фундаментальних підходів до побудови штучного інтелекту.[2]

Нейронна мережа, також штучна нейронна мережа, або ШНМ – це один із напрямків у створенні штучного інтелекту, який ставить своїм завданням відтворити аналітичну роботу людського мозку. Математична модель ШНМ бере свої витоки з біології, а в її основі лежить принцип роботи нервової системи живих організмів, де мільярди нейронів з'єднані синапсами, приймають вхідні дані у вигляді електричних імпульсів, обробляють і передають іншим нейронам.[3]

Нейромережа за допомогою штучних нейронів може визначати закономірності, збирати та аналізувати інформацію, розпізнавати звуки, символи та зображення, вчитися на власному досвіді.

Одним зі способів утілення прикладного ШІ в найближчому майбутньому має стати агентний штучний інтелект, під яким розуміється автономні системи ШІ, здатні самостійно планувати й виконувати завдання для досягнення поставлених цілей. Вони можуть діяти незалежно, ухвалюючи рішення без постійного втручання людини з

[1] Вальчук Д. В. Авторське право штучного інтелекту: проблеми та шляхи вирішення. *Modern scientific journal.* 2024. № 3 (1). С. 8-9.

[2] Баранов О. А. Визначення терміну «штучний інтелект». *Інформація і право.* 2023. № 1(44). С. 46.

[3] Ладуба М. Нейромережі пишуть книги та рятують життя: що таке нейронна мережа і як вона працює. URL: https://mc.today/uk/shho-take-nejronna-merezha/

метою спростити й автоматизувати різноманітні процеси – від відповідей на електронні листи до оцінювання студентських робіт та опрацювання замовлень інтернет-магазинів.[1]

Одним з найбільш поширених і зрозумілих на сьогоднішній день видів ШІ, що на сьогоднішній день використовуються в мережі Інтернет є генеративний штучний інтелект. Генеративний ШІ – це інноваційний напрямок штучного інтелекту, що дозволяє створювати унікальний контент: тексти, зображення та аудіо. Він відрізняється від традиційного ШІ тим, що не просто аналізує або класифікує дані, а генерує новий унікальний контент.[2]

«Творчість» штучного інтелекту вже сьогодні широко використовується та непогано монетизується. Однак, слід однак зазначити, що авторські права на творчість алгоритмів – поки сіра зона світу юриспруденції.[3] Т. Харебава виділяє три підходи до визначення, хто може бути автором створеного за допомогою ШІ об'єкта:

- розробник штучного інтелекту: у цьому випадку авторство може належати особі або групі людей, які розробили алгоритми та програми штучного інтелекту, що використовуються для створення творів;
- користувач штучного інтелекту: іноді особа, яка використовує штучний інтелект, може бути визнана автором твору, який був згенерований ШІ, особливо якщо вона надала важливі вхідні дані, параметри або інструкції для генерації твору;
- безпосередньо штучний інтелект (концепція «електронної особи»): у деяких контекстах розглядається можливість визнання штучного інтелекту як автора твору, якщо він має достатньо високий рівень самостійності і творчості у генерації контенту.[4]

---

[1] Баловсяк Н. Прикладний штучний інтелект і заборона соцмереж для дітей. Чого чекати від 2025-го технологічного. *Український тиждень.* 2024. URL: https://tyzhden.ua/prykladnyj-shtuchnyj-intelekt-i-zaborona-sotsmerezh-dlia-ditej-choho-chekaty-vid-2025-ho-tekhnolohichnoho/

[2] Що таке генеративний штучний інтелект і де він застосовується? URL: https://blog.colobridge.net/uk/2023/11/generative-artificial-intelligence-ua/

[3] Дудко В. Як палає Кремль. Нейромережі генерують картини з тексту і допомагають збирати на ЗСУ. Чи може нейроарт стати бізнесом. *Forbes Digital.* 2022. URL: https://forbes.ua/inside/yak-palae-kreml-neyromerezhi-generuyut-kartini-z-tekstu-i-dopomagayut-zbirati-na-zsu-chi-mozhe-neyroart-stati-biznesom-23082022-7861

[4] Харебава Т. Авторські права на об'єкт, створений штучним інтелектом. *Юрліга.* 2024. URL: https://jurliga.ligazakon.net/analitycs/225383_avtorsk-prava-na-obkt-stvoreniy-shtuchnim-ntelektom

Два роки тому набрав чинності Закон України «Про авторське право і суміжні права». Згідно положень даного закону результат роботи штучного інтелекту підпадає під правове регулювання як неоригінальний об'єкт, згенерований комп'ютерною програмою, що охороняється правом особливого роду (sui generis). Однак, як відмічають дослідники, питання авторських та суміжних прав, пов'язаних з штучним інтелектом, є складними і потребують уточнення у законодавстві. На сьогоднішній день в більшості країн законодавці продовжують вивчати цю проблему і шукати оптимальні рішення, які враховували б потреби розвитку технологій та гарантували захист прав власників інтелектуальної власності.[1]

Питання застосування ШІ на сьогоднішній момент стикається з необхідністю визначення ряду факторів, що обґрунтовують етичність такого застосування.

Ю. Гайдай визначає наступні ризики етичного характеру щодо використання ШІ в мережі Інтернет:

– ризики для особистих даних і приватності. Мовні моделі, по-перше, можуть робити дуже багато узагальнень, поєднань інформації і висновків з отриманих даних, які можуть бути недоступними для людини, що аналізує інформацію. Наприклад, з наборів даних про поведінку людини у соцмережах та інтернеті загалом, тих же запитів до чатботів великих мовних моделей, можна робити глибокі висновки щодо її психічного стану, звичок, розкладу дня тощо. Поєднання великих масивів даних та їх аналіз ШІ створюють додаткові загрози приватності, які не очевидні для користувачів, бо окремо ці дані не створюють загроз.
– ризики сегрегації – мовні моделі, за рахунок того, як саме і на основі яких даних навчаються, можуть надавати перевагу окремим соціальним групам. Вони будуть краще працювати з цими групами, а іншим приділяти менше уваги і маргіналізувати їх, вилучати певні меншини (етнічні або інші) та відтворювати людські упередження щодо цих меншин;
– ризики неточності і неправдивості інформації – мовні моделі не дуже добре відрізняють факти від вигадок, але при цьому ство-

[1] Вальчук Д. В. Авторське право штучного інтелекту: проблеми та шляхи вирішення. *Modern scientific journal.* 2024. № 3 (1). С. 14.

рюють враження, що вони є достовірними співрозмовниками, що може створювати багато загроз;
- безпекові ризики – мовні моделі дуже зручно використовувати для масової дезінформації, причому персоналізованої дезінформації «з людським обличчям», заточеної під конкретні групи людей, наприклад, шляхом коментування у соцмережах та у медіа;
- загроза правам людини через використання штучного інтелекту державними органами – передбачається насамперед здатність опрацьовувати величезні масиви даних, роблячи узагальнення і висновки щодо окремих людей. Це можливості розпізнавання, а отже, відстежування людей як фізично, так і деанонімізація їхньої онлайн-поведінки. Це дає державним органам потужні інструменти втручання у приватність, а безконтрольне застосування ШІ може призвести до ухвалення неправомірних чи хибних рішень стосовно громадян – застосування санкцій, відмови у доступі до послуг, кредиту, працевлаштування тощо.[1]

Для певної структуризації та побудови логіки дослідження слід визначити сфери, в яких консолідується використання штучного інтелекту в Інтернеті. Окреслення останніх дасть змогу визначити основні джерела потенційних загроз штучного інтелекту, в тому числі потенціал використання штучного інтелекту для цілей ведення гібридної війни.

Серед основних функцій мережі Інтернет зазвичай називають інформативну. Оперативність та розмаїття інформації, наявної в мережі залишається значною перевагою використання Інтернету для задоволення інформаційних потреб.

Серед вкрай важливих в умовах воєнного стану видів інформації слід окремо виділити новини в мережі Інтернет, наявність яких дає змогу реалізувати поточну потребу в доступі до даних щодо подій в Україні та світі. Дослідники природи ЗМІ підтримують позицію, що засоби масової інформаціє залишаються засобом формування громадської думки,[2] адже ще з часів появи газет, а згодом телебачен-

[1] Гайдай Ю. Тренди ШІ: які етичні загрози несе використання штучного інтелекту. URL: https://speka.media/trendi-si-yaki-eticni-zagrozi-nese-vikoristannya-stucnogo-intelektu-v4q3wp?utm_source=google&utm_medium=cpc&utm_campaign=20972733776&gad_source=1

[2] Мороз Н. О. Роль засобів масової інформації у формуванні громадянського суспільства в Україні. *Гуманітарний журнал.* 2012. № 2-3. С. 206.

ня, методи, способи і форма подачі новин визначалися відповідно до мети публікації такої новини.

Широке використання сучасних технологій в новинній сфері пов'язане з необхідністю якнайшвидшої трансляції новини на широку аудиторію в умовах конкуренції ЗМІ, запитом аудиторії новин на фільтрацію новин, потребою в забезпеченні доступу до новин за будь-яких обставин та з будь-якого пристрою. Залучення функціоналу нейромереж та штучного інтелекту в сфері створення та розповсюдження новинного контенту здійснюється за наступними напрямками:

– використання ШІ для збору, обробки, перекладу, фільтрування, групування, перевірки, ранжування новинного контенту;
– використання ШІ для аудіовізуального оформлення новинного контенту;
– використання ШІ для генерування фейкових новин.

Слід відзначити, що не лише зміст та інтерпретація інформації про подію, що формують новину, впливають на сприйняття адресатом даної новини. Потенційну реакцію споживача новинного контенту визначають також форма подачі матеріалу, контекст, оформлення тощо. Крім того певний новинний контент не може сприйматися відокремлено від супутніх новин, а отже при формуванні думки в споживача новинного контенту мають значення як розподіл та ранжування новин, так і новини, що подаються поряд (на фоні яких сприймається новина).

Як відзначають дослідники проблематики використання штучного інтелекту в журналістиці, попри значні перспективи та переваги широкого залучення штучного інтелекту при відборі новинного контенту, невирішеними залишаються питання дотримання прав інтелектуальної власності авторів новинного контенту.[1] Крім того, безконтрольне використання штучного інтелекту при генеруванні новинного контенту може призвести до значних етичних колізій, адже не будь-який контент слід поширювати з етичних міркувань, а методи збору інформації повинні виходити з принципів (та сама журналістська етика).

[1] Горон Д. Епоха штучного інтелекту: як журналістиці пристосуватися до змін. *Детектор медіа.* 2025. URL: https://detector.media/infospace/article/237260/2025-01-20-epokha-shtuchnogo-intelektu-yak-zhurnalistytsi-prystosuvatysya-do-zmin/

Шкідливий вплив використання ШІ та нейромереж в сфері генерації новинного контенту чинить також свідоме використання даного контенту в воєнних або політичних цілях. Саме в цьому контексті доречно звернутися до широко вживаного в останній час поняття ІПСО (інформаційно-психологічні спецоперації).

Під ІПСО розуміється комплекс заходів з поширення спеціально підготовленої інформації для впливу на емоції, почуття, поведінку людей. До елементів ІПСО зазвичай відносять дезінформацію, пропаганду, кібератаки, перебільшення певної інформації або применшення іншої.[1]

Як зазначає І. Колеснікова, в умовах гібридної війни актуалізується проблема протидії пропаганді та дезінформації. Дослідниця відмічає значне поширення інформації, що спрямована на глорифікацію військового вторгнення РФ на територію України та його учасників, дискредитацію керівництва України, ЗСУ та правоохоронних органів, посилення фрустраційних настроїв або розпалювання ворожнечі серед населення за етнічними, релігійними та іншими ознаками. На думку науковиці, «особлива небезпека російської пропаганди та дезінформації обумовлена тим, що значна частина її здійснюється в мережі Інтернет у відкритих джерелах, зокрема, у тих, в яких відсутня цензура. Реалізація злочинного наміру пропагандистів несе у собі велику загрозу, оскільки Інтернет має низку переваг, які зловмисники використовують у злочинних цілях. Серед них такі як широке охоплення аудиторії, можливість анонімного розміщення інформації, вільний доступ та висока швидкість поширення у географічній площині. Тому російська пропаганда, яка розповсюджується в мережі Інтернет представляє масштабну загрозу для національної безпеки країни, несвоєчасне вирішення якої може призвести до руйнівних наслідків, як у межах України, так і для всього цивілізованого світу».[2]

---

[1] Бартельова А., Рудь О. Інформаційно-психологічні операції як основна загроза інформаційній безпеці держави. *Протидія дезінформації в умовах російської агресії проти України: виклики і перспективи*: Матеріали конференції. 2023. URL: https://www.researchgate.net/publication/376773925_Informacijno-psihologicni_operacii_ak_osnovna_zagroza_informacijnij_bezpeci_derzavi

[2] Колеснікова І. А. Проблеми протидії пропаганді та дезінформаці у відкритих джерелах інформаційно-телекомунікаційної мережі інтернет. *Актуальні проблеми протидії злочинності та корупції*: збірник тез Всеукраїнської науково-практичної конференції (Харків, 17 лютого 2023 р.). С. 88.

На сьогоднішній день генерування фейкових новин з метою викликати у адресата хибну впевненість у події, що не відбулася, є складовою інформаційної війни проти України. Так, свого часу російська держава створила цілу систему інформаційно-психологічного забезпечення як складову системи своєї національної безпеки.[1]

Значний доробок використання ШІ припадає на соціальні мережі. Так, соціальні мережі, з одного боку, є платформою для вільного обміну інформацією та думками, проте, з іншого боку, вони можуть стати засобом поширення ненависті, дискримінації та маніпуляції.[2]

Лідером із поширення фейків у соціальних мережах є Facebook. У Facebook найрозгалуженіша інструментальна мережа, що працює в двох напрямках: для збору даних і зміни поведінки людей – впливу чи нав'язування.[3]

Наявні діджитал-інструменти дозволяють за допомогою ШІ розрізняти органічне та скоординоване розповсюдження контенту, виявляти автоматизовані системи розповсюдження спаму, оцінювати вплив на аудиторію різних облікових записів користувачів соцмереж, відрізняти ботів від реальних користувачів тощо.[4]

В умовах гібридної війни штучний інтелект широко застосовується для ідентифікації та розпізнавання мертвих солдатів противника та знищеної техніки за допомогою аналізу соціальних мереж та аналогічних матервалів в новинному сегменті мережі Інтернет.

Так, в умовах повномасштабної війни технології компанії Clearview AI використовуються для встановлення осіб російських солдатів, навіть на фото низької якості та навіть фото мертвих солдатів з поля бою.

Так за допомогою відповідного програмного забезпечення стало можливим точне розпізнавання як живих, так і мертвих противників з можливістю виявлення ім'я солдата, рідного міста та профілів у соціальних мережах.

---

[1] Дмитренко М. А. Інформаційно-психологічні операції в контексті інформаційної безпеки України. *Інформація і право.* 2025. № 1(52). С. 116.

[2] Хоменко Ю. І. Мова ворожнечі в соціальних мережах: форми прояву та механізми протидії. Запоріжжя: ЗНУ, 2024. 49 с.

[3] Ейсмунт В. Як створюють фейки у Facebook, YouTube, Telegram та Viber. URL: https://zaxid.net/statti_tag50974/

[4] Штучний інтелект і дезінформація: можливості та ризики в умовах війни. *Укрінформ.* URL: https://www.ukrinform.ua/rubric-technology/3691961-stucnij-intelekt-i-dezinformacia-mozlivosti-ta-riziki-v-umovah-vijni.html

Як зазначає Ю. Коваленко, застосування технологій ШІ на сьогоднішній день надає широкий спектр можливостей в військовій сфері, адже «ШІ може покращити та оптимізувати процес прийняття рішень на полі бою, поглибити обізнаність та розуміння поля бою, забезпечити перевагу, адаптивність планування сил та підвищити точність і швидкість прийняття рішень, зокрема й щодо виявлення, ідентифікації, оцінки загроз та реагування на них. Впровадження ШІ у військовій сфері може передбачати, серед іншого, розробку БпЛА, антидронових рушниць, систем управління боєм, тренувальних модулів, систем кібербезпеки. Завдяки ШІ стає можливою й розробка новітнього озброєння, впровадження автономних систем озброєнь (АСО), тобто бойових систем, що здатні самостійно ідентифікувати та вражати ціль, а також летальних автономних систем озброєнь (ЛАСО), тобто таких систем зброї, які можуть виявляти, визначати цілі та атакувати їх без прямої участі людини у прийнятті рішення про момент та об'єкт атаки. Однак використання ШІ у військових цілях нерідко викликає й певні етичні та моральні занепокоєння, особливо у контексті використання летального автономного озброєння».[1]

Як відзначає В. Шевчук, у сучасних умовах гібридної війни правоохоронні органи також активно використовують технології штучного інтелекту за різними напрямками, серед яких дослідник виокремлює: 1) розпізнавання обличчя та ідентифікація російських військових-окупантів у соціальних мережах та камерах відеозапису; 2) забезпечення безпеки на дорогах, виявлення та фіксація порушень правил дорожнього руху; 3) використання безпілотників для протидії незаконному обігу вогнепальної зброї, наркозлочинності, збирання доказової інформації умовах війни і ведення активних бойових дій з метою фіксації воєнних злочинів; 4) попередження кримінальних правопорушень з використанням інтелектуальних систем безпеки з різними пристроями (датчиками) збору інформації; 5) прогнозування кримінальних правопорушень методом картографування злочинності, за допомогою якого формуються прогнози щодо місцевої злочинності та індивідуальної злочинної поведінки.[2]

---

[1] Коваленко Ю., Войнов М. Штучний інтелект та права людини: орієнтири та обмеження у контексті національної безпеки та оборони. 2024. URL: https://www.helsinki.org.ua/wp-content/uploads/2024/05/Preview_AI_human_right_A4-1.pdf

[2] Шевчук В. М. Використання технологій штучного інтелекту та процес цифровізації криміналістики в умовах війни. *Актуальні проблеми протидії злочинності та корупції*: збірник тез Всеукраїнської науково-практичної конференції (Харків, 17 лютого 2023 р.). С. 172-173.

Одночасно з безцінним результатом, що надає функціонал відповідного ШІ, процес ідентифікації викликає занепокоєння експертів в контексті етико-юридичної оцінки такого використання ШІ. Так, неодноразово наголошувалося на сумнівах щодо легальності збору даних, необхідних для ідентифікації, адже такі дані збираються з порушенням прав на конфіденційність, а подальше їх використання може бути пов'язане з ризиками контролю над населенням.

Так, в експертному середовищі панує думка, що використання цих інструментів для потреб безпеки у країні насправді може призвести до масового стеження чи інших зловживань. Продовження використання ШІ з подібним функціоналом на державному рівні може стати перепоною для подальшої інтеграції до європейської спільноти, адже ряд держав Європи визнали використання технології Clearview незаконним, наклали високі штрафи та намагалися заборонити збирати базу даних облич своїх громадян.[1]

Широкого застосування штучний інтелект набув і в основних месенджерах – Telegram, Whatsapp, Viber, Messenger. Серед основних напрямків його використання – створення чат-ботів з різноманітним функціоналом (генерування зображень та відео, збереження графічного та аудіовізуального контенту з окремих інтернет-ресурсів, пошук та підбір інформації тощо), використання можливостей месенджера для генерації запитів до нейромереж та ШІ, використання останніх з метою введення в оману та шахрайських схем.

На сьогоднішній день можливості нейромереж генерувати голосові та відео-повідомлення, які є настільки реалістичними та неможливими для виявлення їх штучного походження, надають зловмисникам можливість використовувати дані технології для введення в оману користувача (або цілої групи користувачів) месенджера. Генеративний ШІ може навіть зробити застарілими найкращі на сьогодні заходи запобігання шахрайству, як-то голосова автентифікація чи «живі перевірки», коли зображення людини у реальному часі має збігатися із тим, що зберігається в системі.[2] На теперішній час значно-

[1] Tokariuk O. Ukraine's Secret Weapon – Artificial Intelligence. *Center for European Policy Analysis.* 2023. URL: https://cepa.org/article/ukraines-secret-weapon-artificial-intelligence/

[2] Кофлін Д. ШІ допомагає всім, навіть шахраям. Як штучний інтелект став новою зброєю кіберзлочинців та стимулював афери на $8 млрд. *Forbes Digital.* URL: https://forbes.ua/innovations/shi-dopomagae-vsimi-navit-shakhrayam-yak-shtuchniy-intelekt-stimulyuvav-aferi-na-8-mlrd-19092023-16102

го поширення набрали шахрайські схеми, в яких знайома особа просить грошові кошти в борг або доступ до якогось додатку, але сама така особа не в курсі, що від її імені і, нерідко, її голосом відбувається спроба заволодіти чужими коштами. В умовах же інформаційної війни дані технології використовуються для отримання оперативний військових даних, дезінформації військовослужбовців, що однозначно створює загрозу державній безпеці.

Боротьба ж випадками шкідливого використання генеративного ШІ ускладняється з наступних причин:

– подальша еволюція технології дозволяє обходити технологічні засоби протидії застосування ШІ – генеративні ШІ вже зараз здатні обманювати детектори ШІ;
– розвиток даної технології напряму пов'язаний з перевагами, які вона надає при створенні ефективного голосового помічника або в допомозі особам, що мають вади мови;
– ефективність боротьби напряму пов'язана з інформаційною гігієною користувачів, а отже й залежить від раніше означеної проблеми наявності значного масиву інформації про людину в соціальних мережах.

Окрім класичних соціальних мереж широке використання штучного інтелекту та нейромереж можемо споглядати й у випадку **дейтинг**-платформ та додатків. Під дейтингом зазвичай розуміють діяльність спеціалізованих онлайн-платформ, які використовуються користувачами для онлайн-знайомств. Основною метою користувачів дейтинг-платформ є пошук людини на основі своїх уподобань, для чого означені сервіси використовують різні механіки пошуку за певними критеріями.

Вже зараз з метою забезпечення ефективності надання комунікативних послуг дейтинг-сервіси застосовують сучасні технології, в тому числі ШІ. Так, наприкінці 2024 року компанія Match Group, яка володіє такими популярними додатками для знайомств як Tinder та Hinge, оголосила про плани інтегрувати генеративний ШІ у свої сервіси для покращення біографій та профілів користувачів.[1] Крім того ШІ та нейромережі використовуються дейтинг-платформами для оцінки

[1] Довірити своє серце алгоритмам: як штучний інтелект змінює сучасний дейтинг і що з цим може бути не так? 2025. URL: https://zaborona.com/doviryty-svoye-sercze-algorytmam-yak-shtuchnyj-intelekt-zminyuye-suchasnyj-dejtyng-i-shho-z-czym-mozhe-buty-ne-tak/

сумісності пари, надання порад в спілкуванні та оформленні профілю, опосередкованого спілкування замість користувача, здійснення перекладу текстових та голосових повідомлень тощо.

Одночасно з цим штучний інтелект в дейтинг-сфері використовується також і з метою надання користувачу послуг персоналізованого спілкування з віртуальним партнером. Слід відмітити розвиток технологічних можливостей таких платформ, що зумовлюється стрімким збільшенням попиту на такий цифровий продукт. Так, сервіси на зразок Candy.ai та Kupid.ai надають можливість користувачу, вибравши стать майбутнього партнера, створити вигаданого персонажа, який за допомогою штучного інтелекту дає можливість спілкуватися з ним голосовими повідомленнями.[1]

Відкидаючи морально-етичні моменти відносин з цифровою особою слід однак звернути увагу на юридичний контекст, а саме на захист прав користувача подібних дейтинг-платформ. В першу чергу слід говорити про захист інформації, отриманої в межах комунікації з віртуальним партнером, власником платформи від розповсюдження та витоку, а також збереження режиму приватності щодо персональних даних та самого факту надання послуг, адже користувач може не бажати публічності факту надання таких послуг дейтинг-сервісом.

Сучасні додатки для знайомств вже збирають величезну кількість чутливої інформації, такої як геолокація, їхні вподобання, історію листування та навіть фото і відео.[2] Окрім традиційного неконтрольованого поширення таких даних загрозу становить також використання таких даних для створення небіологічних осіб, наділених штучним інтелектом, які, навчаючись на зазначених даних, можуть створювати цифрові клони реальної людини, тим самим користуючись чужою особистістю та вводячи в оману осіб, з якими спілкується в подальшому.

Використання таких цифрових копій осіб вже зараз зумовило проблему поширення випадків свідомого використання можливостей ШІ для маніпулювання емоціями і шахрайських схем. На даний момент

[1] Коноплицький С. Майбутнє дейтингу – «Тіндер» для знайомств із ШІ-моделями. URL: https://speka.media/maibutnje-deitingu-tinder-dlya-znaiomstv-iz-si-modelyami-pk4lzd

[2] Довірити своє серце алгоритмам: як штучний інтелект змінює сучасний дейтинг і що з цим може бути не так? 2025. URL: https://zaborona.com/doviryty-svoye-sercze-algorytmam-yak-shtuchnyj-intelekt-zminyuye-suchasnyj-dejtyng-i-shho-z-czym-mozhe-buty-ne-tak/

практично надзвичайно важко захистити свої права щодо такого «викрадення» особистості через складність доказування та відсутність законодавчих механізмів захисту від використання чужої особистості без дозволу особи.

Використання таких цифрових інструментів як нейромережі та інших видів штучного інтелекту в Інтернеті не обмежується означеними сферами та методами, адже сама сфера інтернет-відносин формується та змінюється ледь не щодня, а отже на тлі цього кількість напрямків застосування даних технологічних рішень збільшується в геометричній прогресії. Вважаємо за необхідне дослідити окремі приклади застосування ШІ, що актуалізувалися саме в умовах гібридної війни.

В межах російсько-української війни зараз наявне інформаційне протиборство, яке можна аналізувати як в рамках підсистеми кібербезпеки, так і в рамках інформаційно-психологічної підсистеми. Це інформаційне протиборство проявляється за допомогою фейків, спекуляцій, маніпуляцій, дезінформації, антиукраїнських наративів, інформаційного насильства, масованих інформаційних атак, інформаційно-психологічних спецоперацій та війн, інформаційно-психологічного та кібертероризму.[1]

На сьогодні представники збройних сил використовують ШІ для вербування солдатів; підготовки воєнних до виконання завдань; ухвалення стратегічних рішень; обробки даних та досліджень; прогнозування майбутнього; виявлення та розпізнавання об'єктів; ліквідації цілей; моніторингу загроз; транспортування людей та об'єктів; допомоги медикам; забезпечення режиму кібербезпеки.[2]

Українські збройні сили дедалі частіше використовують ШІ в мережі Інтернет для ідентифікації ворожих цілей. Як зазначають спеціалісти видання The Economist, оскільки російські солдати і військові блогери стали більш обережними у своїх публікаціях, прості пошуки будь-яких ознак розташування військ стали менш плідними. Однак, обробляючи велику кількість повідомлень та відео, ШІ-моделі мо-

[1] Воропаєва Т., Авер'янова Н. Штучний інтелект в системі інформаційної безпеки України в умовах російсько-української війни. *Collection of Scientific Papers «SCIENTIA»*, (August 23, 2024; Valencia, Spain), P. 63.

[2] Війна та нейромережі: як штучний інтелект використовують на полі бою. URL: https://forklog.com.ua/exclusive/vijna-ta-nejromerezhi-yak-shtuchnyj-intelekt-vykorystovuyut-na-poli-boyu

жуть знайти потенційні підказки, об'єднати їх і потім видати ймовірне місце розташування системи озброєння або військ противника.[1]

Спірним з етичної точки зору виглядає використання ШІ для виявлення схильних до зради співвітчизників. Так, використовуючи ШІ, здійснюється пошук зв'язки у розрізнених масивах даних з метою виявлення та оцінку ризику зради окремих громадян.[2]

Одночасно з цим ШІ широко використовується ворогом в межах ІПСО, а також іншими суб'єктами для створення синтетичного контенту в межах інформаційної війни проти нашої держави.

Як вже зазначалося, генеративний ШІ набуває здатності до навчання та імітації творчого процесу людини, в результаті чого алгоритми штучного інтелекту можуть створювати контент, використовуючи величезні обсяги даних для аналізу структури, стилю та особливостей різних типів творів. Крім того, штучний інтелект може генерувати контент за допомогою методів машинного навчання і нейронних мереж.[3]

Як відзначає А. Юшина, на сьогоднішній день в наукових колах актуалізується дискусія навколо правомірності використання ШІ творів для навчання, які охороняються авторським правом, оскільки на основі їх аналізу ШІ створює нові схожі об'єкти, а автори творів не отримують винагороду за таке використання.[4] Крім того, авторка вбачає проблемним питання, чи порушується авторське право під час генерування нового контенту ШІ, адже авторські твори використовуються для машинного навчання.

Д. Прилипко приходить до висновку, що на сьогоднішній день законодавча база стосовно авторських прав на твори, створені за допомогою штучного інтелекту, перебуває на початковому етапі формування. В світі склалася ситуація, що жодна країна на законодавчому рівні належним чином не врегулювала питання забезпечення

---

1 Як Україна використовує штучний інтелект у війні з Росією – The Economist. 2024. URL: https://texty.org.ua/fragments/112210/yak-ukrayina-vykorystovuye-shtuchnyj-intelekt-u-vijni-z-rosiyeyu-the-economist/

2 Як Україна використовує штучний інтелект у війні з Росією – The Economist. 2024. URL: https://texty.org.ua/fragments/112210/yak-ukrayina-vykorystovuye-shtuchnyj-intelekt-u-vijni-z-rosiyeyu-the-economist/

3 Вальчук Д. В. Авторське право штучного інтелекту: проблеми та шляхи вирішення. *Modern scientific journal.* 2024. № 3 (1). С. 10.

4 Юшина А. Штучний інтелект: кому належать авторські й майнові права. URL: https://mind.ua/openmind/20255019-shtuchnij-intelekt-komu-nalezhat-avtorski-j-majnovi-prava

правової охорони та належності авторських прав на твори, створені штучним інтелектом, однак деякі розвинені держави мають низку нормативно-правових актів, що частково регулюють сферу відносин, пов'язаних з творами, створеними штучним інтелектом.[1]

Функціональні можливості генеративного ШІ успішно використовуються при створенні так званих «емоційних фейків» в соціальних мережах. У соціальних мережах зараз поширюється багато дописів, які містять фото з ознаками генерації штучним інтелектом. На них зображені нібито українські військові з закликами привітати їх чи то з днем народження, чи то з весіллям. Також є схожі дописи про врятованих тварин, дітей або літніх людей.[2]

Ледве не кожен в запропонованих механізмами соціальних мереж публікація стикається з зображеннями, на яких відображено надзвичайні результати творчості, що викликають захват, відображені непересічні ситуації людського горя, нестандартних ситуацій та несприятливих умов, а також з аудіовізуальним контентом, що відображає надзвичайно сентиментальні ситуації та закликає до проявлення емпатії (так звані пости «ніхто нас не вітає», «ви не повірите» або «ці брати»).

Завдання контенту таких публікацій викликати емоції та заохотити користувачів відреагувати, спіймати вразливу аудиторію в емоційну пастку і змусити поширити їх далі, тиснучи на почуття провини, викликаючи емпатію та співчуття.

Довгий час дані публікації сприймалися з гумором, адже, на перший погляд дані публікації, не загрожують шкідливими наслідками, а самі зображення, згенеровані ШІ, містять ряд кумедних для сприйняття артефактів, що очевидно свідчать про несправжність запропонованого фото та ситуації на ньому. Однак, дані публікації не просто не є нешкідливими, при подальшому вивченні можна визначити загрози, які несуть на собі такі емоційні фейки.

Так, докладний аналіз релевантних шляхів використання емоційних фейків свідчить про наступні мотиви, з яких публікують такі записи у Facebook, Instagram та TikTok:

---

[1] Прилипко Д. Штучний інтелект та авторське право. *Теорія і практика інтелектуальної власності.* 2021. № 2. 15-22. URL: http://uran.inprojournal.org/article/view/236526/235043

[2] Денисяка О. «У військового день народження, а його ніхто не привітав»: чим небезпечні ШІ-світлини у Facebook. URL: https://hromadske.ua/suspilstvo/232022-u-viyskovoho-den-narodzennia-a-yoho-nikhto-ne-pryvitav-chym-nebezpechni-shi-svitlyny-u-facebook

- збір аудиторії для подальшого просування рекламних продуктів, пропагандистських наративів тощо. В даному випадку завданням публікації виступає заохочення користувачів соціальної мережі до взаємодії, тобто йде мова про використання емоцій для прикриття шкідливого змісту самої публікації. Розміщення в соціальній мережі емоційних фейків певного характеру (співчутливі, ушановуючі, схвальні) дають змогу виділити певну групу людей, схильних до проявлення емоцій та не здатних відрізняти справжні фотографії подій від згенерованих за допомогою ШІ. В подальшому відповідний користувацький ресурс може бути використаний для успішного просування сумнівних продуктів або пропагандистських тез, що особливо небезпечно в умовах війни. Емоційні фейки в даному випадку слугують маркером людської сентиментальності та можливості нав'язувати певним особам необхідної думки;
- ілюстрація підтримки певної позиції або провокація аудиторії – особливо актуально через можливість заміни первинного матеріалу (цифрового контенту) без анулювання реакцій користувачів у вигляді лайків та коментарів. Крім того дані публікації є відомим майданчиком для використання ботів при провокуванні дискусії та м'якого просування шкідливих наративів;
- витіснення дійсно важливого та актуального контенту шляхом заповнення рекомендацій емоційними фейками та подібним шкідливим контентом;
- просування негативних настроїв в суспільстві в межах ІПСО, формування негативного ставлення до керівництва Збройних сил, політичної системи держави; формування
- збір даних про користувачів з метою подальшого використання; шахрайство, шляхом спонукання до переходу за сторонніми посиланнями, фішинг тощо.

Одним з найпоширеніших способів використання ШІ в умовах гібридної війни залишається створення діпфейків.

Діпфейки (англ. deepfake – глибока підробка), що ширяться інтернетом у формі фальшивих зображень та відео представляють собою технологію, що базується на штучному інтелекті, синтезує зображення чи відеозапис, поєднує і накладає справжні і згенеро-

вані зображення та відео.[1] Ці фальсифікації можуть виглядати дуже реалістично і використовуються для поширення дезінформації, маніпуляції громадською думкою, шантажу та навіть викрадення особистих даних.[2]

Головна небезпека, яку несуть діпфейки є простота виробництва та використання таких матеріалів, які використовують для поширення фальшивих наративів, паніки та з метою скомпрометувати особу. Особливої ефективності діпфейки набувають у випадках обмеженості часу на перевірку інформації, адже доведення синтетичності контенту та подальше спростування інформації здійснюється набагато повільніше, ніж вірусне поширення контенту, що потенційно має значний резонанс.

Ще в 2020 році прогнозувалося використання діпфейків в промислових масштабах з метою ведення інформаційних війн, пропаганди і маніпуляції. Крім того, експертами прогнозувалося становлення правового регулювання в даній сфері, а саме формування на рівні національних законодавств положень, які контролюють продукцію і поширення контенту з використанням діпфейків із метою дезінформації.[3] Однак, попри такі прогнози, на сьогоднішній день вітчизняне законодавство не містить дієвих механізмів боротьби з діпфейками.

В ситуації повномасштабного вторгнення та інформаційної напруги використання діпфейків для створення синтетичного контенту, що відображає неправдиві способи дій та заяви високопосадовців України може мати серйозні наслідки, адже такі дії не лише спотворюють реальну картину подій, а й можуть спричиняти паніку серед населення, підривати довіру до уряду та військового керівництва, а також впливати на міжнародну підтримку України.[4]

Слід однак зазначити, що вже зараз наявні інструменти для протидії таким інформаційним атакам. Так, автоматизована система SemanticForce дозволяє аналізувати шкідливі інформаційні потоки й

[1] Голос на відео не належить мені: ворог запустив «діпфейк» про ситуацію в Покровську. Армія Інформ. 2024. URL: https://armyinform.com.ua/2024/09/28/golos-na-video-ne-nalezhyt-meni-vorog-zapustyv-dipfejk-pro-sytuacziyu-v-pokrovsku/

[2] Юридичні аспекти боротьби з дезінформацією на основі діпфейків. URL: https://consultant.net.ua/consultant-article/5394

[3] Подус С. Діпфейки в інформаційній війні. Матеріали IV Міжнародної наукової конференції ХНУПС ім. І. Кожедуба, 21-22 травня 2020. С. 108-110.

[4] Бірюкова А. Г., Колісникова Г. В. Способи захисту порушених прав при створенні та розповсюдженні діпфейків. *Проблеми законності.* 2024. Вип. 164. С. 8.

зображення, а також відстежувати реакцію на них користувачів, відрізняти хибні акаунти від реальних користувачів тощо. Поряд з цим, система Attack Index використовується для виявлення конкретних інформаційних операцій та їхніх характеристик (мережа поширення інформації, ініціатор операції, час, інтенсивність, масштабність тощо), а також для подальшої розробки сценаріїв ефективної протидії інформаційним загрозам.

Використання ШІ для боротьби з шкідливим ШІ виглядає перспективним, однак треба обов'язково враховувати, що штучний інтелект має деякі недоліки. Наприклад, цілком можливе порушення прав людини через недосконалість сучасних біометричних систем, а також через значну кількість помилок у їхній роботі.[1]

На сьогоднішній день використання діпфейків в цивільно-правовому контексті може розглядатися з трьох сторін: з точки зору захисту персональних даних (якщо діпфейк використовує особисту інформацію або зображення), захисту честі та гідності (якщо діпфейки впливають на репутацію або наносять моральну шкоду), захисту прав інтелектуальної власності (якщо діпфейк порушує авторські права або права на торговельну марку тощо).

Використання діпфейків з неправомірних цілях напряму пов'язане з незаконним використанням чужих персональних даних. Слід відмітити, що початково наявні дані (в тому числі персональні) в мережі були відкритими для перегляду, однак ШІ несанкціоновано використовував ці дані для конкретних цілей, при цьому нехтуючи принципом транспарентності системи.[2]

Масивні бази даних, що зберігають конфіденційну інформацію, регулярно приваблюють зловмисників. У разі успішної атаки постраждати можуть як репутація організації, так і безпека користувачів, чиї персональні відомості можуть опинитися у відкритому доступі.[3]

---

[1] Воропаєва Т., Авер'янова Н. Штучний інтелект в системі інформаційної безпеки України в умовах російсько-української війни. *Collection of Scientific Papers «SCIENTIA»*, (August 23, 2024; Valencia, Spain), P. 63.

[2] Остіян Є. З. Штучний інтелект та персональні дані: захист приватності в цифровому середовищі. *Науковий вісник Ужгородського Національного Університету.* 2024. URL: https://visnyk-juris-uzhnu.com/wp-content/uploads/2024/11/9-2.pdf

[3] Петрів О. Захист персональних даних у добу штучного інтелекту: міжнародні підходи та виклики. 2025. URL: https://cedem.org.ua/consultations/zahyst-personalnyh-danyh-u-dobu-shtuchnogo-intelektu-mizhnarodni-pidhody-ta-vyklyky/

Використання технологій діпфейк може бути також пов'язане з порушенням авторських прав та інших прав інтелектуальної власності в наступних випадках:

– незаконне копіювання та розповсюдження творів автора – з метою виготовлення діпфейків зазвичай використовуються твори, захищені авторським правом, без дозволу правовласника;
– створення похідних творів без дозволу автора – створення власних творів на основі вже існуючого твору, захищеного авторським правом;
– маніпуляція та спотворення творів з метою створення хибного враження про автора або зміст твору;
– використання творів в комерційних цілях без дозволу автора –використання для створення реклами або інших комерційних матеріалів творів, захищених авторським правом, без згоди правовласника.[1]

На практиці прикладами порушення прав інтелектуальної власності з використанням технологій діпфейку можуть слугувати:

– виготовлення фальшивих відео з відомими особами – такі відео можуть завдати шкоди репутації цих осіб та порушити їх права на використання свого образу;
– виготовлення синтетичних музичних творів, записів голосу відомих осіб, що може вводити в оману слухачів та порушувати авторські права на музичні твори;
– незаконне дублювання фільмів;
– просування підроблених продуктів за допомогою рекламних матеріалів, які демонструють функціональність, схожу на запатентовану, без фактичного використання запатентованої технології;
– нанесення шкоди репутації бренду шляхом створення фальшивих рекламних матеріалів або відео, які асоціюють торгову марку з негативною або компрометуючою інформацією.[2]

Аналіз чинного вітчизняного законодавства в сфері протидії дезінформації, що хоча національне законодавство розвивається у відповідь на сучасні виклики, існує потреба в подальших реформах. Як

[1] Deepfake та право на образ як захистити свою репутацію в епоху штучного інтелекту. URL: https://polikarpov.legal/blogposts/deepfake-ta-pravo-na-obraz/

[2] Deepfake та право на образ як захистити свою репутацію в епоху штучного інтелекту. URL: https://polikarpov.legal/blogposts/deepfake-ta-pravo-na-obraz/

зазначають А. Г. Бірюкова, Г. В. Колісникова, запровадження відповідальності за розповсюдження дезінформації, реалізація процедур спростування та встановлення компенсацій за завдану шкоду є критичними аспектами для забезпечення ефективного захисту прав в епоху цифрових технологій.[1]

У юридичній науці ШІ виступає каталізатором для переосмислення багатьох правових режимів, адже дана технологія може входити одночасно до декількох галузевих юридичних конструкцій через специфіку різноманіття даних, які вона збирає.[2]

Як вже зазначалося, машинне навчання алгоритмів штучного інтелекту потребує значних об'ємів даних, обчислювальної потужності та часу. З точки зору роботи з особистою інформацією потреба у великій кількості даних створює найбільші перешкоди розробникам, адже в більшості випадків така інформація не знаходиться у вільному доступі, навіть, соціальні мережі не розцінюють сторінки користувачів, як відкрите джерело. [3] З появою великих об'ємів даних (Big Data) і швидким розвитком штучного інтелекту зростають ризики витоку (неправомірного поширення), неправомірного доступу та маніпулювання особистою інформацією.[4]

Обіг особистої інформації має певні відмінності в залежності від регіону чи країни, однак базові принципи залишаються незмінними. Головною метою є надати користувачам контроль над своїми даним та протидіяти їх неправомірному збору, збереженню та використанню.[5]

Відповідно до частин першої, другої статті 32 Конституції України ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України. Не допускаєть-

---

[1] Бірюкова А. Г., Колісникова Г. В. Способи захисту порушених прав при створенні та розповсюдженні діпфейків. *Проблеми законності.* 2024. Вип. 164. С. 16.

[2] Остіян Є. З. Штучний інтелект та персональні дані: захист приватності в цифровому середовищі. *Науковий вісник Ужгородського Національного Університету.* 2024. URL: https://visnyk-juris-uzhnu.com/wp-content/uploads/2024/11/9-2.pdf

[3] Тамашев В. Персональні дані у контексті обробки штучним інтелектом. URL: https://legalitgroup.com/personalni-dani-u-konteksti-obrobki-shtuchnim-intelektom/

[4] Петрів О. Захист персональних даних у добу штучного інтелекту: міжнародні підходи та виклики. 2025. URL: https://cedem.org.ua/consultations/zahyst-personalnyh-danyh-u-dobu-shtuchnogo-intelektu-mizhnarodni-pidhody-ta-vyklyky/

[5] Тамашев В. Персональні дані у контексті обробки штучним інтелектом. URL: https://legalitgroup.com/personalni-dani-u-konteksti-obrobki-shtuchnim-intelektom/

ся збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини. Водночас статтею 64 Конституції України передбачено положення, що в умовах воєнного або надзвичайного стану можуть встановлюватися окремі обмеження прав і свобод із зазначенням строку дії цих обмежень.

Як зазначають дослідники механізмів захисту персональних даних користувачів мережі Інтернет, правовозастосовча практика у сфері використання персональних даних штучним інтелектом формується за такими напрямками: право власності на дані, їхня безпека, відповідальність за прозорість системи та регулювання обробки збору даних.[1]

Попри те, що контроль за дотримання конфіденційності та безпеки персональних даних здійснюється відповідними органами, слід враховувати, що вони не здатні відстежувати та вчасно звертати увагу на всі порушення. Тому користувач має усвідомлювати, яку інформацію надає, та передбачати можливість її протиправного використання, особливо це стосується соціальних мереж.[2]

В юридичній літературі контексті порушення права на приватність в мережі Інтернет, зазвичай згадують порушення ще двох прав людини – право на свободу висловлення та право мирних зборів. Х. Солодовнікова приходить до думки, що особа, яка знає, що за нею можуть слідкувати, буде більш обережною у висловлюваннях та буде брати менш активну участь у громадському житті. Безпосередньо ж право на свободу висловлення може порушуватися через тимчасове або постійне припинення дії акаунтів у соціальних мережах за допомогою фільтрів, які відслідковують дописи, які штучний інтелект визначає як такі, що порушують права інших людей: несуть загрозу, булінг, дискримінацію за національністю, релігією тощо.[3] Крім того,

---

[1] Остіян Є. З. Штучний інтелект та персональні дані: захист приватності в цифровому середовищі. *Науковий вісник Ужгородського Національного Університету.* 2024. URL: https://visnyk-juris-uzhnu.com/wp-content/uploads/2024/11/9-2.pdf

[2] Тамашев В. Персональні дані у контексті обробки штучним інтелектом. URL: https://legalitgroup.com/personalni-dani-u-konteksti-obrobki-shtuchnim-intelektom/

[3] Косілова О. І., Солодовнікова Х. К. Права і свободи людини і громадянина V. S. Штучний інтелект: проблемні аспекти. *Інформація і право.* 2020. № 4(35). URL: http://bulletin.kpi.ua/index.php/2616-6798/article/view/221218

слід відмітити можливість зловживання системою скарг і «банів» для користувачів з використанням необмеженої кількості ботів для формування видимості небезпечності контенту.

Як вже зазначалося, вітчизняні збройні сили широко використовують технології ШІ для розпізнавання облич противники. Якщо використання таких інструментів лише пов'язують з ризиком подальшого порушення конфіденційності та встановлення контролю за громадянами, то в той же час російський спосіб використання даного функціоналу вже пов'язують з відстеженням, цензуруванням та контролем за власними громадянами та нашими співвітчизниками на окупованих територіях.[1]

В Україні ж за допомогою технології Big Date та штучного інтелекту неодноразово викривали в такий спосіб великі ботоферми, а також піддавалися реальному кримінальному переслідуванню люди, які в соцмережах закликали до дій, що КК України кваліфіковано як «сепаратизм» та «тероризм». Аналіз відомих на сьогодні випадків використання Великих Даних та ШІ в мережі, до списку порушуваних прав можна також віднести свободу пересування, право володіти майном, право на демократію, а також різні форми дискримінації, які виникають в результаті застосування моделей, що спираються на Big Date та конвергенцію новітніх технологій.[2]

Ще одним шляхом використання ШІ в умовах гібридної війни може бути маскування рекламних матеріалів, в тому числі політичної реклами.

Попри стрімкий технологічний розвиток методів та форм просування рекламних продуктів, широке впровадження контекстної та нативної реклами в мережі Інтернет, значну конкуренцію методологій та бюджетів просування реклама в мережі Інтернет на сьогоднішній не має в вітчизняному законодавстві окремого режиму правового регулювання, а її використання підпорядковується загальним вимогам Закону України «Про рекламу» 1996 року прийняття.

---

[1] Штучний інтелект може бути ключем до перемоги України у війні – західні експерти. *Голос Америки.* 2024. URL: https://www.radiosvoboda.org/a/ukrayina-shtuchnyy-intelekt-viyna/32785722.html

[2] Косілова О. І., Солодовнікова Х. К. Права і свободи людини і громадянина V. S. Штучний інтелект: проблемні аспекти. *Інформація і право.* 2020. № 4(35). URL: http://bulletin.kpi.ua/index.php/2616-6798/article/view/221218

Попри цей факт законодавством передбачено ряд норм, що безпосередньо стосуються онлайн-реклами. Так, відповідно до положень ч.1 ст. 9 Закону України «Про рекламу» реклама має бути чітко відокремлена від іншої інформації, незалежно від форм чи способів розповсюдження, таким чином, щоб її можна було ідентифікувати як рекламу.

Ч.2 тієї ж статті закріплює правило, згідно якого реклама в інших (в тому числі онлайн) медіа повинна бути чітко відокремлена від іншої інформації з використанням слова «реклама».[1]

Як відзначає Д. Ківелюк, порушення, які виникають у сфері виробництва та поширення інтернет-реклами, можуть стосуватись приналежності права на створені об'єкти реклами, що є результатами творчої діяльності, законності використання в рекламі чужих творів та інших охоронних об'єктів (товарних знаків, знаків обслуговування, фірмових найменувань), захисту прав споживачів інтернет-реклами.[2]

Слід також відмітити використання ШІ для просування прихованої реклами безпосередньо в цифровому середовищі. Зокрема, як відзначає О. Косілова, технології, що впроваджуються з метою якісного покращення повсякденного побуту передбачають такі заходи як збір персональної інформації про користувачів Інтернету. В подальшому неодноразово відмічалося використання результатів аналізу цієї інформації для таргетування осіб та груп осіб відповідно до їх уподобань та психологічних особливостей, внаслідок чого особа піддається нав'язливому тиску контекстної реклами, що зокрема відображається й у технології, використовуваній Google Maps, а саме фізичне перебування людини у певний момент часу використовується для того, щоб вчасно надсилати пропозиції з метою вплинути на її вибір при покупці або виборі ресторану, відвідуванні музея тощо.[3]

Отже, на сьогоднішній день за допомогою інструментів ШІ розширюються можливості аналізу та оброки великої кількість інформації, автономного приймати рішень, вчасного розпізнання загрози тощо.

---

[1] Про рекламу: Закон України від 03.07.1996 № 270/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/270/96-%D0%B2%D1%80#Text

[2] Ківелюк Д. А. Цивільно-правове регулювання рекламних відносин в мережі Інтернет: дис.... канд. юрид. наук: 12.00.03. Хмельницький, 2019. С. 4

[3] Косілова О. І., Солодовнікова Х. К. Права і свободи людини і громадянина V. S. Штучний інтелект: проблемні аспекти. *Інформація і право.* 2020. № 4(35). URL: http://bulletin.kpi.ua/index.php/2616-6798/article/view/221218

Водночас використання ШІ несе й певні ризики у контексті гарантування прав людини. В цілому, технології ШІ можуть негативно впливати на право на життя, право на приватне життя та право на свободу вираження поглядів, а також інші основоположні права людини. Відтак важливим завданням є забезпечення належних гарантій, які б унеможливили порушення прав людини при використанні таких технологій, в тому числі у військовій справі.[1]

Підсумовуючи вищезазначене, можна зробити висновок, що на сьогоднішній день використання штучного інтелекту окрім явних переваг несе значну загрозу порушення прав людини, може суперечити індивідуальним та суспільним інтересам, загрожує державній безпеці та є прямим інструментом ведення інформаційної війни.

Як відзначають Т. Воропаєва та Н. Авер'янова, штучний інтелект може стати ефективним засобом протидії російській дезінформації та ключовим чинником вдосконалення системи інформаційної безпеки України в умовах гібридної війни у тих випадках, коли інструменти штучного інтелекту будуть не тільки технічно досконалими й надійними, але й будуть відповідати морально-етичним нормам, діючому законодавству та демократичним цінностям суспільства.[2]

Сьогодні з вільним і відкритим доступом до інформації та різноманітністю творчого та розважального контенту в Інтернеті пересічному громадянину часто важко зрозуміти, що можна вільно використовувати, а що ні.[3]

Вітчизняне законодавство та правозастосовча практика виходять із позицій захисту прав та свобод людини, однак стрімкий розвиток технологій штучного інтелекту зумовлює значні труднощі в формуванні дійсно ефективного механізму захисту від шкідливого впливу при застосуванні штучного інтелекту.

Сфера цифрових відносин в мережі Інтернет залишається специфічною для визначення методів протидії негативному впливу ШІ в

---

1 Коваленко Ю., Войнов М. Штучний інтелект та права людини: орієнтири та обмеження у контексті національної безпеки та оборони. 2024. URL: https://www.helsinki.org.ua/wp-content/uploads/2024/05/Preview_AI_human_right_A4-1.pdf

2 Воропаєва Т., Авер'янова Н. Штучний інтелект в системі інформаційної безпеки України в умовах російсько-української війни. *Collection of Scientific Papers «SCIENTIA»*, (August 23, 2024; Valencia, Spain), P. 65.

3 Попович К. Г. Правове регулювання реклами (цивілістичний аспект). *Науковий вісник Ужгородського університету*: серія: Право. 2023. Т. 1. Вип. 78. С. 219.

даній сфері, адже такі її специфічні риси як анонімність та відносна свобода дій є одночасно перепонами для ефективної протидії негативному впливу, що свідчить про необхідність подальшого вивчення та врахування етико-юридичних аспектів проблематики теми при формуванні законодавства в даній сфері.

Так, на думку В. Шевчука, для вирішення етико-юридичних проблем використання штучного інтелекту, необхідно створити глобальне (обов'язкове) міжнародне законодавство щодо розробки та впровадження штучного інтелекту, зокрема для запобігання його нелегальному, тобто нецивілізаційному використанню. Крім того, уряди та компанії повинні знати про недосконаліть даних, на яких базується технологія штучного інтелекту, і подбати про запобігання дискримінації та порушенням прав людини.[1]

Серед практичних способів захисту від шкідливого впливу ШІ в мережі Інтернет в умовах гібридної війни серед найбільш актуальних залишаються пропаганда інформаційної гігієни на державному рівні, боротьба з фейками, шкідливими емоційними згенерованими ШІ шляхом запровадження відповідальності за таку діяльність та формування адміністративної та судової практики з даних питань. Крім того вважаємо слушним на законодавчому рівні встановити вимогу маркування зображень, створених ШІ, а також розробку концептуальних положень контролю за використанням ШІ розробниками додатків з метою уникнення випадків створення «бекдорів» для корисних та неправомірних цілей.

Ключові слова: штучний інтелект, нейромережі, соціальні мережі, месенджер, емоційні фейки, право інтелектуальної власності, інформаційна гігієна, ІПСО, маркування зображень, інформаційна війна, діпфейк, генеративний штучний інтелект, дейтинг-сервіси, викрадення особистості, синтетичний контент

[1] Шевчук В. М. Використання технологій штучного інтелекту та процес цифровізації криміналістики в умовах війни. *Актуальні проблеми протидії злочинності та корупції*: збірник тез Всеукраїнської науково-практичної конференції (Харків, 17 лютого 2023 р.). С. 175.

Розділ 13

ЗАСТОСУВАННЯ СИСТЕМ АВТОМАТИЗОВАНОГО ПРИЙНЯТТЯ РІШЕНЬ ПІД ЧАС ЗБРОЙНОГО КОНФЛІКТУ

DOI

Віра Токарева
кандидатка юридичних наук, доцентка

По мірі впливу четвертої промислової революції на сучасне життя, зростає значення технологій великих даних та машинного навчання у суспільстві. Аналіз великих даних та предикативної аналітики дозволяє передбачувати ймовірні майбутні події, поведінку контрагентів, розраховувати ризики та допомагає приймати рішення [1]. Системи автоматизованого прийняття рішень покликані покращити процес вибору та прийняття рішень. Попри те, що технології машинного навчання та автоматизованого прийняття рішень наразі, вони вже використовуються у медицині для виявлення осіб та ризиків розвитку патологій, для проведення профілактичного лікування[2], у судочинстві для профілювання, оцінки ризиків та прогнозування ймовірності повторного вчинення правопорушень[3], у фінансовій сфері при прийнятті рішень про видачу кредиту, визначення платоспроможності, тощо. Технології машинного навчання, аналізу великих даних, дистанційної біометричної ідентифікації, зокрема, використовуються під час аналізу розвідувальних даних та збройних конфліктах.

Під час збройних конфліктів особливу роль відіграють системи підтримки прийняття рішень на основі ШІ, які аналізують дані та розробляють рекомендації для прийняття рішень. У порівнянні із повністю автономними системами озброєння, перевагами систем під-

[1] Rainie L., Anderson J. Code-dependent: pros and cons of the algorithm age. 2017. № 8. P. 2-41. 02/08181534/PI_2017.02.08_Algorithms_FINAL.pdf

[2] Faggella D. Applications of Machine Learning in Pharma and Medicine. *Tech Emergence.* July 19, 2018. URL: https://www.techemergence.com/machine-learning-in-pharma-medicine/

[3] Токарева В. О. До питання прийняття рішень із застосування алгоритмів. *Публічне та приватне право.* 2023. № 1. С. 30-35. URL: http://pp-law.in.ua/archive/1_2023/5.pdf

тримки прийняття рішень на основі ШІ є допомога в прийняті оптимальних рішень особі та підвищення обізнаності про ситуацію [1].

Поряд із значною увагою, дослідженню правових питань застосування технологій обробки великих даних, автоматизованих систем прийняття рішень, машинного навчання, віддаленої біометричної ідентифікації, застосування даних технологій в умовах збройного конфлікту, заслуговує пильної уваги. Застосування вищезгаданих технологій у збройному конфлікті актуалізує наступні питання.

По-перше, використання машинного навчання, може призвести до автоматизації окремих видів самооборони. Насьогодні, використовуються подекуди, автоматизовані системи реагування, які є стаціонарними оборонними системами, призначеними лише для реагування на вхідні загрози і мінімізації шкоди.

По-друге, поширення використання автоматизованих систем для допомоги прийняття рішень людиною актуалізує питання достовірність та надійності результатів такого аналізу, а також ступеня довіри людиною рекомендаціям алгоритмів. Актуалізується питання, здатності людини відкинути вочевидь хибне рішення запропоноване алгоритмом та прийняти рішення опираючись на власні переконання, досвід та судження.

По-третє, дискусії щодо використання технологій машинного навчання актуалізують питання прозорості процесу прийняття рішень, через нерозуміння логіки функціонування алгоритмів. Порід із цим, непрозорість рішень або рекомендацій автоматизованої системи, обумовлено тим, що її функціонування захищено як об'єкт права інтелектуальної власності [2].

Висуваються позиції, що використання систем прийняття рішень на основі ШІ може допомогти ефективно захищати цивільне населення під час збройного конфлікту. Оскільки система швидко сканує та аналізує ситуацію[3]. Разом з тим, дане твердження залишається вель-

[1] Zhou W. Greipl A. R. Artificial Intelligence in military decision-making: supporting humans, not replacing them August 29, 2024. URL: https://blogs.icrc.org/law-and-policy/2024/08/29/artificial-intelligence-in-military-decision-making-supporting-humans-not-replacing-them/

[2] Zwanenburg M. Know Thy Enemy: The Use of Biometrics in Military Operations and International Humanitarian Law. *International Law Studies (Naval War College).* 2021. № 97. P. 1404-1431.

[3] Joint Statement on Lethal Autonomous Weapons Systems First Committee, 77th United Nations General Assembly Thematic Debate – Conventional Weapons URL: https://estatements.unmeetings.org/estatements/11.0010/20221021/A1jJ8bNfWGlL/KLw9WYcSnnAm_en.pdf

ми дискусійним. Безумовно, міжнародне гуманітарне право зобов'язує військових командирів та інших осіб, відповідальних за напади, засновувати свої рішення на інформації з усіх джерел, доступних їм у відповідний момент часу. Зокрема, Міжнародний Комітет Червоного Хреста (далі МКЧХ) в контексті ведення міської війни рекомендує, проводити перевірку даних про наявність цивільних осіб та цивільних об'єктів, у відкритих джерелах, таких як Інтернет. Відповідно до висновків МКЧХ системи підтримки прийняття рішень на основі ШІ можуть допомагати збору, обробці даних з метою оперативного прийняття рішень та мінімізації ризиків для цивільного населення [1].

Водночас, будь-яка інформація, отримана за допомогою автоматизованих систем, має бути перевірена з різних джерел, щоб уникнути упередженої або неточної інформації. Проте, МКЧХ констатує складність проведення такої перевірки, а іноді й неможливість, через специфіку функціонування системи та способу взаємодії людини з автономними машинами.

Крім того, відповідно до міжнародного гуманітарного права, сторони збройного конфлікту, а саме людина, а не алгоритм несе відповідальність за дотримання норм права. Тому, дотримання норм міжнародного гуманітарного права покладається виключно на уповноважених осіб. Разом з тим, командувачі відповідальні за прийняття рішення та здійснення атак, можуть використовувати технологічну підтримку на підставі систем ШІ, для обґрунтування прийнятих власних рішень. Наразі, розроблені системи дозволяють проводити ідентифікацію осіб та об'єктів, оцінювати озброєння супротивника та нанесенні збитки. Відтак, при виборі цілі для атаки, можуть використовуватися системи підтримки прийняття рішень на основі ШІ, рішення яких носять рекомендаційний характер. Рекомендації таких систем не заміщають людину при прийнятті остаточного рішення [2].

Перевагою використання автоматизованих систем, також називають зменшення часу для прийняття рішення, даючи таким чином стороні переваги у порівняні з його супротивником.

Оскільки алгоритми машинного навчання, створені для передбачення майбутніх подій, держави прагнуть створити «системи ранньо-

[1] Stewart R. Hinds G. Algorithms of war: The use of artificial intelligence in decision making in armed conflict. October 24, 2023. URL: https://blogs.icrc.org/law-and-policy/2023/10/24/algorithms-of-war-use-of-artificial-intelligence-decision-making-armed-conflict/

[2] Там само.

го попередження», які б дозволяли виявляти майбутні загрози. Наразі, алгоритми дозволяють встановлювати місця розташування, переміщення озброєння. Навіть, виявляти посилення частоти листування на тему атак та загроз. Алгоритми здатні аналізувати та рекомендувати розташування представників правоохоронних органів у місцях, де існує висока вірогідність вчинення правопорушень. Алгоритми машинного навчання дозволяють виявляти зміни у висвітленні новин в авторитарних режимах напередодні збройного конфлікту. Такі інструменти можуть надавати критично важливу інформацію державам, у разі високої вірогідності збройного нападу сусіда. Безумовно, така аналітика та оцінка ризиків на основі машинного навчання має оцінюватися всебічно та приймати до уваги потенційні упередження[1].

Відносно використання системи дистанційної біометричної ідентифікації під час збройного конфлікту, то такі системи покликані забезпечити точне застосовування озброєння під час конфлікті, ніж, наразі, відбувається. Якщо від початку технології біометричної ідентифікації, як такі, розроблялися для цивільного застосування, зі спливом часу стали використовуватися під час збройних конфліктів. Наразі, збройні сили США мають найбільший досвід впровадження біометричної ідентифікації під час ведення військових операцій[2].

Технології біометричної ідентифікації можуть використовуватися в усьому спектрі операцій ведення збройного конфлікту: веденню бойових дій, забезпеченню безпеки, підтримання миру та військовими діями в мирний період. Технологія біометричної ідентифікації дає змогу з високим ступенем достовірності конкретно ідентифікувати особу та ворожу загрозу.

Використання технологій біометричної ідентифікації застосовується Організацією Північноатлантичного договору (НАТО) для розпізнавання суб'єктів які несуть загрози. У 2020 році НАТО оголосила про створення власної Автоматизованої системи біометричної ідентифікації, розробленої Агентством зв'язку та інформації НАТО [3].

---

[1] Deeks A., Lubell N., Murray D., Machine Learning, Artificial Intelligence, and the Use of Force by States. *Journal of National Security Law & Policy.* 2019. № 10. URL: https://ssrn.com/abstract=3285879

[2] Mitchell A. Distinguishing Friend from Foe: Law and Policy in the Age of Battlefield Biometrics. *Canadian Yearbook of International Law.* 2012. № 50. P.289-297.

[3] Див.: Zwanenburg M. Know Thy Enemy: The Use of Biometrics in Military Operations and International Humanitarian Law.

Серед аргументів проти використання автоматизованих систем та біометричної ідентифікації, зокрема, під час збройного конфлікту, слід назвати, упередження, помилки у ідентифікація алгоритмів, брак прозорості тощо.

Відносно такої переваги як зменшення часу для прийняття рішення, слід зазначити, що стратегія та тактика військового планування передбачає необхідність прийняття рішень військовим командуванням з урахуванням аналізу оперативної обстановки, місцерозташування супротивника та цивільного населення, оцінки переваг та недоліків вірогідних варіантів подій. У свою чергу, використання автоматизованих систем, в наслідок скорочення часу для ухвалення рішення, знижує здатність людини об'єктивно оцінити ситуацію. У випадку використання систем підтримки прийняття рішень на основі ШІ людина отримує обмежену інформацію про логіку «рекомендованого» рішення ШІ та аргументів які лягли в основу такої рекомендації. До того, ж як свідчать спостереження, використання автоматизованих систем здатне знизити пильність та здатність людини зберігати об'єктивну оцінку ситуації.

Серед помилок, слід назвати, некоректне розпізнавання осіб через ознаки шкіри, рекомендація маршрути руху транспорту без врахування актуальних дорожник умов, некоректне розпізнавання стін та відбійників, що приводило до ДТП за участі автономних транспортних засобів, тощо. Відтак, автоматизована система може бути введена в оману. Наприклад, під час конфлікту, через некоректне функціонування алгоритму, під час наведення на ціль цивільний транспортний засіб може бути ідентифікований як ворожий та навпаки [1].

По мірі зростання використання автоматизованих систем для розв'язання дедалі складніших завдань, накопичення досвіду навчання та прийняття рішень, стає складнішим перевірка помилок, які сприяли отриманню кінцевого результату. В свою чергу по мірі ускладнення систем, зростає ймовірність вчинення помилок, адже, навіть, невелика неточність у навчальних даних та розробці систем, може призвести до повторення помилок та виведення їх у еталоне значення.

[1] Див.: Deeks A., Lubell N., Murray D., Machine Learning, Artificial Intelligence, and the Use of Force by States.

Прийнято виділяти такі основні види упереджень: 1) упередження у навчальних даних; 2) упередження у дизайні та розробці; 3) упередження у використанні програми. Це означає, що упередження можуть виникати протягом усього життєвого циклу алгоритмічних моделей, починаючи зі збору даних, навчанні, використанні тощо [1].

Упередженості у навчальних даних обумовлені тим, що будь-які навчальні дані відображають певну обмежену вибірку. Така вибірка може містити як прямі упередження, щодо стереотипу, так і непрямі упередження щодо частоти їх виникнення. Відтак, упередженості у даних виникають внаслідок не репрезентативності даних або неповноти представлених даних, що призводить до нерепрезентативних результатів. Таким чином, упередження виникають, коли певні типи даних відсутні або представлені більше, ніж інші, що часто пов'язано зі способами отримання даних. Відтак, якість вхідних навчальних даних, визначає якість результату який буде отриманий. Оскільки система ШІ навчається відповідно до скормлених їй навчальних даних, які є єдиною інформацією яка використовується на етапу навчання та тестування, то неточності у цих даних, у подальшому будуть у підсумкових рішеннях.

Упередженості у дизайні та розробці. Упередженість даних може посилюватися на різних етапах обробки даних, наприклад, під час навчання моделі. Під час процесу навчання моделі штучного інтелекту, програмісти та інженери роблять проводять анотування, маркування, класифікація зразків даних, моделювання, оцінку моделі тощо. Таким чином, алгоритмічні упередження можуть також бути результатом, несвідомих упереджень, які люди вносять у життєвий цикл системи машинного навчання через різні завдання, які вони виконують. Поряд із цим упередження можуть виникати через відсутність прозорості функціонуванням алгоритму. На цьому етапі технології ШІ відображають упередження, притаманні навчальним даним та упередженням розробників.

Упередженості обґрунтовані використанням автоматизованих систем. Технології ШІ, як такі, будуть нести упередження через їх поширення та по мірі їх використання. Будь-які упередження, які

[1] Bode I. Falling under the radar: the problem of algorithmic bias and military applications of AI. March 14, 2024. URL: https://blogs.icrc.org/law-and-policy/2024/03/14/falling-under-the-radar-the-problem-of-algorithmic-bias-and-military-applications-of-ai/

містить система ШІ, будуть посилюватися, вводячи їх в еталон. В тому числі, через те, що люди схильні надмірно покладатися на результати які пропонує їм система, навіть, попри їх очевидну хибність. Таким чином існує вірогідність, що системи будуть генерувати все «більше даних заснованих на вже упереджених рішеннях». Таким чином, упереджені результати, отримані за допомогою технологій ШІ, також можуть бути додатковим виправданням для існуючих упереджень. На етапі використання технологій необхідно приймати до уваги упередженості у тому, як люди взаємодіють з технологіями ШІ, насамперед упередженість автоматизації. Наразі існує тенденція, що людина надмірно покладається на рекомендації автоматизованих систем та надмірно довіряє результатам, отриманим за допомогою таких технологій[1]. Існує чимало доказів упередженості щодо автоматизації, отриманих з досліджень поза межами військової сфери. Тому, на жаль, ми можемо легко уявити собі ситуації, коли люди занадто довіряють системам штучного інтелекту у військовому контексті.

Так, наприклад, у період поширення короновірусної інфекції, відомі випадки, коли система розпізнавання обличчя встановлена на об'єктах транспортної структури в одному із мегаполісів світу, розпізнала людину як таку, що перебуває у розшуку, при цьому черговим співробітниками поліції, було очевидно, що людина яку вони затримують, не схожа на особу яка перебуває в розшуку, але автоматизована система його розпізнала. Упередження автоматизації виявилося у тому, що співробітники поліції, навіть, розуміючи абсурдність затримання, віддали перевагу рішенню алгоритму, а ніж власними очам, уявленням про справедливість та законність.

Наслідком упереджень, невідомості як працює система «чорного ящику», є спроби підігнати та обґрунтувати рішення алгоритму. Американським фахівцями пропонується називати – алгоритмічним або математичним відмиванням (переклад з «mathwashing» або «farewashing») випадки коли суб'єкт намагається підвести будь-яку логіку та обґрунтувати рішення алгоритму, знайти правдоподібне логічне пояснення рішенню алгоритму, яке не має розумних підстав

[1] Proceed with Caution: Artificial Intelligence in Weapon Systems. Ordered to be printed 23 November 2023 and published 1 December 2023. Report of Session 2023–24. Published by the Authority of the House of Lords. URL: https://publications.parliament.uk/pa/ld5804/ldselect/ldaiwe/16/16.pdf

обґрунтування. Іншими словами алгоритмічне або математичне відмивання відбувається коли суб'єкт перестає довіряти собі, а автоматично обирає довіряти програмі, нехтуючи критичним мисленням. Ф. Бененсон, колишній начальник відділу даних Kickstarter зазначив, що математичне відмивання виникає внаслідок надмірної ідеалізації діяльності алгоритмів[1]. Т. Шеп відрізняє математичне відмивання яке відбувається випадково та яке проводиться цілеспрямовано. Відмивання відбувається випадково (суб'єкт обґрунтовує правдоподібність рішення алгоритму не навмисно, не розуміє вразливість рішення алгоритмічної системи) або цілеспрямовано (коли суб'єкт дотримуються, очевидно упередженого рішення прийнятого системою). Цілеспрямоване дотримання, вочевидь, упередженого рішення може бути обумовлено тим, що особа побоюється публічного осудження, бажає зберегти репутацію, хоча для суспільства є очевидним упередженість рішення алгоритму[2]. Проблема постає із розумінням упередженості як такої, оскільки стандарту упередженості не існує і також варіюється залежно від історичних, територіальних чинників, соціальних груп, релігійної приналежності, статі, тощо. Так, наприклад, 100 років тому не визнавалося упередженістю недопущення жінок до певних професій та посад. Водночас, сьогодні встановлення будь-яких обмежень, щодо зайняття жінками певних посад або певної діяльності буде визнано упередженістю. Прикладом упередженості для більшості цивілізованих держав світу, також є різний обсяг прав осіб в залежності від віросповідання. Тому, провідною умовою успішного функціонування алгоритмів, під час розробки та роботи є недопущення різного ставлення та різного обсягу прав суб'єктам, соціальним групам.

Відтак, можна припустити, що упередження у системі можуть призвести до неминучих наслідків, якщо суб'єкт певного віку, статті, расової приналежності буде помилково ідентифікований системою в якості комбатанта[3]. Упередження крім того впливають на функціональність і передбачуваність систем. Рішення можуть залишатися не

[1] Byrnes N. Why We Should Expect Algorithms to Be Biased 2016. URL: https://www.technologyreview.com/2016/06/24/159118/why-we-should-expect-algorithms-to-be-biased/

[2] What is mathwashing? url: https://www.mathwashing.com

[3] Chandler K. Does military AI have gender? Understanding bias and promoting ethical approaches in military applications of AI. UNIDIR, Geneva, 2021. URL: https://doi.org/10.37559/GEN/2021/04

ясними та незрозумілими, через брак інформації яким саме властивостям алгоритм надав переваги. Відтак, упередженість у навчальних даних, що використовуються для цивільного та військового застосування може посилюватися. Причиною може бути, використання навчальних даних які не приймають до уваги специфіку збройного конфлікту, коли дані відображають конкретний конфлікт або операцію, які не можуть бути застосовані у іншому випадку.

Вирішення проблеми алгоритмічної упередженості вимагає докорінної зміни дискримінаційного ставлення. Наприклад, на етапі розробки системи мають бути інтегровані стратегії пом'якшення наслідків.

Значної уваги потребує прийняття рішення про застосування сили, під час встановлення об'єкту нападу. Досить широкий спектр завдань і рішень, до яких може застосовуватися ШІ, також може нести наслідки для осіб які постраждали внаслідок збройного конфлікту, наприклад, у разі застосування арешту, затримання тощо.

МКЧХ наголошує про необхідність збереження контролю людини за рішеннями які можуть нести ризики та вплив для життя та здоров'я в умовах збройного конфлікту. Системи ШІ мають використовуватися саме в якості інструментів, здатних допомогти в прийнятті рішень людною, але в жодному разі не замінити її. З огляду на те, що системи ШІ розробляються для виконання завдань, які зазвичай виконуються людиною, залишається суперечність між прагненням до застосування ШІ та центральною роллю людини в збройному конфлікті, яка потребує подальшого дослідження. МКЧХ наголошує, на важливості забезпечення людиноцентричного підходу при розробці та використанні ШІ [1].

Підсумовуючи вищевикладене, з урахуванням низької прозорості функціонування автоматизованих систем, упередженості, прийняття юридично значущих має здійснювати виключно людина. Особливого значення набуває залишення контролю та ухвалення остаточного рішення за людиною у разі завдання шкоди здоров'ю та життю людям, пошкодження, руйнування цивільної інфраструктури, покладення відповідальності та дотримання сумлінності використання новітніх

[1] ICRC and International Federation of Red Cross and Red Crescent Societies, The Fundamental Principles of the International Red Cross and Red Crescent Movement: Ethics and Tools for Humanitarian Action, Geneva, November 2015. URL: https://shop.icrc.org/les-principes-fondamentaux-de-la-croix- rouge-et-du-croissant-rouge-2757.html.

технологій та недопущення зловживання правом у збройних конфліктах. Оскільки, не можна допустити ситуацію, при якій рішення про позбавлення людину життя, буде приймати алгоритм.

Ключові слова: штучний інтелект, біометрична ідентифікація, автоматизовані системи прийняття рішення, міжнародне гуманітарне право, машинне навчання, IT-право, інформаційні технології, інформаційне суспільство, цифрова доба, гібридна війна, воєнний стан.

Розділ 14

ГІБРИДНА ВІЙНА І КІБЕРЗБРОЯ

DOI

Євген Харитонов
доктор юридичних наук, професор,
член-кореспондент НАПрН України

Олена Харитонова
докторка юридичних наук, професорка,
членкиня-кореспондент НАПрН України

Попередні зауваження

Як зазначалося, термін «гібридна війна» набув популярності відносно недавно. До того, протягом століть йшлося просто про «війну», яку Геракліт називав «батьком усіх речей», і яка стала, врешті, «батьком» більш чи менш чітко визначеного доктринального концепту (класична /ідеальна війна), «легалізованого» міжнародними угодами поняття («конвенційна» війна).

Дослідники, які обґрунтовують застосування терміну «гібридна війна», як парасолькового, розглядаючи «гібридну війну» як новітній конфлікт і як форму глобального протистояння, концептуалізацію цього терміну починають зі згадки, що «гібридну війну у загальному вигляді розуміють як воєнні дії, що здійснюють шляхом поєднання мілітарних, квазімілітарнх, дипломатичних, інформаційних, економічних та інших засобів з метою досягнення стратегічних політичних цілей. Специфіка такого поєднання полягає в тому, що кожний з військових і невійськових способів ведення гібридного конфлікту застосовується у воєнних цілях та використовується як зброя».[1]

До цього слід додати також, що при типізації сучасних воєнних конфліктів типи війн розглядаються як «репрезентації загального конструкту війни як антагоністичного руйнівного зіткнення сторін,

[1] Яворська Г. М, Їжак О. І. Феномен гібридної війни. *Світова гібридна війна: український фронт:* монографія. За заг. ред. В. П. Горбуліна. Харків: Фоліо, 2017. С.19.

з подальшою конкретизацією, редукцією до певного методу, режиму, форми ведення війни, котрі беруться як характерні ознаки типів війни».

За такого підходу на чільне місце природно виступає «військова/ воєнна/ мілітарна війна», «нові воєнні теорії зазвичай виникають разом із виникненням нових воєнних феноменів, які потребують розробки мистецтва ведення війни в нових умовах з новим інструментарієм … уявлення про типи війни у своїй сукупності впливають на формування доктрин і бойових статутів, які мають практичне застосування, а найбільш розробленою у сучасній військовій науці є теорія звичайної або конвенційної війни, котру можна охарактеризувати як війну звичайними озброєннями звичайними методами, що ведеться державами з використанням регулярних військ».[1] Водночас термін «війна» у широкому сенсі застосовується у сферах, які не передбачають будь-якого використання військової зброї, наприклад, інформаційна, економічна, політична війна. У кожному випадку можна говорити про певні характерні методи дій у названих сферах, однак у традиційному (буквальному) сенсі вони є тільки компонентами «воєнної війни». Їхня абсолютизація як окремих видів війни є спірною. Натомість принциповою для розуміння специфіки гібридної війни є ідея функціонального перетворення на зброю традиційно невійськових засобів силового впливу та об'єднання їх на цій підставі з власне військовими методами».[2]

Головна вада такого підходу полягає в тому, що заперечуючи доцільність визнання окремих видів війни і прив'язуючи їх до ідеї (вимоги) «функціонального перетворення на зброю традиційно невійськових засобів силового впливу та об'єднання їх на цій підставі з власне військовими методами», ми втрачаємо можливість їхнього самостійного аналізу у випадках, коли агресор уникає «визнання стану війни» (і навіть «збройного конфлікту»), не використовує «власне військові методи» тощо, а досягає мети/ цілей у інший спосіб (політичний, економічний, юридичний, ментальний-релігійний, дипломатичний, культурний тощо тиск). Що росія, власне, і чинила досить успішно протягом 1991-2013 років. Більш того, навіть після 2014 року їй удавалося уникати «воєнної війни», вдаючись для досягнення сво-

[1] Яворська Г. М, Їжак О. І. Феномен гібридної війни С. 23.
[2] Яворська Г. М, Їжак О. І. Феномен гібридної війни. С. 26, 28.

їх цілей до «традиційно невійськових засобів силового впливу, але без об'єднання їх з власне військовими методами».

На нашу думку, спад інтересу до концепції «гібридної війни» в Україні після буму 2016-2018 років значною мірою був зумовлений саме тим, що «воєнна війна» не визнавалася, а «традиційно невійськові засоби силового впливу» внаслідок відсутності об'єднання (у кожному разі, – видимого) їх з власне військовими методами привертали усе менше уваги влади і суспільства (за винятком хіба що інформаційно-пропагандистських аспектів цієї проблеми).

Відтак концепти «війна» та «гібридна віна» потребують окремого вивчення під кутом зору проблематики, яка розглядається у цьому розділі.

Гібридна воєнна війна, як тло застосування кіберзброї

Розгляд цього питання варто почати зі з'ясування чинників зростання популярності концепту «гібридна війна».

Деякі автори вважають, що гібридна війна стала здобутком нового часу саме тому, що багато потрібних для неї завдань можна виконати за рахунок інформаційного компоненту. Чим сильнішим стає розвиток інформаційного компоненту, тим легшим буде виконання цих завдань.[1]

Натомість, інші автори зростання інтересу до категорії «гібридна війна» пов'язують з вадами чинного її розуміння. При цьому зазначається, що «згідно з міжнародним правом, «війна» – це стан справ між двома державами, або між двома групами держав, або між державою і групою держав, який супроводжується здебільшого розірванням дипломатичних відносин, подальшим призупиненням застосування загальних норм міжнародного права мирного періоду і загальною рішучістю вчинити насильницькі дії, навіть якщо такі дії насправді не мають місця. Процеси глобалізації, необхідність ведення війн за ресурси та у вирішенні геополітичних конфліктів неминуче призводять до настання юридичних наслідків для країн-учасниць війни у вигля-

[1] Гібридна війна: інформаційна складова. Георгій Почепцов. 25 жовтня 2015. URL: https://ms.detector.media/mediaanalitika/post/14501/2015-10-25-gibrydna-viyna-informatsiyna-skladova/

ді міжнародних санкцій». На такій тезі ґрунтується висновок, що «у XXI столітті постає гостра необхідність заміни класичного розуміння «війни» на модерне поняття «гібридна війна», яке *у* законодавстві країн учасників «війни» не визначене».[1]

Як на наш погляд, слушними є і одна, й інша точка зору, оскільки вони відображають обставини залежні (бажання обійти правила міжнародних угод та пов'язані з цим санкції тощо) та менш залежні (формування інформаційного суспільства, розвиток інформаційних технологій тощо) від волі людей.

Спираючись на аналіз точок зору зарубіжних науковців, А. А. Довженко визначає поняття «гібридна війна» у контексті загроз національній безпеці як «різновид збройного конфлікту, який включає у себе політичну, ідеологічну, економічну, інформаційну та військову складову, необхідні для досягнення поставлених цілей шляхом встановлення контролю над певною територією або соціальною групою».[2]

На думку Бориса Бідічева, керівника «Центру вивчення гібридної війни» ГО «Українська тактика», «гібридна війна поєднує традиційні і нетрадиційні методи. Тобто, симетричні і асиметричні, військові і невійськові методи ведення війни. Найважливішим є те, що гібридна війна – це війна, яка поєднує звичайні і незвичайні форми ведення війни, які дійсно переплітаються, і ніхто вже не може зрозуміти взагалі: це війна чи не війна точиться»[3].

Філіп Карбер розрізняє 4 воєнних і 4 невоєнних чинники гібридної війни. 4 воєнних – це використання традиційних якихось військових конвенційних сил, сил спеціальних операцій, сил нетрадиційних, якихось неконвеційних, а також проксі-сил. Це військова складова. Невійськова складова – це політичні, економічні чинники, це кіберпростір і медіа-простір. Сюди входять пропаганда, інфовійни і все, що з цим пов'язано. І всі ці чинники тісно переплітаються. Найнебезпечніше і найдивовижніше для військових у цій війні – це те, що на застосування одним ворогом одного з чинників, інший відповідає зовсім іншим. Асиметрія є головною ціллю, а головне, чим ми користуємося – полі-

[1] Долженко О. О. Концептуальні засади та понятійно-категоріальне визначення «гібридної війни» в контексті загроз національній безпеці України. *Гілея.* 2018. Вип. 128. С. 315-317.

[2] Долженко О. О. Концептуальні засади та понятійно-категоріальне визначення «гібридної війни» в контексті загроз національній безпеці України. *Гілея.* 2018. Вип. 128. С. 315-317.

[3] Так що ж таке гібридна війна? І чи гібридна війна в Україні? 18 липня 2017. URL: https://www.armyfm.com.ua/tak-shho-zh-take-gibridna-vijna-i-chi-gibridna-vijna-v-ukraïni/

тичний простір. І це досить ефективно. Ми не перші, ми не останні, але це доволі ефективно, це дозволяє нам чинити реальний опір тій агресії, яка відбувається. Фактично на якісь перемоги ворога на полі бою, ми відповідаємо рішенням політичних, економічних, інформаційних сил… І так само робить наш ворог. І це є гібридна війна.

Відтак далі доцільно розмежувати категорії «гібридна воєнна війна» і «гібридна війна – загальне явище».

У першому випадку йдеться про «гібридність» війни як збройного конфлікту – конструкту, що виник на традиційному підґрунті, а тепер трансформується внаслідок використання нових методів, форм і засобів воєнних дій («моногібридна війна»).

У другому випадку – мається на увазі «гібридність» війни у широкому сенсі – як соціального конфлікту, протистояння держав, спільнот, суспільств, цивілізацій. Війна у такому сенсі охоплює також «воєнну війну» (збройний конфлікт), але може відбуватися взагалі без застосування традиційної зброї, але із застосуванням інших засобів впливу (примусу) підпорядкування однієї сторони конфлікту іншій його стороні («полігібрида війна»).[1]

Критерієм розмежування як моногібридної й полігібридної війни, так і класифікації другої є: 1) мета (цілі), 2) мотивація (потреби, очікування), 3) умови (середовище, сфера), 4) засоби (інструменти, методи), 5) результат.

З них найбільш важливими для прагматичних класифікацій є середовище (сфера), де йде протиборство (війна), і засоби (інструменти, методи) протиборства (війни).

Із врахуванням названих критеріїв можуть бути виокремлені наступні види «полігібридної» війни (перелік орієнтовний і, звісно, не може бути вичерпним): 1) воєнна (терміну «війна» часто уникають, використовуючи позначення «визвольний похід», «братська допомога», «інтернаціональний обов'язок», «уведення обмеженого контингенту», «СВО» тощо); 2) інформаційна; 3) релігійна; 4) економічна; 5) юридична; 6)ідеологічна; 7) культурна; 8) психологічна; 9) історична; 10) дипломатична; 11) кібернетична; 12) технологічна та ін.

Отже поняття гібридної війни є родовим і охоплює низку видів протистояння, зокрема протистояння у вигляді збройного конфлікту, ко-

[1] Так що ж таке гібридна війна? І чи гібридна війна в Україні? 18 липня 2017. URL: https://www.armyfm.com.ua/tak-shho-zh-take-gibridna-vijna-i-chi-gibridna-vijna-v-ukraïni/

тре також іменують просто – «війна», що, на наш погляд, є неточним (можемо умовно називати її «воєнна (але краще – «мілітарна») війна».

Характеризуючи гібридну війну, будемо спиратися на твердження К. фон Клаузевіца: «війна... це, передусім, «акт насильства, який має на меті змусити противника виконати нашу волю».[1]

Коментуючи цю тезу, Реймон Арона зазначав: «формула Клаузевіца … констатація очевидного факту: війна – не мета в собі, воєнна перемога – так само. Торгівля між державами не припиняться в той день, коли заговорять гармати, воєнна фаза вкладається в послідовність взаємин, що завжди підпорядковані тим намірам, які спільнота мають одна щодо одної. Підпорядкування війни політиці, як інструмент підпорядковується меті … лежить в основі і є виправданням різниці, яку ми проводимо між війною абсолютною і війнами реальними. … реальні війни тим більше наближаються до війни абсолютної, чим більше насильство вислизає з-під влади керівника держави. … Щоразу, коли входять у суперечність великі інтереси, війна наближається до своєї ідеальної форми. Клаузевіц... нагадує керівникам війни та миру принцип, що його повинні шанувати і ті, й ті: першість має належати політиці, війна – це лише інструмент для досягнення цілей, визначених політикою, один момент або один аспект відносин між державами, кожна держава має підпорядковуватися політиці, тобто розумінню довготривалих інтересів спільноти».[2]

Спираючись на такі засади розуміння сутності війни, розглянемо далі особливості сучасного розуміння її та гібридної війни, попередньо зауваживши, що в нашій країні дослідження цієї категорії були особливо популярними у перші роки після початку російської збройної агресії в Україні,[3] зі зниженням інтересу протягом часу

[1] Карл фон Клаузевіц. Природа війни. пер. Руслан Герасимов. Харків: Vivat, 2018. С. 8-11.

[2] Арон, Реймон. Мир і війна між націями: Пер. фр. К.: Юніверс, 2000. С. 47.

[3] Магда Є. Гібридна війна: вижити і перемогти. Харків: Віват, 2015. 304 с.; Почепцов Г. Гібридна війна: інформаційна складова. Media Sapiens. 2015. URL: http://osvita.mediasapiens.ua/trends/1411978127/gibridna_viyna_informatsiyna skladova/; Пьювельде Д. Гибридная война – существует ли она вообще? NATO Review. 2015. URL: https://www.nato.int/docu/review/ru/articles/2015/05/07/gibridnaya-vojnasushchestvuet-li-ona-voobshche/index.html; Світова гібридна війна: український фронт: моногр. За заг. ред. В. П. Горбуліна. Харків : Фоліо, 2017. 496 с.; Тараненко М. Гібридна війна в Україні: історія та сучасність. *Вісник НТУУ «КПІ»*. Політологія. Соціологія. Право. 2016. Вип. 3/4 (31/32). С. 190-200. URL: https:// ela.kpi.ua/bitstream/123456789/25058/1/VPSP2016-3-4_190–200.pdf; Яворська Г. Гібридна війна як дискурсивний конструкт. Strategic priorities. 2016. № 4 (41). С. 41–48. URL: http://ippi.org.ua/sites/default/files/yavorskaya.pdf

АТО і ООС[1] і констатувавши недостатню активність дослідників після початку повномасштабного російського вторгнення 24.2.2024 року (хоча сама тема залишилась злободенною, але увага до неї науковців знизилась, – можливо, через триваліше оформлення публікацій).

Наразі врахування позицій фахівців у цій галузі полегшується появою низки праць оглядового характеру. Зокрема, такою працею є розвідка Ж. Павленко та А. Антонова 2023 року «Гібридна війна»: аналіз визначень поняття».[2] Її автори слушно зазначають, що наукові доробки щодо проблематики здійснюються здебільшого в межах воєнних та політичних наук, хоча ці дослідження вимагають у першу чергу глибокого й ретельного філософського, зокрема логіко-методологічного, осмислення з метою конструювання поняття «гібридна війна».

Погоджуючись з цією тезою, разом із тим зауважимо, що автори послуговуються популярними, але хибними, як на наш погляд, уявленнями про співвідношення роду та виду при характеристиці цих понять, коли пишуть: «Неможливо зрозуміти поняття «гібридна війна» без його родового поняття – «війна». При цьому остання розглядається ними як феномен «суттєвими ознаками якого вважається організована збройна боротьба між державами, суспільними класами тощо; конфлікт, що здійснюється силою зброї, як між країнами, так і між сторонами всередині країни; період збройної ворожнечі або активних військових операцій, що здійснюються наземним, морським або повітряним шляхом». До того ж вони посилаються на авторів, які

[1] Воєнні аспекти протидії «гібридній» агресії: досвід України: моногр. За заг. ред. А. М. Сиротенка. Київ: НУОУ ім. Івана Черняховського, 2020. 176 с.; Соколов Б. Гібридна війна в дії. День. 11 листопада 2021. URL: https://day.kyiv.ua/ uk/article/den-planety/gibrydna-viyna-v-diyi; Bratko A., Zaharchuk D., Zolka V. Hybrid warfare – a threat to the national security of the state. Revista de Estudios en Seguridad Internacional. 2021. Vol. 7, № 1. P. 147–160. URL: http://www.seguridadinternacional.es/revista/; Osiichuk M., Shepotylo O. Conflict and well-being of civilians: The case of the Russian-Ukrainian hybrid war. Economic Systems. 2020. Vol. 44(1). С. 1–31. URL: https://www.sciencedirect.com/science/article/pii/S0939362518303960; Tkachuk I., Shynkarenko R., Tokovenko O., Svorak S, Lavoryk A. Hybrid threats and the transformation of the state political institute: a neo-institutional approach. Journal of interdisciplinary research. 2021. Special Issue, № 11/01-XVI. URL: http://www.magnanimitas.cz/ADALTA/110116/papers/A_05.pdf

[2] Павленко Ж., Антонов А. «Гібридна війна»: аналіз визначень поняття. *Вісник Національного юридичного університету імені Ярослава Мудрого.* Серія: філософія, філософія права, політологія, соціологія. 2022. № 2 (53). С. 106-119.

«вказують родовим до поняття «гібридна війна» поняття «збройний конфлікт» (Г. Яворська) і трактують війну як насамперед фізичний, матеріальний феномен.[1]

Насправді, навпаки: «гібридна війна» тут є родовим поняттям щодо поняття «війна – збройний конфлікт».

Розуміння гібридної війни як категорії, родової щодо поняття «війна-збройний конфлікт», має місце і в працях українських науковців. Скажімо, Є. Магда пропонує таке бачення змісту феномену війни: «Очевидно, що війна – це не лише безпосередньо бойові дії, але і конкуренція економік, способів життя і мислення правителів, змагання систем державного управління, сутичка потенціалів і протистояння ідеологій».[2]

Можна припустити, що чинником розуміння поняття війни як родового (ширшого) щодо гібридної війни стало не зовсім коректне тлумачення позиції низки зарубіжних авторів, котрі торували шлях до теоретичних побудов сучасного концепту.

Зокрема, Ж. Павленко та А. Антонова ведуть мову про «концепцію «гібридного» типу війни» (hybrid warfare).[3] Разом із тим, далі вони зауважують, що «… термін «hybrid warfare» буквально означає «гібридні засоби ведення війни».[4]

На наш погляд саме другий з наведених варіантів переклад є більш точним. Його переваги помітні й при аналізі висловлювань зарубіжних авторів, які наводяться та аналізується далі у цій науковій розвідці. Для нас є важливим зазначити, що формулювання більшості з них укладаються у концепцію «гібридна війна – родове поняття, що охоплює різні види війни».

Застосовність такої концепції легко проглядається на досвіді України. Російські операції в Україні порівнюють із китайською концепцією війни без обмежень, (котра, як на наш погляд, за своєю суттю є війною гібридною, бо містить дуже багато невійськових інструментів). І одній, і другій властиві однотипні елементи: інвестиції, купівля медіа, підтримка політичних партій, розвідувальне проникнення в європейські структури, встановлення зв'язків між релігійними інституціями, використання нерозв'язаних етнічних конфліктів,

[1] Павленко Ж., Антонов А. «Гібридна війна»: аналіз визначень поняття. С. 110.
[2] Магда Є. В. Гібридна війна: вижити і перемогти, Х.: Віват, 2015. С. 12.
[3] Павленко Ж., Антонов А. «Гібридна війна»: аналіз визначень поняття. С. 107.
[4] Павленко Ж., Антонов А. «Гібридна війна»: аналіз визначень поняття. С. 108.

підтримка російських засобів інформації за кордоном (типу Russia Today), координовані кібератаки.[1]

Але маємо зауважити, що першість у створенні концепції гібридної війни ведуть американці, котрі у пошуках засобів боротьби з міжнародним тероризмом звернули увагу на доцільність акценту «невоєнних операцій» (Operations Other Than War) за тісної взаємодії з недержавними акторами та медіа-середовищем. Це радикально змінювало підходи до військової стратегії – щонайменше, першочергові цілі ударів обиралися тепер виходячи із подальшого «потрібного» інформаційного «резонансу» таких дій.

Ці стратегії пройшли перевірку під час операції «Буря в пустелі» (1991 р.), яка засвідчила ефективність використання інформаційно-психологічного інструментарію Збройних сил США, а потім використовувалися їхніми європейськими союзниками практично в усіх наступних військових операціях кінця XX – початку XXI ст. Першою жертвою війни ставала інформаційна інфраструктура противника: вороже суспільство отримувало вже спеціально підготовану інформацію. Новий етап розвитку ця концепція отримала після трагічних подій 11 вересня 2001 року, коли головним противником стали розосереджені, горизонтальні мережі терористичних груп з автономними «комірками», без жорсткої вертикалі управління «країна-спонсор – лідер угруповання – польові командири – бойовики». Для боротьби з таким противником був потрібен новий інструмент, який би обов'язково враховував і нову інформаційну реальність світу «Інтернету 2.0». Так з'явилася нова концепція інформаційно-психологічного протиборства, яка дістала назву Мережно-центричне протиборство (Network-Centric Warfare – NCW).

Фактично ці ідеї стали методологічним підґрунтям застосування кіберзброї у гібридних війнах, як «війнах не за правилами», де будь-які інформаційні технології, зокрема кіберзброя, також можуть використовуватися «не за правилами».

Разом із тим, такий висновок не дає відповіді на питання про «конвенційність» кіберзброї у війнах, які ведуться «за правилами» (конвенційних війнах). Позитивна відповідь на це питання означає, що за-

[1] Гібридна війна: інформаційна складова. Георгій Почепцов. 25 жовтня 2015. URL: https://ms.detector.media/mediaanalitika/post/14501/2015-10-25-gibrydna-viyna-informatsiyna-skladova/

стосування кіберзброї – нормальне явище, тоді як негативна – взагалі ставить застосування кіберзброї «поза законом» і дає підстави розглядати її використання у конвенційних війнах як воєнний злочин.

Конвенційна війна, конвенційна зброя і питання «конвенційності» кіберзброї

Як зауважили Вілл та Аріель Дюрант, війна належить до історичних констант; вона не підвладна ані цивілізації, ані демократії. Протягом 3421року писаної історії людства лише 268 років минуло без війни. «Причини війни ті самі, що змушують окремих людей змагатися між собою. Усі наші інстинкти, притаманні також державі, причому в цьому масштабі вони нічим не обмежені. Окрема особистість мусить зважати на обмеження, які накладають на неї мораль і закон, і погоджується замість бійки вдаватися до переговорів, позаяк держава гарантує, що її життя, майно та юридичні права на базовому рівні будуть захищені. Держава ж не визнає для себе жодних обмежень: або вона достатньо міцна, щоб покласти край будь-яким спробам утрутитися в її волю, або ж не існує жодної наддержави, яка могла б запропонувати їй такий захист, а також міжнародного законодавства чи морального кодексу, які мали б реальну силу», – проводять вони паралель, яка нам до вподоби.[1]

Всеохопність феномену війни, гібридної за суттю, цілями, формами, проявами та засобами, значно ускладнює або й робить неможливим правовий вплив на її учасників та сторонніх (приватних) осіб, що потрапили до сфери її впливу.

Спроби надати цьому явищу якихось правових рамок вживалися від давніх часів. Але створюється враження, що у Стародавньому світі ці зусилля були спрямовані головним чином на правове забезпечення підготовки до війни, а не якесь її обмеження.Показовим у цьому сенсі є слідування у Стародавньому Римі, з його прагненням юридичного облаштування світу, гаслу «Si vis pacem para bellum». Принагідно зауважимо, що Пентагон високо цінує уроки Риму щодо військової справи. Означимо далі кілька важливих моментів, скорис-

[1] Дюрант В., Дюрант А. Уроки історії людства як продукту людського досвіду. Пер.з англ. Г. Пшеничної, Х.: Віват, 2022. С. 126-127.

тавшись для цього висновками статті Ноя Шахтмана,[1] присвяченої дослідженню 8 Управління мережевої оцінки Пентагону «Військова перевага в історії», завершеного в 2002 році дослідниками, що фінансуються Net Assessment. Мета дослідження «розглянути «ключові гегемоністські сили», щоб зробити висновки про те, як Сполучені Штати «повинні думати про збереження військової переваги в 21 столітті». В ньому «у надзвичайному уривку дослідження наводиться римський досвід – понад тисячолітню давність – як прецедент довгострокового домінування Америки»: «Римська модель передбачає, що Сполучені Штати можуть зберігати свою військову перевагу протягом століть, якщо вони залишаться здатними трансформувати свої сили до того, як супротивник зможе розвинути контрспроможність. Трансформація в поєднанні з сильними стратегічними інститутами – це потужна комбінація, яку супротивник має подолати». Відтак важливість стратегії полягає в тому, що підкреслюється значення сильних стратегічних інститутів та трансформації для збереження військової переваги.[2]

Разом із тим, попри значення війн у бутті людства і прагнення не надто часто апелювати до міжнаціональних фобій у Європі поза періодом релігійних війн ХУІ ст.[3] міждержавних стосунках протягом століть відносини війни і миру залишалися невпорядкованими. Аж до Вестфальського миру 1648 року.

Попри розбіжності у розумінні понять війни і миру у політичних, філософських і правових сенсах, деякі автори вважають, що «вони тим не менш можуть бути визначені доволі чітко. Війна має розумітися як насильницьке вирішення конфлікту між державами – а не як гоббсівський стан тривалої невизначеності. Мир вимагає щонайменше відсутності війни. Якщо ми не сприйматимемо мир як протилежність війни, то можливо визначити його через ознаки відсутності ворожнечі, або ж, що ще краще, через порядок альтернативного вирішення конфліктів. Між цими двома поняттями є третє, яке у кантівських термінах може бути назване припиненням вогню. Під час припинення вогню не відбуваються насильницькі дії, однак немає й жодного іншого способу вирішення конфлікту. Поширення поняття війни на терористичні акти й контртероризм заперечує новочасне обмеження

[1] Ной Шахтман. URL: Військове навчання чекає на уроки в Римі | ПРОВОДОВИЙ (wired.com)

[2] wired.com

[3] Дюрант В., Дюрант А. Уроки історії людства як продукту людського досвіду. С. 128.

кола можливих суб'єктів державами, а тому несе ризики легітимації ерозії гуманізму під час війни, так само як і ерозії принципу суверенітету й розмежування кримінального права і права війни… все ж більш адекватним підходом є вирішення проблеми транснаціонального тероризму в термінах миру, коли насильницькі акти юридично караються в порядку альтернативного вирішення конфліктів, а не в термінах війни і миру, що може призвести до емоційної, а не раціональної легітимації риторики ворожості».[1]

У спрощеному вигляді війну визначають як «соціально-політичне явище, пов'язане з докорінною зміною характеру відносин між державами, народами, націями, класами і соціальними групами та переходом протиборчих сторін від застосування ненасильницьких форм і способів боротьби до прямого застосування зброї та інших насильницьких засобів для вирішення певних суспільно-політичних, економічних, ідеологічних, а також національних, релігійних, територіальних та інших протиріч.

При цьому, попри розмаїття поглядів на війну, загальновизнаним є її зв'язок з політикою. В їх складній взаємозалежності визначальними є соціально-політичні чинники. Глибинні причини, справжній механізм виникнення війни зумовлюється багатофакторним комплексом причинно-наслідкових зв'язків, вкрай загостреними суперечностями, які вже не можуть бути вирішені політичними засобами, без застосування насильницьких засобів. Отже, мають місце певні розбіжності у трактуванні поняття війни, які відповідають різним науковим парадигмам, але за суттю вони однакові».[2]

Спираючись на такі засади розуміння сутності війни, далі торкнемося «права війни», як результату визнання певної сутності війни і юридичної основи визначення характеристики війни, як правової категорії.

Насправді виглядає досить ризикованим братися до проблем характеристики «права війни» на тлі існування фундаментальної праці Джеффрі Беста «Війна та право після 1945 р.».[3]

---

[1] Філіп Гізбертц. Поняття «мир» і «війна в контексті транснаціонального тероризму. *Філософія права і загальна теорія права.* 2019. № 1. С. 214.

[2] Локальна війна і воєнний конфлікт: сутність понять та їх типологія. Реферат.URL: Локальна війна і воєнний конфлікт: сутність понять та їх типологія. Реферат – Освіта.UA (osvita.ua)

[3] War and Law Since 1945 by Geoffrey Best. Oxford: Clarendon Press, 1994. 434 pp.

У детальній рецензії авторитетного фахівця зазначається, що ця книга є роздумом вченого, який не є юристом, озброєного «сумішшю шматочків усіх так званих академічних дисциплін», на тему, яка «містить у собі надто багато людської крові та майбутнього, щоб її можна було безпечно довірити піклуванню будь-якої з кількох сторін, які мають претензії до неї».

Увага, яка приділялася праву війни до 1945 року, вказує на те, що це питання належить не лише до атомної ери Статуту ООН. Міждисциплінарний контрапункт, який є сильною стороною цієї книги, мабуть, найкраще оцінений у цьому турі по горизонту права та війни до 1945 року.

Доктор Бест інтегрує філософські та теоретичні основи небойового імунітету з практикою держав дев'ятнадцятого та початку двадцятого століть, протягом яких відбулися значні зміни в технологіях та військовій стратегії. Блокада і бомбардування нової національної держави розмили різницю між комбатантами і цивільним населенням, оскільки морські міни, підводні човни, далекобійна артилерія, а потім і літаки принесли більш потужні засоби в руки політичних і військових лідерів, і, за іронією долі, громадяни-солдати Руссо і колективна «нація зі зброєю» розширили сферу застосування законних цілей і розмили різницю між цивільними і воюючими сторонами. Соціологія вступила в змову з політикою, підкріпленою технологіями, щоб підірвати філософію і право, і призвела до ситуації, коли «після закінчення Другої світової війни стало ясно, що мирні жителі в тотальній війні не можуть розраховувати на імунітет ні у відкритому морі, ні на заблокованій землі».

Д-р Бест представляє генезис текстів відповідних договорів, укладених у період, що розглядається, насамперед чотирьох Женевських конвенцій 1949 року та двох Додаткових протоколів 1977 року, з відповідною екзегезою ключових положень у контексті.

Він розповідає історію переговорів щодо монументальних Женевських конвенцій з пильним поглядом на поступки багатосторонньої дипломатії, яка різко висвітлює отримані положення.

На завершення свого великого огляду війни та права д-р Бест розмірковує про місце та корисність міжнародного гуманітарного права у пом'якшенні жорстокості збройних конфліктів. Він зауважує, що «ми, хто вірить у [міжнародне гуманітарне право] або хоче вірити

в нього, недостатньо усвідомили його обмеженість і знехтували достатньою кількістю (більш вимогливих) інституцій, які з інших напрямків наближаються до тієї ж мети: уникнення війни і, якщо це неможливо, поміркованість її ведення». Він виступає за зміцнення регіонального та міжнародного права та організацій, які можуть запобігти виникненню збройних конфліктів і які можуть швидко застосувати силу, щоб зупинити тих, хто це робить. Ці альтернативні засоби досягнення обіцянок права війни ще раз підкреслюють необхідність міждисциплінарного підходу до врегулювання збройних конфліктів, у який д-р Бест зробив важливий внесок.[1]

Враховуючи викладене і не вважаючи себе фахівцями з питань міжнародного права, але прихильниками міждисциплінарного підходу, далі дозволимо собі обмежитися викладом тих загальних положень, які безпосередньо стосуються проблематики нашого дослідження, взявши за основу концепцію та окремі концепти зі згаданої книги Дж. Беста і для зручності об'єднавши їх у кілька тез.

Теза перша. Право – не єдиний засіб, що має людство, для зменшення масштабу і пом'якшення наслідків насильства, але воно здається – не в останню чергу завдяки його тісним зв'язкам з релігією та етикою, – одним з найбільш вартих уваги засобів /заходів, що набув останнім часом значної популярності завдяки стурбованості сучасного суспільства питаннями гуманності та прав людини.

Теза друга. Слабким місцем міжнародного права є те, що воно – це в першу чергу право, що визначає стосунки між державами, створене державами для своїх цілей і заради власних переваг; Тобто, якщо держави бажають порушити або обійти норму права, то немає сили, яка б мала повноваження їм завадити.

Теза третя. Значна частина міжнародного права, зокрема у гуманітарній сфері і сфері захисту прав людини, особливо там, де задіяна Генеральна Асамблея ООН, має «нормативний» характер, що дає підстави розглядати далі термін «Право» у двох сенсах, а саме: те, чого дотримуються і що підкріплюється санкціями тут і зараз; і те, чого мають дотримуватися і що підкріплюється санкцією у майбутньому – у тому майбутньому, якого варто прагнути. З цим розще-

[1] «Війна і закон з 1945 року» Джеффрі Беста. Оксфорд: Кларендон Прес, 1994. 434 с. Рецензія-огляд: Університет Ессекса ДЖЕЙМС ДЖ. С. 88-89. URL: https://journals.sagepub.com/doi/pdf/10.1177/004711789501200407

пленням понять намагалися упоратися, придумавши два види права: «жорстке» і «м'яке». Різниця між ними в тому, що коли у першому випадку наразі існує певна можливість карати за порушення правової норми, то в другому випадку така можливість відсутня.

Теза четверта. З погляду оцінки його джерел міжнародне публічне право відоме також з більш повною назвою «міжнародне право миру, війни і нейтралітету»; шляхи, яке воно проходить: «Грандіозний лабіринт, але не позбавлений плану». Ідея верховенства права у міжнародних відносинах стосується війни так само, як і миру, а у міжнародному праві війни ця ідея втілюється. Право війни ніколи не діяло так само ефективно, як зазвичай діє право миру. Але розумна цивілізована людина і не чекає іншого. Це менше зло; у кожному разі це краще, ніж нічого.

І нарешті, ми хочемо приєднатися до Дж. Беста у обранні висловлювання Герша Лаутерпахта у Британському Щорічнику Міжнародного Права (1952. С. 382) для ключової характеристики міжнародного права і права війни: «Якщо можна сказати, що міжнародне право знаходиться у певному сенсі на тій межі, за якою закінчується право, то мабуть, ще більш очевидним було б твердження, що право війни знаходиться на тій межі, за якою закінчується міжнародне право».[1]

З таких позицій ми можемо оцінити здобутки «права війни» у конкретизації поняття власне війни. Філіп Гізбертца своє дослідження починає з констатації того, що «У політичному й правовому сенсі найбільш впливовими подіями для формування понять війни і миру в ранню модерну добу стали Тридцятилітня війна (1618-1648 рр.) й укладення Вестфальського миру», що складався з двох договорів», головне значення яких полягає у тому, що в них «щонайменше містяться норми щодо заборони сили й щодо публічної монополії на легітимне застосування фізичної сили».[2]

Утім ця подія не завадила ідеалізації війни у XIX ст., коли Гегель наполягав на тому, що «війна приносить внутрішню цілісність та спокій і є необхідним засобом вирішення конфліктів, які неможливо вирішити мирно. Звідси, війна є необхідним морально цінним інстру-

[1] Харитонов Є., Харитонова О. Приватне право як концепт. Том VI. Приватне право в умовах гібридної війни: монографія. Одеса: Фенікс, 2024. С. 87-93.

[2] Філіп Гізбертц. Поняття «мир» і «війна» в контексті транснаціонального тероризму… С. 205.

ментом, і лише у війні держава як колектив підтримує свою моральну якість і цілісність».

Водночас зі згаданими процесами, у розвитку міжнародного права у ту добу відбувається «зустрічний рух»: перші спроби гуманізувати війну в міжнародному праві (праці Ф. Найтінгел, заснування Міжнародного Комітету Червоного Хреста, укладення І Женевської конвенції 1864 року і Гаазьких конвенцій 1899/1907 років. Навіть висловлюються досить категоричні твердження, що «після досвіду двох світових війн міжнародне право … більш не обмежене встановленням гуманітарних правил і стає міжнародним режимом попередження й заборони війни».

Однак такі висловлювання, як і сподівання, виявилися помилковими, хоча для них, здавалося, існувало достатньо надійне підґрунтя: з 1871 по 1914 рік Європа насолоджувалася періодом відносного спокою (котрий, озираючись назад, зазвичай іменують «Прекрасною епохою», «Золотим віком») – періодом, коли «європейська цивілізація досягла своєї найбільшої сили у світовій політиці, а також мала максимальний вплив на народи за межами Європи»,[1] демонструючи оптимізм, технічний прогрес, гарні економічні умови, художні досягнення, культурний прогрес.

Але, попри встановлення міжнародного права та Гаазький трибунал, які мали слугувати механізмами вирішення міжнародних суперечок, зміцнення миру, сприйняття їх як провісників періоду, який, здавалося б, вийшов за межі жорстокості війни, ідилічна «Бель Епок» розлетілася вщент влітку 1914 року з початком військових дій[2] між Австро-Угорщиною та Королівством Сербія після вбивства ерцгерцога Франца Фердинанда[3]. Оголошення війни на тлі ескалації напруженості спричинило ланцюгову реакцію, яка занурила Європу, а згодом і світову спільноту, у затяжний і руйнівний конфлікт, який тривав роки, супроводжуваний кровопролиттям і стражданнями.

У підсумку Перша світова війна, яку зазвичай називають Великою війною, стала добою глибоких потрясінь, зумовлених тим, що великі

[1] Palmer, Robert Roswell (20 вересня 2013). *Історія Європи в сучасному світі.* Колтон, Джоел, Крамер, Ллойд С. (11-е вид.). Нью-Йорк, Нью-Йорк. ISBN 978-0076632855. OCLC 882719311

[2] Австро-Угорщина оголосила війну Сербії | 28 липня 1914 | ІСТОРІЯ (history.com)

[3] Чи призвело це вбивство-самогубство до вбивства Франца Фердинанда і початку Першої світової війни? | Вінтажні новини (thevintagenews.com)

держави вступили в інтенсивні та смертоносні протистояння, попри існування згаданих Конвенцій, ба більше, навіть, попри особисті зусилля пом'якшити ескалацію конфлікту кайзером Німеччини Вільгельмом і російським царем Миколою II».[1]

Велика війна, здавалося, стала катарсисом, одним з найбільш помітних проявів якого стала поява «втраченого покоління», а відтак, пов'язаних з ним політичних, соціальних, літературних та мистецьких феноменів.[2]

Переосмислення трагічного досвіду Першої світової не вберегло людство від Другої світової війни, але, усе ж, сприяло тому, що з пактом Бріана-Келлога (1928) і формуванням ООН (1945) загальна заборона насильства стає частиною міжнародного права.

Поняття війни майже повністю витісняється поняттям збройного конфлікту. Відтак протягом практично усієї другої половини XX ст. фахівці у різних галузях прагнули чітко з'ясувати різницю між поняттями «війна» і «збройний конфлікт», сподіваючись, що це дасть змогу узгодити концепти «право війни» та «право збройних конфліктів», а також низку похідних категорій і понять гуманітарного права в умовах суперечливих процесів глобалізації та глокалізації.

Оголошення війни тягне для держав – її учасників – настання певних наслідків: розірвання дипломатичних відносин та припинення консульських стосунків між цими державами; анулювання двосторонніх договорів, зокрема політичних; призупинення дії багатосторонніх міжнародних договорів для воюючих сторін (зберігають чинність договори у сфері захисту прав людини, гуманітарного права, про кордони тощо); припиняються будь-які економічні, торгові, фінансові взаємини між фізичними та юридичними особами країни противника; торгові судна сторін, які на момент початку війни знаходяться в порту держави противника, можуть бути реквізовані або затримані до кінця війни незалежно від того, належать вони державі, фізичним чи юридичним особам; до громадян держави противника застосовується спеціальний правовий режим (інтернування), пов'язаний з частковим обмеженням прав людини.

[1] Кайзер Вільгем і цар Микола II намагалися (і не змогли) відвернути Першу світову війну (англ. мовою). 16 квітня 2024 р. Нікола Буданович. URL: https://www.warhistoryonline.com/world-war-i/willy-nicky-telegrams.html

[2] Олександр Андрієвський. І мертві, і живі, й непроговорені: літературне покоління Першої світової. В кн.: Втрачене покоління. Антологія. К. Стилет і стилос. 2021. С.5-15.

Повоєнний досвід свідчить, що чимало великих держав, які «de jure» проголосили принципи демократії та поваги до норм міжнародного права, не раз розпочинали великі війни чи збройні конфлікти, не оголошуючи про їх початок. Пояснення таких фактів не становить особливих труднощів, оскільки застосування терміну «війна» вимагає формального її оголошення, що тягне за собою згадані вище наслідки, а також створює ризик притягнення до міжнародно-правової відповідальності (ст. 5 визначення агресії, яке прийняте Генеральною Асамблеєю ООН 14 грудня 1974 р.).

Відтак класична характеристика війни доповнюється інтерпретаціями її поняття, як комплексу заходів, спрямованих на захоплення чужих природних, енергетичних та людських ресурсів, де перетинаються такі категорії як «збройний конфлікт», «військова експедиція», «інцидент», «інтервенція», «спеціальна військова операція» та ін.

Разом із тим, хоча у Женевських конвенціях і Додаткових протоколах досить часто зустрічається термін «збройний конфлікт», у цих документах немає визначення цього поняття. Відсутність його супроводжується певними як теоретичними, так і практичними труднощами щодо уніфікації його застосування. У загальній ст. 2 Женевських конвенцій зазначається, що «ця Конвенція застосовуватиметься в разі оголошення війни або під час будь-якого іншого збройного конфлікту, який виник між двома або декількома Високими Договірними Сторонами, навіть у тому випадку, якщо одна з них не визнає стану війни».

Отже, якщо виникає збройний конфлікт між двома або декількома державами, то міжнародне гуманітарне право стає чинним автоматично, незалежно від того, чи оголошено війну і чи визнають учасники конфлікту стан війни. Єдиною підставою, достатньою для застосування гуманітарного права, є наявність збройного конфлікту.

Будь-який спір, що виникає між державами і призводить до застосування збройних сил, вважається збройним конфліктом, навіть якщо одна зі сторін заперечує наявність стану війни. Згідно зі ст. 2, загальною для Женевських конвенцій, під конфліктом розуміють будь-яке зіткнення між двома або більше державами із застосуванням збройних сил. При цьому не має значення ані тривалість конфлікту, ані кількість жертв. Навіть незначного прикордонного інциденту досить, щоб ситуацію визнали збройним конфліктом.[1]

[1] Поняття війни та збройного конфлікту – Міжнародне публічне право. Навчальні матеріали онлайн. URL: pidru4niki.com

Отже межа між «війною» і «збройним конфліктом» досить умовна, хоча такий поділ має значення для права, що застосовується під час збройних конфліктів. При цьому вважається, що поняття «збройний конфлікт» є ширшим і включає поняття «війна». Але не кожний збройний конфлікт можна називати війною, оскільки між ними існують відмінності змістовно-формального характеру: у випадку війни – це вимога певного суб'єктного складу – між двома державами, або між двома групами держав, або між державою і групою держав, який супроводжується здебільшого розірванням дипломатичних відносин, подальшим призупиненням застосування загальних норм міжнародного права мирного періоду і загальною рішучістю вчинити насильницькі дії, навіть якщо такі дії насправді не мають місця» тощо. Кваліфікуючим формальним чинником такого «стану справ» (війни) є акт оголошення війни (III Гаазька конвенція 1907 р.). Початком війни вважається момент фактичного відкриття воєнних дій або формального оголошення війни, навіть якщо за цим практично не почалися воєнні дії. [1]

Оскільки стосовно дій росії в Україні часто вживається термін «агресія», зауважимо його відмінності від позначення «війна». Зокрема Резолюція Генеральної Асамблеї ООН 3314 (XXIX) «Про визначення агресії» – від 14 грудня1974 року та поправки до Статуту Міжнародного кримінального суду, схвалені 11 червня 2010 року, передбачають, що, незалежно від того, оголошено війну чи ні, актом агресії, поміж інших дій, кваліфікованих як агресія, – є «Засилка державою або від імені держави озброєних банд, груп, нерегулярних сил чи найманців, які застосовують збройну силу проти іншої держави» (пункт «g» ст. 3 згаданої Резолюції та пункт «g» ст. 8 bis Статуту Міжнародного кримінального суду).[2] Таким чином, відмінною ознакою агресії можна вважати те, що у випадку застосування збройної сили визнання її агресією не залежить від оголошення війни.

---

[1] Міжнародне публічне право. Підручник. За ред. В. М. Репецького. URL: Поняття війни та збройного конфлікту – Міжнародне публічне право – Навчальні матеріали онлайн (pidru4niki.com)

[2] Василенко Володимир. На війні як на війні: tertium non datur. Книга 3. К.: Темпора, 2020. С. 18.

Варто згадати про існування терміну «стан війни»

В українському законодавстві формулювання «стан війни» згадується всього кілька разів і докладних тлумачень щодо нього немає. У Конституції України стан війни згаданий двічі: у розділі про Верховну Раду, до повноважень якої належить «оголошення за поданням президента України стану війни і укладення миру», а також у розділі про президента, який «вносить до Верховної Ради України подання про оголошення стану війни та у разі збройної агресії проти України приймає рішення про використання Збройних Сил України». Ця ж процедура прописана і в законі Про оборону України[1].Там також зазначено, що з моменту оголошення стану війни чи фактичного початку воєнних дій настає воєнний час, який закінчується у момент припинення стану війни. Однак визначення, що таке «воєнний час», у законодавстві немає. Окрім цих трьох згадок, інших пояснень про «стан війни» в українському законодавстві немає.

У міжнародному праві про «стан війни» (state of war – англ.) вперше згадується у Конвенції про початок воєнних дій[2], схваленій у Гаазі 1907 року. За нею, про стан війни має повідомити та сторона, яка напала, а не жертва агресії: «Держави, що уклали цей договір, визнають, що воєнні дії між ними не повинні починатися без попереднього та недвозначного попередження, яке матиме або форму мотивованого оголошення війни, або форму ультиматуму з умовним оголошенням війни».

Однак ця вимога не означає, що, якщо держава формально не оголосила війну іншій, вона не вважається агресором.

Міжнародне право регламентує, які саме дії є актом агресії, незалежно від того, була оголошена війна, чи ні. Відповідно до Резолюції Генасамблеї ООН від 14 грудня 1974 року, якщо якась держава застосувала збройну силу першою – це достатнє свідчення акту агресії[3]. Тож на міжнародну кваліфікацію російської агресії наявність чи відсутність стану війни ні для України, ні для Росії не впливає.

---

1 Про оборону України | від 06.12.1991 № 1932-XII (rada.gov.ua)

2 Конвенція про початок воєнних дій. URL: IHL Treaties – Hague Convention (III) on the Opening of Hostilites, 1907 (icrc.org)

3 Визначення агресії. Затверджене резолюцією 3314 (XXIX) Генеральної Асамблеї ООН від 14 грудня 1974 року. URL: https://www.un.org/ru/documents/decl_conv/conventions/aggression.shtml

Встановлення стану «війни» та її характеристика ускладнюються тим, що погляди на війну та її соціально-політичний зміст постійно еволюціонують, а відтак потребують адаптації до сучасних військових трансформацій[1] (з урахуванням при цьому «гібридності» війни).

Нація, яка не в змозі, або ж яка не бажає сприймати новий «гібридний» вид війни, буде комфортно і далі розробляти плани в межах застарілої та черствої воєнної ідеї минулого століття, опускаючи можливість досвіду в асиметричних конфліктах. Так само і притримуючись статусу кво та застарілих тактик ведення війни, держави роблять помилкові кроки в бік розподілу державного бюджету, відкидаючи розробки нової воєнної доктрини та переробки інноваційних технологій.[2] Нераціональний розподіл державних ресурсів призводить до того, що збройні сили держави готові до ведення війни «минулого століття», але вони повністю безсилі до нових задач гібридного конфлікту.

Це стосується й права збройних конфліктів, синонімом якого є міжнародне гуманітарне право або право війни – частина міжнародного права, яка регулює та контролює дії сторін, котрі беруть участь в конфлікті. Воно складається як з договірних, так і з звичаєвих норм. Це право є основним правом, обов'язковим для учасників збройного конфлікту.[3]

Гібридизація війни поглиблює ці проблеми і може призвести до того, що право збройних конфліктів втратить своє значення як неспроможне вирішити правові питання сучасної гібридної війни, забезпечити правовий контроль та захист сторін.[4]

Якщо тенденція до розвитку права збройних конфліктів як чогось застарілого та неактуального буде зберігатися, учасники збройних

---

[1] Валіулліна З. В. Військова теорія К. Клаузевіца в теоретичному дискурсі. *Ефективна економіка.* 2017. № 11. URL.: http://www.economy.nayka.com.ua/?op=1&z=5881

[2] The origins of the concept of a hybrid war. *Electronic journal «The Bell»*28 Feb. 2015. URL: http://www.thebellforum.com/showthread.php?t=130013

[3] Interparliamentary Conference for the Common Foreign and Security Policy and the Common Security and Defence Policy//Andis Kudors. Hybrid War – A New Security Challenge for Europe. 4-6 March 2015. Riga. URL: http://www.parleu2015.lv/files/cfsp-csdp/wg3-hybrid-war-background-notes-en.pdf

[4] Bachmann, Sascha-Dominik Oliver Vladimir and Gunneriusson, Hakan, Hybrid Wars: The 21st-Century's New Threats to Global Peace and Security (September 16, 2014). Scientia Militaria, South African Journal of Military Studies, Vol 43, No. 1, 2015, pp. 77 – 98. URL: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2506063

конфліктів, а також і все міжнародне співтовариство, почне розглядати міжнародне право в якості більш анахронізму, ніж правового імперативу.[1]

Якщо авторитет права зменшиться, правові заборони будуть безкарно порушуватися і лише певні категорії моралі зможуть якось впливати на дії учасників війни. Внаслідок цього, сторони конфлікту будуть ігнорувати зобов'язання, що входять в право збройних конфліктів, та приписуватимуть титули своїм діям як самооборони чи проводитимуть маніпуляції з самим змістом права збройних конфліктів шляхом стратегічного застосування «lawfare» (асиметрична, гібридна війна).[2]

Власюк В. В., Карман Я. В. визначають поняття «гібридна війна» як сучасний вид війни, де в конфлікті використовуються різноманітні засоби нападу та оборони держав, що виходять за рамки конвенційно-визначених варіантів та видів ведення війни. При цьому зброєю вже є не тільки матеріальні традиційні її види, а й модельно-організаційна та інформаційна види зброї.

Для того щоб попередити можливості підриву зусиль, що були спрямовані на гуманізацію війни, міжнародне співтовариство має визнати, що ефективність та практичність права збройних конфліктів повинні розширюватися по мірі розвитку нового «гібридного» виду війни.

Ігнорування цієї тенденції робить сучасні правові зусилля недієвими, неефективними засобами регулювання сучасних збройних конфліктів, що підриває довіру до права збройних конфліктів. Замість продовження застарілої практики, міжнародне співтовариство має включити в право збройних конфліктів поняття «гібридна війна» та «зброя». Той, хто застосовує акти «асиметричної війни/зброї (lawfare)», має нести покарання, для уникнення їх зловживання правом. Якщо міжнародна спільнота вчинить зазначені дії, то можна

[1] Major Shane R. Reeves, Major Robert E. Barnsby The New Griffin of War. Hybrid International Armed Conflicts. *Academic joutnal article "Harvard International Review"* 2013. URL: https://www.questia.com/library/journal/1G1-316203914/the-new-griffin-of-war-hybrid-international-armed

[2] Interparliamentary Conference for the Common Foreign and Security Policy and the Common Security and Defence Policy//Andis Kudors. Hybrid War – A New Security Challenge for Europe. 4-6 March 2015.- Riga. URL: http://www.parleu2015.lv/files/cfsp-csdp/wg3-hybrid-war-background-notes-en.pdf

буде стверджувати примат міжнародного права навіть у складній гібридній війні. [1]

Однією з ознак конвенційної війни є розрізнення «конвенційної» (дозволеної) та «неконвенційної» (недозволеної) зброї. З погляду проблематики нашого дослідження це означає, що ми маємо визначити, до якої з цих категорій належить кіберзброя.

Варто зауважити існування з цього приводу різних позицій: від заперечення визнання кіберзброї «зброєю» взагалі[2] до визнання її ефективним засобом протидії кіберзагроза.[3] Втім для нас наразі це не має принципового значення, оскільки з логічного і структурно-системного тлумачення положень Гаазьких конвенцій випливає, що «конвенційною» є будь-яка зброя, яка не згадується в цих конвенціях як заборонена (неконвенційна)

Оскільки кіберзброя не згадується ні поміж одних, ні поміж інших, маємо підстави для висновку, що вона не заборонена і може використовуватися у війні, яка ведеться згідно міжнародному праву.

Разом із тим, це не усуває низку правових проблем, котрі розглянемо далі.

Кіберзброя і штучний інтелект у гібридній війні

Значення кіберзброї у сучасному світі та сучасній війні яскраво охарактеризував Девід Е. Сенгер, згадавши як через рік після вступу на посаду президента США Дональда Дж. Трампа (під час першої його каденції), міністр оборони США Джим Меттіс дав Президенту пораду: заздалегідь попередити кожну державу, яка намагатиметься завдати кіберзброєю нищівного удару найважливішій інфраструктурі Америки, що Сполучені Штати можуть навіть на неядерний

---

[1] Власюк В. В., Карман Я. В. Деякі основи поняття «гібридна війна» в міжнародному праві. URL.: АПП – науково-практичний журнал (knu.ua)
Право і громадянське суспільство – ДЕЯКІ ОСНОВИ ПОНЯТТЯ "ГІБРИДНА ВІЙНА" В МІЖНАРОДНОМУ ПРАВІ – Власюк В. В., Карман Я. В. (knu.ua)

[2] Хакер, що біжить. Блог про кібер, біг та медитацію. URL: https://styran.com/what-is-cyberweapon-and-why-there-is-no-such-thing/

[3] Кіберзброя: сучасні загрози національній безпеці та шляхи протидії. Автор(и) А. Д. Білюга Національний університет оборони України імені Івана Черняховського, Україна. *Наука і оборона.* 2021. № 2. URL.: http://nio.nuou.org.ua/article/view/239047

удар застосувати у відповідь ядерну зброю. «Як з'ясувалося, вслід за рекомендацією Пентагону з'явилися інші, в яких пропонувалося значно агресивніше застосовувати кіберзброю… Вони засвідчували, як швидко страх перед нищівними кібератаками вийшов з царини наукової фантастики та кінофільмів…і опинився у фокусі американської оборонної стратегії. [1]

«Ядерна стратегія, запропонована Трампу, відображала побоювання Пентагону, що кібератаки становлять особливу загрозу, до протидії якій Штати зовсім не готувалися, – констатує Девід Сенгер., «Іронія в тому, що США залишаються засекреченою і наймогутнішою кібердержавою світу... Однак розрив між державами скорочується. Створити кіберзброю настільки дешево, а приховати так легко, що спокуса стає непереборною».[2]

Два зауваження Девіда Сенґера, важливих для визначення акцентів нашого дослідження.

По-перше, він нагадує, що коли «десять років тому лише три-чотири країни володіли ефективною кіберзброєю, то зараз таких уже понад тридцять. Крива обсягу виробництва кіберзброї за останні десять років загалом нагадує траєкторію злету бойового літака. Нову зброю вже застосовували багато разів, навіть якщо результати були неоднозначні…

… Сучасні збройні сили будь-якої країни не можуть функціонувати без кіберарсеналу так само, як після 1918 року годі було уявити військо без літаків. Сьогодні, як і тоді, неможливо передбачити, наскільки цей винахід змінить застосування державних сил».[3]

По-друге, це нагадування-застереження: «Ми всі живемо в страху, що нашу залежність від цифрових технологій обернуть проти нас інші держави, які за останнє десятиліття знайшли нові способи продовжити давнє протистояння. Ми вже знаємо, що перед кіберзброєю, як і перед ядерною, усі рівні. І в нас є всі підстави непокоїтися, що через кілька років ця зброя вкупі зі штучним інтелектом[4] діятиме настільки швидко, що люди не встигнуть ні усві-

[1] Сенгер, Девід Е. Досконала зброя. Війна, саботаж і страх у кіберепоху. Пер. з англ. Вікторія Дєдик: фах.ред.укр.вид Олександр Дєдик і Олег Фешовець. Львів: Астролябія, 2022. С. 6-7.

[2] Сенгер, Девід Е. Досконала зброя. Війна, саботаж і страх у кіберепоху. С. 8.

[3] Сенгер, Девід Е. Досконала зброя. Війна, саботаж і страх у кіберепоху. С. 19.

[4] Підкреслено нами – Є. О., О. Х.

домити загрози, ні запобігти їй – тож атаки відбудуться і призведуть до ескалації конфлікту».[1]

Отже враховуємо цю обставину, яка зумовлює вищий ступінь загрози – такий, що може вийти з-під влади людини: поєднання кіберзброї зі штучним інтелектом. Цей випадок є головною гібридною загрозою, а відтак потребує гібридної відповіді, зокрема, шляхом юридичних заходів.

Передусім, зауважимо, що коли створення чи удосконалення кіберзброї вже за визначенням є справою непублічною, а регламентація відносин, пов'язаних з нею, є таємницею, то розробка штучного інтелекту сама по собі виглядає заняттям більш мирним, а досягнення часто стають матеріалом для обговорення у ЗМІ (хоча й переважно у популярній формі).

Разом із тим штучний інтелект може застосовуватися як кіберзброя (або – як елемент кіберзброї) у інформаційній війні (скажімо, для приховування інформації, важливої для розслідування воєнних злочинів).

Зокрема, як з'ясувала BBC, докази потенційних порушень прав людини можуть бути втрачені внаслідок їхнього видалення соцмережами, котрі за допомогою штучного інтелекту видаляють зі своїх платформ відео, що містять сцени насильства. Meta і YouTube кажуть, що у такий спосіб прагнуть захистити користувачів від шкідливого контенту.

Соцмережі наполягають, що відео із зон бойових дій можуть залишатися онлайн, якщо становлять суспільний інтерес. Проте коли BBC спробувала завантажити кадри вбивства цивільних в Україні, їх прибрали.

Штучний інтелект запрограмований автоматично видаляти шкідливий і насильницький контент. Утім, коли справа доходить до модерації відео з країн, де триває війна, машина просто не може визначити, чи ці кадри – доказ порушення прав людини. «Штучний інтелект програмували так, щоби у момент, коли машина бачить щось, що здається важким або травматичним, одразу прибирати це», – пояснює Расбріджер BBC. Раду Meta, до якої він входить, створив Марк Цукерберг. Це своєрідний незалежний «верховний суд» компанії, якій належать Facebook й Instagram.

[1] Сенгер, Девід Е. Досконала зброя. Війна, саботаж і страх у кіберепоху. С. 21.

Ігор Захаренко від початку повномасштабної війни документує вбивства росіянами цивільних, на кадрах, зафіксованих Захаренком, – щонайменше 17 тіл цивільних та згорілі автівки. Він хотів викласти відео в інтернет, щоби світ дізнався, що відбувається в Україні. Але коли завантажив кадри у фейсбук й інстаграм, їх швидко видалили.

Використовуючи фіктивні акаунти, BBC теж виклали кадри Ігоря в інстаграм і ютюб. Протягом хвилини інстаграм видалив три з чотирьох відео.

Ютуб спочатку застосував вікові обмеження до трьох відео, але за десять хвилин прибрав їх усі. Клопотання відновити відео на тій підставі, що вони містили докази воєнних злочинів, ютуб відхилив.

Компанії YouTube і Meta кажуть, що чутливий контент може залишатися в мережі, якщо він становить суспільний інтерес. Але експеримент BBC з відео Ігоря свідчить про протилежне.

Некомерційна організація Mnemonic, що базується в Берліні і займається документуванням порушень прав людини, розробила програму для автоматичного завантаження й збереження доказів потенційних воєнних злочинів. Спочатку вона це робила для Сирії, а тепер – для Ємену, Судану та України. Було збережено понад 700 тисяч відео із зон бойових дій, перш ніж їх видалили із соціальних мереж.

Але організаціям на кшталт Mnemonic бракує ресурсів. Тому архівування матеріалів з соцмереж часто лягає на плечі простих людей чи волонтерів, що ускладнює можливе притягнення до відповідальності за воєнні злочини у майбутньому».[1]

Разом із тим, ШІ може не лише видаляти інформацію, а й створювати її, викривлюючи сутність подій або створюючи події, яких не було. Про це вже йшлося у попередньому розділі, тому перейдемо далі до визначення ролі ШІ у воєнній війні.

До прикладу, ще раз згадаємо історію, котра набула широкого розголосу завдяки публікації BBC News Ukraine. Українська студентка і блогерка Ольга Лоєк виявила в китайських соцмережах свої аватари, створені штучним інтелектом, які китайською мовою розповідають

[1] Як соцмережі видаляють докази воєнних злочинів Росії в Україні. Розслідування BBC. Джек Гудман і Марія Коренюк. Відділ BBC з боротьби з дезінформацією. 1 червня 2023.URL: Як соцмережі видаляють докази воєнних злочинів Росії в Україні. Розслідування BBC – BBC News Україна

про міцну дружбу між Пекіном і Москвою, а також рекламують російські товари.

Ольга Лоєк живе в Мюнхені й навчається в Університеті Пенсільванії. У 2023 році вона завела свій YouTube-канал, де розповідає про психічне здоров'я. За деякий час дівчина почала отримувати повідомлення від підписників про те, що її бачили у китайських соцмережах. І там вона зовсім не Ольга Лоєк, а росіянка, що розмовляє китайською, яку сама Ольга ніколи не вчила. Її клон представляється Наташею чи Софією, Ейпріл чи Стейсі – залежно від соцмережі, де фігурує її обличчя. Один з найбільших акаунтів «Імпортна їжа від Наташі» має понад три млн підписників. А його господарка запевняє, що Росія – найкраща в світі країна, тож шкода, що інші держави відвертаються від неї. Вона стверджує, що російські жінки мріють приїхати до Китаю, після чого рекламує російські цукерки. Це дуже обурило Ольгу, сім'я якої мешкає в пошматованій російською війною Україні.

Але у ширшому сенсі її справа привертає увагу до ризиків технології, яка швидко розвивається і є справжньою проблемою. Ольга знайшла свої ШІ-клони на Xiaohongshu – китайській версії Instagram та на Bilibili – найбільшому китайському відеосайті, схожому на YouTube. Наразі вона виявила близько 35 облікових записів зі своїм обличчям. Клонів Ольги створили за допомогою сервісу HeyGen, що спеціалізується на реалістичних цифрових аватарах, генерації голосу та перекладах відео на різні мови.

Справа Ольги Лоєк виходить далеко за межі Китаю і показує, як складно регулювати галузь, що розвивається з шаленою швидкістю[1] і яким небезпечним засобом може бути штучний інтелект в інформаційній гібридній війні. Завдяки стрімкому розвитку і своїм унікальним можливостям генеративний штучний інтелект струшує й без того тендітний світ ЗМІ, який уже був значною мірою підірваний Web 2.0. Зокрема, п'ята версія штучного інтелекту Midjourney, яка генерує зображення дуже високої чіткості, наповнює соціальні мережі все більш правдоподібними підробками, які не відрізнити від реальності, про що свідчать напрочуд реалістичні фотографії жор-

[1] Як штучний інтелект перетворив українську блогерку на російську пропагандистку. Author,Фан Ван. Role,BBC News. 15 травня 2024. URL: Як штучний інтелект перетворив українську блогерку на російську пропагандистку – BBC News Україна

сткого затримання Дональда Трампа чи портрет Джуліана Ассанжа, який перебуває у стані овоча, стягнутий гамівною сорочкою, які стали вірусними[1]. Зрозуміло, що це дуже вигідно недемократичним режимам, зокрема рф, у її війні проти України.

Підбиваючи підсумки, зазначимо, що цифрові технології, в міру свого поступового вдосконалення і вплетіння в культурно-історичний контекст, все більшою мірою стають віртуальними, перестаючи відображати реальність і починаючи симулювати дійсність. Віртуальна реальність і симулякри не є нейтральними стосовно людини, вони змінюють психіку людей, дійсність навколо них, і, таким чином, отримують бажаний замовнику симулякру результат.

Використання штучного інтелекту у «мілітарній війні» ускладнюється, крім усього іншого, існуванням колізії публічних та приватних інтересів, вирішення якої потребує також відповідного юридичного забезпечення.

Хоча ми вже торкались загальних проблем такої колізії у більш ранніх наших працях та у попередніх розділах цієї розвідки, але вважаємо доцільним тут ще раз звернутися до цієї проблематики, аби поглянути як впливає на її вирішення «участь ШІ» та ставлення до нього людської спільноти.

Спеціально аналізу проблем у цій сфері присвячений матеріал Дарини Бойко та Івана Городиського з Центру Дністрянського «Штучний інтелект у сфері оборони: виклики регулювання», підготовлений у січні 2024 року за підтримки Європейського Союзу та Міжнародного фонду «Відродження» у рамках спільної ініціативи «Європейське Відродження України»[2].

Не переказуючи змісту цього дослідження, констатуємо лише, що, на думку його авторі, головною проблемою у цій сфері є використання Україною технологій ШІ для розпізнавання осіб за допомогою зображень з соціальних мереж та інтернету,[3] автоматизованого аналізу даних з використанням технології обробки природної мови тощо, розроблених відомими іноземними компаніями, які раніше зазнавали критики

[1] Всесвітній індекс свободи преси 2023 року: загроза індустрії симулякрів – Детектор медіа. (detector.media)

[2] Бойко Д., Городиський І. Штучний інтелект у сфері оборони: виклики регулювання. 12 січня 2024. URL: https://dc.org.ua/news/shtuchnyy-intelekt-u-sferi-oborony-vyklyky-regulyuvannya

[3] Україна – Clearview AI

через «безпекові і праволюдинні моменти». Попри те, що застосування згаданих технологій ШІ дає очевидні позитивні результати в ході збройного протистояння з Росією, вагомим викликом для їх використання в Україні, вважається проблема забезпечення захисту прав людини.[1]

Застосування технологій ШІ навіть у суто воєнних цілях викликало занепокоєння серед міжнародних організацій, а кшталт OpenDemocracy, котрі у березні 1922 року, (тобто у то час, коли доля України висіла буквально на волосині) хвилювалася, що українські військові отримали технологічні засоби, здатні допомогти їм стримати агресора.[2] На цю «схвильованість» відреагували представники громадянського суспільства в Україні, висловлюючи побоювання, що подальше використання технологій, заборонених на території деяких держав ЄС, може загальмувати або поставити під загрозу процес вступу України до ЄС.[3] Існування проблеми контролю над використанням ШІ відзначали зарубіжні та вітчизняні правознавці.[4]

Враховуючи згадані ризики для подальшого використання в Україні технологій, схожих на системи Clearview AI, Palantir та ін., автори роблять акцент на тому, що захист прав людини при використанні технологій ШІ є головною проблемою для українських регуляторів у контексті війни, а вирішення її вбачають у розмежуванні двох сценаріїв розвитку ШІ – «мирного» та «воєнного» – і розробки для кожного з них відповідних правил.[5]

---

[1] Бойко Д., Городиський І. Штучний інтелект у сфері оборони: виклики регулювання. 12 січня 2024. URL: https://dc.org.ua/news/shtuchnyy-intelekt-u-sferi-oborony-vyklyky-regulyuvannya

[2] Чи наближає технологія розпізнавання облич під час війни в Україні роботів-убивць? Clearview AI пропонує Україні свою суперечливу технологію для ідентифікації ворожих солдатів, тоді як автономні машини для вбивства набирають обертів. Даріан мічеммартін Гак. 30 березня 2022, URL: Українські військові отримали штучний інтелект для розпізнавання облич. Ми хвилюємося | opendemocracy

[3] Людва А., Авдєєва Т. Наскільки «зрозуміла» законність Clearview AI в Україні? 9 жовтня 2023. *Аналітичний звіт підготовлено в рамках програми «Сприяння свободі Інтернету в Україні», що реалізується Американською асоціацією юристів в Україні / Ініціатива з верховенства права.* Наскільки «зрозуміла» законність Clearview AI в Україні? – Лабораторія цифрової безпеки (dslua.org)

[4] Костенко О., Джейнс Т., Журавльов Д., Дніпров О., Усенко Ю. Проблеми використання автономного військового ші на фоні військової агресії росії проти україни. *Балтійський журнал юридичних та соціальних наук.* 2023. № 4. С. 131-145. https://doi.org/10.30525/2592-8813-2022-4-16

[5] Бойко Д., Городиський І. Штучний інтелект у сфері оборони: виклики регулювання. 12 січня 2024. URL: https://dc.org.ua/news/shtuchnyy-intelekt-u-sferi-oborony-vyklyky-regulyuvannya

Така пропозиція видається нам логічною, оскільки є ситуації звичайні, а є аномальні; правила, що стосуються звичайних відносин, не діють в аномальних ситуаціях.

Але тут слід зауважити, що проблема регулювання використання ШІ в Україні загострюється необхідністю враховувати не тільки особливості «мирного» та «воєнного» алгоритмів, а ще й євроінтеграційних процесів. У зв'язку з цим у жовтні 2023 року Міністерство цифрової трансформації оприлюднило Дорожню карту з регулювання штучного інтелекту в Україні, котра розглядається як підтвердженням намірів уряду поступово імплементувати Закон ЄС про ШІ (AI Act), який приділяє значну увагу захисту прав людини при впровадженні та застосуванні ШІ.

На першому етапі регулювання, який, згідно з Дорожньою картою, триватиме до 2025/2026 року, уряд намагатиметься «не зарегулювати» галузь ШІ, водночас готуючи бізнес до юридично обов'язкової регуляції. При цьому під час повномасштабної війни регуляція ШІ у проєктах, що стосуються воєнних потреб, не передбачається.

«Нам потрібно використовувати принцип зонування: яким має бути регулювання ШІ під час війни та після перемоги. Під час війни ми плануємо розробити законодавчу базу, яка не заважатиме використанню інновацій та технологій ШІ задля перемоги. Але після війни регуляція ШІ має допомогти Україні й надалі посилювати демократичність», – повідомила для Delo.UA Анна Булах, голова з етики ШІ та партнерства у Respeecher та член комітету ШІ при Мінцифри.

Нам таке рішення здається цілком виправданим.

Водночас зауважимо, що серед українських експертів у галузі ШІ з'являються дискусії щодо застосування оборонного ШІ після закінчення війни. Однак ці питання потребуватимуть додаткових обговорень та розробки окремих стандартів.

Проте автори дослідження, матеріали якого ми тут використовуємо, попри констатацію тієї обставини, що штучний інтелект довів свою ефективність під час російсько-української війни, наполягають на врахуванні ризиків ШІ, вважаючи, що ці ризики не можуть підлягати лише галузевому «саморегулюванню», зокрема коли це стосується застосування технологій ШІ за межами відсічі російській агресії.

На їхню думку, усунути ризики та забезпечити «справедливе й підзвітне» застосування технологій ШІ у «мирній» сфері, можуть, зокрема, такі заходи:

- Внесення змін до чинного законодавства, усунення прогалин регулювання застосовування технологій ШІ в оборонних цілях, з метою забезпечення гарантій захисту прав та свобод людини. Експерти Лабораторії цифрової безпеки пропонують з цією метою внести зміни до законів «Про захист персональних даних», «Про національну поліцію», а також до Кримінального та Кримінально-процесуального кодексів.
- Забезпечення пріоритетності впровадження регуляції (замість саморегулювання) у завдання розробки та використання технологій Ш, що використовуються для оборонних цілей. Ризик втручання в демократичні права та свободи є головним аргументом на користь проактивних дій.
- Контроль відповідальних осіб або суду за застосуванням цих технологій.
- Публічність процесу регламентації застосування цих технологій: постійні обговорення та дискусії для досягнення балансу інтересів між владою, громадянським суспільством та компаніями-розробниками ШІ.

Наостанок автори ще раз наголошують, що головним завданням для українського регулювання сфери застосування технологій оборонного ШІ має стати забезпечення захисту прав людини[1], які можуть постраждати від такого застосування, особливо якщо ці технології застосовуються не на полі бою. Саме це має стати стрижневою ідеєю при створенні правового регулювання технологій ШІ, поруч із забезпеченням економічного розвитку галузі.[2]

У підсумку, знову повертаємось до питань: так потрібно чи ні розмежувати «воєнне» та «невоєнне» застосування «оборонного» ШІ? І що таке «оборонний ШІ»: «призначений для оборони» чи такий, що колись «розроблявся для оборони», але втратив своє призначення і застосовується «не на полі бою». Тоді, чому він «оборонний»?

---

[1] Підкреслено нами – Є. Х., О. Х.

[2] Бойко Д., Городиський І. Штучний інтелект у сфері оборони: виклики регулювання. 12 січня 2024. URL: https://dc.org.ua/news/shtuchnyy-intelekt-u-sferi-oborony-vyklyky-regulyuvannya

А найбільше сумнівів викликає теза щодо головного завдання для українського регулювання сфери застосування технологій оборонного ШІ. Усе ж таки: головне завдання – це забезпечення захисту прав людини чи забезпечення виживання країни у війні, що має екзістенційний характер, про що часто згадують експерти. Адже якщо не враховувати друге, то й перша проблема просто відпаде, бо кривавий досвід свідчить, що наївно очікувати від російських окупантів забезпечення захисту прав людини.

Висновки

Дослідження правових проблем використання кіберзброї у гібридній війні дає підстави для висновку, що це можливо і практично найчастіше має місце в мілітарній та інформаційній гібридних війнах. При цьому постає практично важливе питання, чи може застосовуватись кіберзброя у «конвенційних війнах», а також, чи не тягне застосування кіберзброї у міліарній війні визнання її «не конвенцію». Концептний аналіз пов'язаних з цим теоретичних понять і законодавства дозволяє впевнено стверджувати, що використання кіберзброї є правомірним і дає гарні результати при відповіді на збройну агресію.

Ключові слова: міжнародне право, гуманітарне право, гібридна війна, кібервійна, збройний конфлікт, агресія, кіберзброя, штучний інтелект, конвенційна війна, конвенційна зброя, права людини, приватні права.

Розділ 15

ВЕРБУВАННЯ НЕПОВНОЛІТНІХ ЧЕРЕЗ СОЦМЕРЕЖІ ТА МЕСЕНДЖЕРИ В УМОВАХ ГІБРИДНОЇ ВІЙНИ: ЗАГРОЗИ, МЕХАНІЗМИ ТА ЗАХОДИ ЗАПОБІГАННЯ

DOI

Вікторія Рябченко
аспірантка

Вступ. Сучасний світ переживає епоху активного розвитку цифрових технологій, які значно змінюють способи взаємодії між людьми, формування інформаційних потоків та доступу до контенту. Віртуальний простір став невід'ємною частиною життя молодого покоління, як наслідок, зростає занепокоєння щодо нових форм руйнівного впливу на дітей.

Нові інформаційні технології та засоби зв'язку суттєво впливають на реалізацію прав дитини, закріплених у міжнародних документах, таких як Конвенція про права дитини (ратифікована 27.02.1991), Європейська Конвенція з прав людини (ратифікована 17.07.1997) та Європейська соціальна хартія (ратифікована із заявами 14.09.2006). Всі діти мають право на безпечний доступ до інформаційно-комунікаційних технологій та цифрових засобів масової інформації. Це право передбачає можливість повноцінно брати участь у суспільному житті, вільно висловлювати свої думки, шукати необхідну інформацію та користуватися усіма правами, гарантованими КПР ООН та її факультативними протоколами, без дискримінації.

Відповідно до статті 9 Закону України «Про охорону дитинства», кожна дитина має право на вільне висловлювання особистої думки, формування власних поглядів та розвиток громадської активності. Це право також передбачає свободу шукати, отримувати, використовувати, поширювати та зберігати інформацію будь-яким чином, зокрема через інтернет. Для забезпечення здорового фізичного, психічного, соціального, духовного та морального розвитку

дитини їй гарантується доступ до інформації з національних та міжнародних джерел[1].

Однак важливо враховувати, що доступ до цифрових технологій повинен бути безпечним і захищеним від будь-яких загроз, які можуть порушити права дитини. Технологічний прогрес, хоча і надає нові можливості для розвитку та самоствердження молоді, також створює ризики.

Соціальні мережі та месенджери, які спочатку були створені для комунікації, освіти та розваг, поступово перетворилися на інструменти маніпуляції свідомістю, зокрема, неповнолітніх. Країна-агресор активно використовує інтернет-платформи для розпалювання суспільного розколу, поширення страху та вербування молоді для здійснення деструктивних дій. Починаючи з ігор типу «Синій кит» (інші назви – «Тихий дім», «Розбуди мене о 4:20», «Море китів», «Чумацький шлях», «U19», «F57») та «Двері розуму» (інша назва – «Червоні двері, жовті двері»), завершуючи сучасними методами вербування неповнолітніх для терористичних актів: підпалів та підривів, ця стратегія є частиною ширшої гібридної війни, спрямованої на дестабілізацію суспільства.

Ці явища не лише демонструють новий рівень маніпуляції свідомістю, але й ставлять перед суспільством ряд важливих питань. По-перше, як саме організатори таких ігор та вербувальники використовують механізми для впливу на неповнолітніх? По-друге, які фактори роблять молодь особливо вразливою до такого роду впливу? По-третє, які інструменти можуть бути застосовані для запобігання та протидії таким явищам?

Стан опрацювання. Різні аспекти захисту прав та інтересів неповнолітніх були предметом аналізу у багатьох наукових праць провідних вчених, таких як *О. В. Мельник, Глиняної К. М., Т. В. Боднар, І. В. Жилінкової, Л. В. Красицької, М. В Менджул, О. В. Розгон, З. В. Ромовської, О. І. Сафончик, Є. О. Харитонова.* Окрім того, є окремі праці, що стосуються заборони участі дітей під час воєнних дій та у збройних конфліктах (*Глушко М. В., Лесько Н. В.* та ін.). Водночас проблематика впливу російських спецслужб через соцмережі та месенджери, зокрема телеграм, на неповнолітніх є достатньо новою,

[1] Про охорону дитинства: Закон України від 26.04.2001 № 2402-III: станом на 1 січ. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/2402-14#Text

тому проблеми захисту молоді України у цьому випадку досліджені фрагментарно.

Це підкреслює ***актуальність*** подальших досліджень для запобігання вербуванню неповнолітніх, формування ефективних механізмів захисту та забезпечення безпеки молоді в умовах гібридної війни. Потреба у комплексному вивченні цього питання обумовлена не лише загрозами для окремих осіб, а й ризиками для стабільності суспільства в цілому.

Виклад основного матеріалу. Гра «Синій кит» є одним із найбільш тривожних феноменів сучасного цифрового суспільства, який набув широкого поширення на платформі соціальної мережі «ВКонтакте» (стосовно якої у 2017 році Президент України своїм указом встановив вимогу блокування доступу на території України), а потім і телеграм у період 2016-2018 років. Її походження пов'язане з росією, де вперше були зареєстровані випадки участі неповнолітніх у грі та її трагічних наслідків.

Ця інтернет-гра спрямована на маніпуляцію свідомістю неповнолітніх через серію завдань, які поступово поглиблюють психологічний тиск і закінчуються інструкцією до самогубства. Гра «Синій кит» представляє собою серію завдань, які користувачі повинні виконувати протягом 50 днів. Завдання починаються з невинних дій, таких як перегляд фільмів жахів або прослуховування депресивної музики і поступово переходять до більш радикальних дій, наприклад, само пошкодження, порізів шкіри. Останнє завдання полягає у стрибку з високої будівлі або іншому способі самогубства.

Організатори гри, як правило, виступають у ролі «кураторів» (або ще вони себе називають «куратори смерті»), які контролюють виконання завдань через месенджери, соціальні мережі або закриті онлайн-чати. Вони використовують психологічний тиск, загрози та шантаж для того, щоб примусити учасників продовжувати гру. Так, за перші 7 місяців 2018 року діти здійснили 156 спроб суїцидів. З них у 58 випадках неповнолітні загинули. За даними ЄРДР, у 2020 році вчинили самогубство 123 підлітки, а вже на початку березня 2021 року органами Національної поліції було зафіксовано 25 випадків самогубств і 91 спробу вчинити такі дії[1].

[1] В Україні торік вчинили самогубство 123 підлітки – МВС. *УКРІНФОРМ.* URL: https://www.ukrinform.ua/rubric-society/3213177-v-ukraini-torik-vcinili-samogubstvo-123-pidlitki-mvs.html

Гра «Синій кит» використовує ряд психологічних механізмів, які сприяють формуванню залежності та втраті критичного мислення, зокрема, прогресивне зростання складності, тобто завдання у грі поступово ускладняються, що створює ефект «просування до мети». Гравець втрачає здатність критично оцінювати наслідки своїх дій. Організатори гри часто використовують загрози, шантаж або обіцянки «відкриття нового світу» для того, щоб примусити гравців продовжувати участь. Ізолювання, оскільки гра створює ілюзію особистого зв'язку з «куратором», що призводить до соціальної ізоляції гравця від родини та друзів. Штучне створення страху, власне «куратори» використовують загрози розкриття секретів або залякування для того, щоб утримати гравця у грі.

Участь у даній грі може мати серйозні наслідки для неповнолітніх: перш за все, наслідком тривалого психологічного тиску та втрати контролю над своїми діями стає самогубство. Багато завдань у грі вимагають само пошкодження (наприклад, порізи, опіки), що може призвести до фізичних травм, які потребують медичної допомоги. Гравці часто стикаються з тривожністю, депресією, параноєю та іншими психічними розладами. Постійний тиск та стресові ситуації можуть призвести до довготривалого впливу на психічний стан. Учасники гри часто віддаляються від родини, друзів та суспільства, що призводить до соціальної маргіналізації та погіршення якості життя.

З початком повномасштабного вторгнення країна-агресор «в темну» використовувала українську молодь для збору даних про місцезнаходження стратегічно важливих об'єктів. На початку 2022 року стали відомі декілька фактів вербування українських неповнолітніх спецслужбами російської федерації, для цього останні використовують смартфон-ігри. Одна з таких ігор пропонує користувачам шукати «коробки» з віртуальними призами, які можна обміняти на електронні гроші. Під час цього процесу діти, не усвідомлюючи наслідків, фотографують місцевість, включаючи об'єкти військової та критичної інфраструктури у різних населених пунктах. Усі дані включно з геопозицією потім зберігаються в базі додатку і потім можуть бути використані для розвідки або планування диверсій.

У 2025 році Національна соціальна сервісна служба України повідомила, що серед неповнолітніх почав поширюватися новий небезпечний тренд – гра «Червоні двері, жовті двері», також відома як

«Двері розуму», що передбачає введення гравця у трансоподібний стан. Ця гра є своєрідним онлайн-ритуалом або челенджем, який зазвичай відбувається в реальному житті під керівництвом іншої особи. Учасник лягає на підлогу, а інша людина здійснює ритмічні масажні рухи його скронь, одночасно повторюючи фразу «Червоні двері, жовті двері». Після досягнення певного стану, учасник нібито потрапляє до уявного коридору з безліччю дверей різних кольорів. Завдання полягає у відкритті цих дверей та описі того, що знаходиться за ними. Ключовим елементом гри є пошук «червоних» та «жовтих» дверей, які, за повір'ями, можуть відкрити доступ до підсвідомості або інших «вимірів».

Незважаючи на те, що гра «Двері розуму» не передбачає прямих завдань, спрямованих на само пошкодження, як у «Синьому киті», такі розваги можуть шкодити школярам як фізично так і психологічно.

Національна соціальна сервісна служба України акцентує увагу на тому, що так зване підкорення «провіднику» чи «куратору» і соціальний тиск можуть використовуватися для підготовки підлітків до виконання небезпечних або злочинних дій, у тому числі на користь країни-агресора[1].

Ці ігри вкотре демонструють, як легко можна залучити неповнолітніх через інтернет, використовуючи їхню вразливість, пошук значущості та бажання належати до «спільноти». Хоча масштаби поширення ігор залишаються предметом дискусій, їх поява стала важливим сигналом про те, що соціальні мережі можуть бути використані для організації більш масштабних «проєктів» за участі неповнолітніх.

За даними проведеного дослідження громадянською мережею «Опора» однією з популярніших соціальних мереж в Україні станом на 2024 рік є телеграм (ним користується 78,1% опитаних), друге і третє місце посідають ютуб (59,5%) та фейсбук (44,6%) відповідно[2]. Варто відзначити, що ще в 2023 році телеграму перевагу надавало 71,3% опитаних осіб, тобто за один рік кількість нових прихильників зросла на 6,8%.

---

[1] Національна соціальна сервісна служба – Небезпечний тренд серед дітей: гра «Червоні двері, жовті двері».. URL: https://nssu.gov.ua/news/nebezpechnyi-trend-sered-ditei-hra-chervoni-dveri-zhovti-dveri

[2] «Опора»: найпопулярнішими соцмережами в Україні є телеграм, ютуб та фейсбук. URL: https://ms.detector.media/sotsmerezhi/post/35557/2024-07-16-opora-naypopulyarnishymy-sotsmerezhamy-v-ukraini-ie-telegram-yutub-ta-feysbuk/

Телеграм став однією з найпопулярніших платформ для впливу на неповнолітніх через інтернет, оскільки його технічні та функціональні особливості ідеально підходять для таких цілей. Однією з ключових переваг телеграму є можливість зберігати анонімність, так користувачі можуть створювати облікові записи без надання реальних даних (наприклад, номер телефону можна замаскувати), можливість використання псевдонімів дозволяє «кураторам» залишатися невпізнаними.

Телеграм надає можливість створювати закриті чати та канали, доступ до яких мають лише конкретні користувачі, тобто, вербувальники можуть створювати приватні групи, де вони координують дії своїх «підопічних», але одночасно з цим учасники не можуть побачити інших учасників чату. Такі чати часто захищені паролями або посиланнями, які доступні лише за запрошенням.

Телеграм використовує технологію кінцевого шифрування для секретних чатів, що робить неможливим перехоплення повідомлень. Правоохоронні органи та провайдери не можуть отримати доступ до контенту, саме ця функція зробила цей месенджер популярним серед організаторів нелегальної діяльності.

Платформа неактивно бореться зі шкідливими групами або каналами, поки вони не отримають великої уваги ЗМІ або офіційних скарг, тому вербувальники часто використовують цю «лазівку» для пошуку потенційних жертв.

Вербування і використання дітей прямо заборонені, як міжнародним правом – норма 136 звичаєвого міжнародного гуманітарного права, спільна ст. 3 Женевських конвенцій 1949 року, ст. 77 Додаткового протоколу до Женевських конвенцій 1949 року, що стосується захисту жертв міжнародних збройних конфліктів, ст. 38 Конвенції про права дитини, факультативний протокол до Конвенції про права дитини щодо участі дітей у збройних конфліктах, так і національним правом – ст. 30 Закону України «Про охорону дитинства». Незважаючи на те, що всі зазначені норми є обов'язковими для виконання, російська федерація, як сторона міжнародних договорів, цинічно порушує ці положення. Такі дії зі сторони країни-агресора є явним порушенням норм міжнародного права та свідчать про нехтування принципами гуманності та захисту прав дитини.

За офіційними повідомленнями правоохоронних органів в період з лютого 2022 року по березень 2025 щонайменше 50 неповнолітніх були завербовані й брали участь у підпалах і підривах. За цей же період відбулись 42 підпали і підриви в адміністративних будівлях, ТЦК, 88 підпалів і підривів військових, військової техніки та правоохоронців[1].

Ці порушення мають систематичний характер і є частиною гібридної війни, тому важливим є не лише документування таких фактів для подальшого їх використання в міжнародних судах, але й проведення активної роботи щодо запобігання вербуванню та захисту прав дітей.

Неповнолітні є особливо вразливими до вербування через ряд психологічних особливостей, які характерні для їхнього вікового періоду. Перш за все, це постійний пошук ідентичності та значущості. У цьому віці молодь часто намагається знайти відповіді на питання «Хто я?» та «Яке моє місце у світі?». Вербувальники використовують цю потребу, надаючи неповнолітнім ілюзію того, що їхні дії мають величезне значення. Наприклад, вони можуть переконувати молодь, що їхня участі у підпалах або підривах є актом «героїзму» або «боротьби за справедливість».

Другий важливий фактор – емоційна лабільність. Неповнолітні частіше дорослих схильні до емоційних коливань, що робить їх більш вразливими до маніпуляцій. Зловмисники часто використовують техніки емоційного тиску, такі як загрози, шантаж або обіцянки нагороди. Наприклад, вербувальники можуть говорити щось подібне: «*якщо ти не виконаєш, твої близькі можуть постраждати*» або «*якщо сьогодні не спалиш машину, я в СБУ відправлю твою розвідку і наші розмови з тобою, у мене все збережено».*

Представники російських спецслужб в телеграмі можуть додати дитину, без її згоди, до приватних груп. У таких чатах молоді пропонують завдання або обіцянки винагороди за залучення нових учасників. Останні часто навіть не знають, хто саме їх додав. Вербувальними часто використовують фальшиві аккаунти, створюють фейкові профілі, які виглядають доволі реалістично: з фотографіями

[1] Гарасим А., Кельм Н., Романишин Н. Вимкніть телеграм. Він робить з українських дітей терористів (інфографіка). URL: https://texty.org.ua/articles/114801/vymknit-telehram-vin-robyt-z-ukrayinskyh-ditej-terorystiv-infohrafika/

та історіями, аналізують відкриті чати (наприклад, волонтерські, тематичні або ті, що є популярними серед неповнолітніх), вибирають потенційних жертв і надсилають їм повідомлення. Вони очікують реакції та намагаються встановити контакт.

Третім і найголовнішим фактором є те, що у підлітковому віці спостерігається значне зростання потреб, які потребують фінансових витрат. Однак через ряд причин реалізувати їх часто стає складно. Це можуть бути обмеження, пов'язані з фінансовим становищем сім'ї, малопривабливі для підлітків способи заробітку (наприклад, фізична праця після занять), правові обмеження на працевлаштування через вік або деякі інші причини. Такі фактори ускладнюють задоволення матеріальних бажань у цьому віці. Проведені дослідження засвідчили, що матеріальні труднощі є однією з найпоширеніших причин учинення неправомірних дій неповнолітніми[1].

Вербування починається з невинних, на перший погляд, завдань, за більш менші суми, таких як намалювати графіті, розклеювати листівки або розповсюджувати інформацію.

Приклад з конкретної ситуацій: *«Почни поки що з малого, моя порада. Якраз і придивимося один до одного. Ну щось дріб'язкове спочатку зроби, а далі вже найбільші куші»*[2].

Вербувальники найчастіше вдаються до маніпуляцій і обіцянок легких грошей. Вони можуть запевняти молодь, що за виконання небезпечних і протиправних завдань вони отримають значну фінансову винагороду. Такі обіцянки часто формулюються так, щоб переконати неповнолітнього, що це «легкий» спосіб швидко заробити, не вимагаючи великих зусиль чи спеціальних навичок. Неповнолітні легко відгукуються на оголошення на кшталт: «2-3 тисячі доларів, навички не потрібні, тільки ваше бажання, ваш телефон і час».

Найчастіше мова йде про суми від кількох тисяч до сотень тисяч гривень, що стає потужним спонукальним мотивом для підлітків. Однак, насправді, ці обіцянки часто є лише приманкою: деякі жер-

[1] Шанскова Т. І. Аналіз причин правопорушень неповнолітніх як підґрунтя соціально-педагогічної роботи з молоддю щодо профілактики злочинності. *Вісник Житомирського державного університету ім. І. Франка.* 2006. № 30. С. 50-53.

[2] Свобода Р. «Тобі за це нічого не буде»: як спецслужби РФ свідомо вербують дітей для підпалів авто ЗСУ і будівель ТЦК. *Радіо Свобода.* URL: https://www.radiosvoboda.org/a/news-fsb-pidlitky-pidpaly-avto-zsu/33151236.html

тви можуть отримати лише частину зазначеної суми як аванс, а інші взагалі залишаються без грошей. Більш того, у багатьох випадках вербувальники ігнорують свої зобов'язання, оскільки їхня мета полягає не в оплаті послуг, а в максимально можливому втягуванні молоді у протиправні дії. У кращому випадку підліток отримує невеликий платіж, але реальна винагорода за свою участь їм так і не сплачується. Такий підхід демонструє маніпулятивну стратегію спецслужб, які намагаються залучити неповнолітніх, використовуючи їх довірливість та недосвідченість.

При цьому вербувальники свідомо замовчують реальні наслідки таких дій. Неповнолітні, які часто ще не мають достатньо життєвого досвіду та критичного мислення, можуть потрапити під вплив таких маніпуляторів і погодитися на небезпечні дії, спокушаючись швидкими грошима.

Наприклад, у переписках з 12-річним хлопцем вербувальник заявив: *«Навіть якщо тебе спіймають, максимум будеш легко фізично покараний»*[1]. Такі заяви формують помилкове враження безкарності.

Співробітник департаменту контррозвідки СБУ вказує наступне: «Були випадки, коли паліями були діти до 14-ти років. Вони ще не мають повністю сформованого бачення, не розуміють всієї серйозності суспільного резонансу і наслідків, і це просто легкий заробіток швидких грошей»[2].

У вербуванні неповнолітніх для здійснення підпалів автомобілів ЗСУ чітко простежується спланована російська пропагандистська кампанія, метою якої є дестабілізація ситуації в Україні. Відомо, що «куратори» часто намагаються замаскувати свої дії під протест проти територіальних центрів комплектування та соціальної підтримки (далі – ТЦК) або мобілізації. Молоді пропонують знайти будь-який старий, згорілий автомобіль, за умови, що в ньому щось залишилося цілим. Далі їм дають вказівку прикріпити до авто наклейку ЗСУ й підпалити його. Це чітко демонструє, що такі дії є частиною спланованої пропагандистської кампанії.

---

[1] Свобода Р. «Тобі за це нічого не буде»: як спецслужби РФ свідомо вербують дітей для підпалів авто ЗСУ і будівель ТЦК. *Радіо Свобода*. URL: https://www.radiosvoboda.org/a/news-fsb-pidlitky-pidpaly-avto-zsu/33151236.html

[2] Свобода Р. «Тобі за це нічого не буде»: як спецслужби РФ свідомо вербують дітей для підпалів авто ЗСУ і будівель ТЦК. *Радіо Свобода*. URL: https://www.radiosvoboda.org/a/news-fsb-pidlitky-pidpaly-avto-zsu/33151236.html

Під час спілкування з потенційними виконавцями куратори активно наголошують, що їхня «мета» – боротьба з ТЦК. *«Наша мета – захистити простих людей, щоб їх не забирали до мобілізації», «Ми – організація, яка бореться з ТЦК. Нас фінансують, і виділяють великі суми на ці завдання»*[1]. Такий наратив спеціально обраний стороною-агресором.

За всіма випадками підпалів стоять російські спецслужби, зокрема ФСБ. Існує спроба створити ілюзію, що підпалювання є актами протесту з боку українців, які не схвалюють політику влади чи мобілізацію. Однак насправді це елемент інформаційно-психологічних операцій (ІПСО), які активно поширюються та набирають обертів у засобах масової інформації та соціальних мережах.

Виходить, що підпал автомобілів – це не окремі випадки вандалізму, а добре продумана стратегія російських спецслужб, метою якої є підрив довіри до української влади та створення ілюзії внутрішнього протистояння.

Однак, країна-агресор не зупиняється лише на підпалах авто, вони «йдуть» далі і вдаються до залучення українських неповнолітніх до терористичних актів.

Так, за інформацією прокуратури та Служби безпеки України, 14-річну неповнолітню завербували через месенджер телеграм для вчинення вибуху біля райвідділу Національної поліції[2]. Вербувальник знайшов дівчину, коли вона шукала можливості швидкого заробітку в інтернеті. Щоб схилити її до співпраці, той «зламав» її телефон і почав шантажувати, загрожуючи оприлюднити її відверті фото. Під тиском погроз дівчина виготовила саморобний вибуховий пристрій за інструкціями, які надавалися онлайн. Конструкція була створена з доступних матеріалів, включаючи елементи електроніки та засоби ініціювання і була прихована під службовим автомобілем поліції.

За даними фахівців, саморобні вибухові пристрої складаються з компонентів, які легко придбати у вільному доступі. Вербувальники надають детальні інструкції через відео зв'язок, пояснюючи, як змішувати хімічні речовини, під'єднати електронні елементи та ство-

[1] Там само.

[2] Неповнолітню жительку Тернопільщини підозрюють у спробі вчинити теракт біля райвідділу поліції. *СУСПІЛЬНЕ ТЕРНОПІЛЬ*. URL: https://suspilne.media/ternopil/975867-nepovnolitnu-zitelky-ternopilsini-pidozruut-u-sprobi-vciniti-vibuh-bila-rajviddilu-policii/

рювати механізм підриву. Для цього не потрібні спеціальні знання з хімії, фізики чи електрики, так як «куратор» контролює процес онлайн, крок за кроком[1].

Як зазначалося раніше, неповнолітнім обіцяють значні суми грошей, але ці обіцянки лише приманка. Окрім несплати грошей, «куратори» знищують своїх «агентів» разом із вибуховими пристроями, щоб уникнути розкриття. 11 березня 2025 року в Івано-Франківську стався завчасно спланований теракт, який двоє місцевих підлітків виконували на замовлення і за вказівками російських спецслужб. Через детонацію вибухових пристроїв один підліток загинув на місці, іншому – ампутували ноги[2].

Наслідки вербування неповнолітніх є руйнівними як для самих жертв, так і для суспільства в цілому. Перш за все, це фізичні та психологічні травми, які отримують неповнолітні. Участь у підпалах, підривах або інших формах насильства часто призводить до травм, інвалідності або навіть смерті або завербовані можуть страждати від посттравматичного стресового розладу (ПТСР), депресії або інших психічних розладів.

Наступним наслідком може стати соціальна маргіналізація. Неповнолітні, які потрапили під вербування, часто стикаються зі стигмою у суспільстві. Їхні родини також можуть страждати від психологічних травм, фінансових труднощів або соціального відвернення. Це створює замкнене коло, де молодь ще більше відчувається відверненою та схильною до повторного впливу.

Далі – дестабілізація суспільства. Дії, організовані через вербування неповнолітніх, спричиняють масову паніку та політичну нестабільність. Це стосується не лише окремих країн, але й глобальної безпеки.

Для ефективної боротьби з вербуванням неповнолітніх необхідно застосовувати комплексний підхід, який включає правові, освітні та психологічні заходи.

Так, у відповідь на тривалу збройну агресію російської федерації проти України та систематичні порушення прав дітей, Кабінет Міні-

[1] Як спецслужби РФ вербують підлітків для терактів: коментарі поліцейських з Тернопільщини. *СУСПІЛЬНЕ ТЕРНОПІЛЬ*. URL: https://suspilne.media/ternopil/983723-ak-specsluzbi-rf-verbuutpidlitkiv-dla-teraktiv-komentari-policejskih-z-ternopilsini/

[2] Вибухи в Івано-Франківську – що відомо. *ТСН.ua*. URL: https://tsn.ua/ukrayina/terakt-v-ivano-frankivsku-shokuvalni-podrobici-vibuhiv-bilya-zaliznichnogo-vokzalu-2786328.html

стрів України затвердив Національний план превентивних заходів від 22 березня 2024 року № 256-р[1]. Цей документ спрямований на припинення та запобігання грубим порушенням прав дітей у зоні конфлікту, зокрема щодо вербування, використання та участі неповнолітніх у бойових діях і збройних конфліктах. Згідно з положеннями якого основними напрямами діяльності держави є: по-перше, інформаційно-просвітницька робота. Одним із ключових завдань плану є проведення широкомасштабної просвітницької кампанії серед дітей, батьків та законних представників. Ця робота передбачає залучення громадських організацій, міжнародних партнерів та медіа для поширення достовірної інформації про загрози, пов'язані з вербуванням дітей. Розробка та розповсюдження інформаційних матеріалів, які пояснюють наслідки вербування та використання неповнолітніх. Залучення експертів для проведення лекцій, семінарів та тренінгів з метою підвищення обізнаності населення. Використання сучасних медіа-платформ для інформування громадян про методи вербування та способи запобігання таким ситуаціям.

По-друге, моніторинг та інформування про факти вербування, офіс Генерального прокурора України має інформувати про будь-які факти вербування (у тому числі прихованого) дітей для участі у збройних формуваннях. Особливу увагу приділяють документуванню таких випадків для подальшого їх використання в міжнародних судових органах.

По-третє, для запобігання можливим випадкам вербування та використання дітей у збройних конфліктах передбачено проведення роз'яснювальної роботи серед молоді щодо того, як розпізнавати методи вербування через соціальні мережі, месенджери та особисті контакти.

Особлива увага приділяється запобіганню залучення дітей до виконання завдань, пов'язаних із збройним конфліктом, таких як розвідка, підпали авто та диверсії. Для цього має проводитись активна робота зі школярами та студентами щодо розуміння наслідків таких дій, впроваджується система раннього виявлення потенційних ви-

[1] Про затвердження національного плану превентивних заходів щодо припинення та запобігання грубим порушенням прав дітей в умовах збройної агресії Російської Федерації проти України: Розпорядж. Каб. Міністрів України від 22.03.2024 № 256-р. URL: https://zakon.rada.gov.ua/laws/show/256-2024-р#Text

падків вербування через аналіз активності в соціальних мережах та месенджерах.

Залучення громадських організацій та міжнародних партнерів є невід'ємною частиною реалізації Національного плану. Співпраця з такими організаціями допоможе як забезпечити широкий охват просвітницьких заходів, так і залучити міжнародні організації до моніторингу порушень прав дітей та документування таких фактів.

Міністерством освіти і науки України батькам стосовно їх дітей рекомендовано: спостерігати за поведінкою, навчати фінансової грамотності, привчати до цифрової безпеки та розпізнаванню маніпуляцій і найголовніше – мати з неповнолітнім відкрите спілкування та підтримувати довірливі стосунки[1].

Відповідно до ч. 2 ст. 150 Сімейного кодексу України батьки зобов'язані піклуватися про фізичний, духовний і моральний розвиток дитини[2]. Батьки мають не тільки створити безпечне середовище для розвитку своєї дитини, а й піддавати її контролю. Інакше кажучи, раціональний та свідомий батьківський контроль може стати запобіжником девіантної поведінки неповнолітнього. Саме для цього існує низка корисних сервісів для батьків, за допомогою яких можна наглядати за неповнолітнім, при цьому не порушуючи його особистих кордонів, таких як Google Family Link, Qustodio, Bark. Однак, батькам не слід покладатися лише на технічні засоби контролю, адже діти можуть знайти способи обійти обмеження. Натомість важливо познайомити їх із прийомами онлайн-вербовки, навчити розрізняти фейки та пояснити наслідки розголошення секретної інформації, яку не слід знати представникам країни-агресора.

Разом з тим, існують ресурси, які допомагають протидіяти дезінформації та вербуванню. Наприклад: телеграм-канал «Брама» надає інформацію про блокування підозрілих акаунтів та дає поради щодо захисту від шахрайства. Канал «StopRussia | MRIYA» пропонує інструкції та завдання для протидії фейкам та інформаційним загрозам. Чат-боти СБУ «Знайди зрадника» та «Спали ФСБшника» дозволяють повідомляти про спроби вербування або інші протиправні дії.

---

[1] *Як розпізнати ознаки вербування дитини? Рекомендації батькам і освітянам.* URL: https://mon.gov.ua/news/yak-rozpiznaty-oznakyverbuvannia-dytyny-rekomendatsii-batkam-i-osvitianam

[2] Сімейний кодекс України: Закон України від 10.01.2002 № 2947-III. URL: https://zakon.rada.gov.ua/laws/show/2947-14#Text

Батьки можуть надати дітям конкретні поради для уникнення вербування: бути обережними в інтернеті та уникати контактів із підозрілими особами, звертати увагу на ознаки обману, такі як пропозиції швидкого заробітку за виконання простих завдань. Якщо дитина отримує підозрілі пропозиції, їй слід негайно повідомити про це дорослих або звернутися до поліції за телефоном «102», або заповнивши форму зворотного зв'язку на сайті кіберполіції.

Протидіяти вербуванню можна також через формування сталої системи цінностей, яка ґрунтується на таких ключових принципах, як патріотизм, відчуття національної приналежності, єдності та поваги до своєї країни. Ці цінності допомагають неповнолітнім розуміти важливість захисту держави та її інтересів, а також створюють моральні бар'єри проти залучення до протиправних дій. Виховання у дітей почуття гордості за свою націю та історію формує стійкий імунітет до маніпуляцій з боку країни-агресора.

Ефективними інструментами для формування таких цінностей є активна волонтерська діяльність, яка надає молоді можливість реалізувати себе у корисних для суспільства справах. Наприклад, організація акцій з виготовлення оберегів для військових не лише сприяє підтримці Збройних Сил України, але й дає молоді відчуття причетності до загальнонаціональної боротьби за незалежність. Такі проєкти часто супроводжуються лекціями, тренінгами та бесідами, де молодь отримує інформацію про значення кожного внеску у загальну перемогу. Крім того, збір коштів для потреб ЗСУ – це ще один спосіб залучити молодь до активної участі у захисті держави. Це можуть бути благодійні ярмарки, флешмоби чи онлайн-кампанії, які не лише допомагають залучати фінансові ресурси, але й формують відповідальне ставлення до суспільних проблем.

Підсумовуючи вищевикладений матеріал, можна зазначити, що сучасний цифровий світ, незважаючи на свою інноваційність та можливості, несе значні загрози для неповнолітніх, особливо в умовах збройних конфліктів та гібридної війни. Російські спецслужби активно використовують соціальні мережі, месенджери та інші онлайн-платформи для вербування молоді до участі в протиправних діях, таких як підпали автомобілів, підриви, або навіть терористичні акти. Психологічна вразливість, пошук ідентичності, потреба в швид-

ких грошах та недосвідченість роблять неповнолітніх доступними цілями для маніпуляторів.

Небезпечні ігри, подібні до «Синього кита» та «Дверей розуму», є лише частиною ширшої стратегії впливу на свідомість молоді. Ці феномени демонструють, як легко можна залучити дітей через інтернет, використовуючи їхню довірливість та через ряд психологічних особливостей. Наслідки такого впливу є руйнівними: самогубства, каліцтва, психічні розлади, соціальна маргіналізація та дестабілізація суспільства в цілому.

Для запобігання вербуванню та захисту прав дітей необхідний комплексний підхід, який включає просвітницьку роботу, правове регулювання, постійний моніторинг. Затверджений Національний план превентивних заходів є важливим кроком у цьому напрямку. Однак успіх залежить від спільних зусиль батьків, педагогів, правоохоронних органів та громадськості. Саме довірливі стосунки, відкрите спілкування та формування стійкої системи цінностей допоможуть захистити молодь від небезпечного впливу та забезпечать майбутнє безпечного та стабільного суспільства.

Ключові слова: неповнолітні, гібридна війна, цифрові загрози, вербування, соціальні мережі, месенджери, інформаційна безпека, радикалізація молоді, безпека дітей в інтернеті, протидія вербуванню.

Розділ 16

ПРАВОВЕ РЕГУЛЮВАННЯ ДІЯЛЬНОСТІ СТАРТАПІВ В УМОВАХ ГІБРИДНОЇ ВІЙНИ: ВИКЛИКИ, МОЖЛИВОСТІ ТА ПЕРСПЕКТИВИ

DOI

Дмитро Розумейко
аспірант

Сучасна економічна реальність і тенденції цифровізації зумовили стрімкий розвиток стартап-індустрії як важливого сегмента інноваційної економіки. Слід зазначити, що в Україні роль стартапів набуває особливого значення у контексті гібридної війни, де поєднання воєнних та інформаційно-економічних чинників створює правові виклики для всієї сфери підприємницької діяльності. Отже, з одного боку, інноваційні технології та передові ідеї спроможні забезпечити економічний ріст і технологічну безпеку держави, але водночас їх розвиток ускладнюється факторами воєнного часу, включно з можливими кібератаками, економічною нестабільністю та потребою у додаткових правових гарантіях.

Актуальність теми обумовлена необхідністю ґрунтовного цивільно-правового дослідження процесів створення, функціонування та захисту стартапів, які сьогодні постають вагомим інструментом підвищення конкурентоспроможності національної економіки. Виходячи з цього, в умовах гібридної війни постає потреба в розробленні комплексного правового механізму для захисту інтелектуальної власності, регулювання електронних правочинів, забезпечення кібербезпеки, а також належного врегулювання взаємовідносин з інвесторами та державними інституціями.

Об'єктом дослідження виступають правовідносини, що виникають у процесі створення, функціонування та припинення стартапів, особливо в контексті викликів гібридної війни. Предметом дослідження є правові норми, доктринальні підходи, судова практика та міжнародні стандарти, що регламентують підприємницьку діяль-

ність інноваційного характеру, захист інтелектуальної власності й укладення цифрових правочинів. Підсумовуючи, актуальність обраної теми зумовлена потребою формування ефективного правового механізму, здатного захистити інноваційні ініціативи від зовнішніх загроз і забезпечити сталі передумови для розвитку української стартап-екосистеми в умовах гібридної війни.

Єдиного визначення терміну «стартап» у законодавстві України наразі немає. В юридичній літературі та бізнес-практиці стартапом зазвичай називають новостворену компанію, що пропонує інноваційний продукт чи послугу та перебуває у пошуку масштабованої бізнес-моделі[1]. Наприклад, за класичним підходом С. Бланка стартап – це тимчасова організація, яка шукає масштабовану і відтворювану прибуткову бізнес-модель[2]. Е. Ріс визначає стартап як новостворену інституцію, метою якої є розробка нових продуктів або послуг в умовах високої невизначеності. Отже, ключові ознаки стартапу – новизна, інноваційність, потенціал швидкого зростання та робота в умовах обмежених ресурсів і підвищеного ризику. Від традиційного малого бізнесу стартап відрізняється саме спрямованістю на новаторство і масштабування: стартап є малим бізнесом, але не кожен малий бізнес можна вважати стартапом.

Стартапи зазвичай засновуються ентузіастами або підприємцями для реалізації унікальної бізнес-ідеї та здатні швидко зростати за сприятливих умов. Вони мають обмежені початкові ресурси, але високий потенціал масштабування, тому часто залучають інвестиції для розвитку. Інноваційна спрямованість стартапів означає, що такі проєкти впроваджують нові технології або незвичні бізнес-моделі, прагнучи зайняти свою нішу на ринку. Стартапи відіграють важливу роль в інноваційній економіці: вони є каталізатором технологічного прогресу, створюють нові робочі місця та сприяють формуванню нових секторів ринку. Розвиток стартап-індустрії особливо актуальний для України – активне виникнення стартапів є важливим чинником перемоги України та відновлення економіки у післявоєнний період[3].

---

[1] Хаустов М. Стартапи: створення та масштабування: монографія. Харків: ФОП Лібуркіна Л. М, 2023. 224 с.

[2] Blank S., Dorf B. The Sturtup owner's manual. California: K&S Ranch Press, 2012. 1090 с.

[3] Чумак А. Л., Ткачова С. С. Розділ 3. менеджмент, публічне управління та адміністрування. Universum № 10. 2024. С. 18–25. URL: https://archive.liga.science/index.php/universum/article/view/1164

Існує багато критеріїв класифікації стартапів залежно від їх характеристик і мети діяльності. Найбільш поширеними є такі види стартапів[1]:

- технологічні стартапи – бізнес яких побудований на використанні новітніх технологій або на створенні технологічних інновацій. Вони часто працюють у сфері IT, електроніки, біотехнологій тощо і пропонують високотехнологічні продукти або послуги;
- соціальні стартапи, що орієнтовані на вирішення соціальних проблем або задоволення суспільних потреб. Як правило, йдеться про проєкти благодійного чи некомерційного характеру, які існують за рахунок грантів або пожертв. Мета соціальних стартапів – створити соціальну цінність (наприклад, освітні платформи, екологічні ініціативи), а не лише отримати прибуток;
- інноваційні та традиційні – за ступенем новизни продукту розрізняють радикально інноваційні стартапи (пропонують принципово новий продукт/технологію) та інкрементальні (удосконалюють чи комбінують існуючі рішення);
- стартапи класифікують за секторами економіки: існують стартапи в IT-сфері, фінтех, медичні (MedTech), агротехнічні (AgroTech), енергетичні, креативні індустрії тощо;
- різняться *масштабовані стартапи*, що націлені стати великими міжнародними компаніями, *стартапи малого бізнесу*, що залишаються невеликими підприємствами, *стартапи-«єдинороги»*, *«лайфстайл»-стартапи*, створені для самозайнятості засновника, та *стартапи великого бізнесу*, що виникають як внутрішні інноваційні проєкти корпорацій

Таким чином, стартап – це особлива форма підприємництва, що базується на інноваціях. Стартапи бувають різних типів (технологічні, соціальні тощо), але всіх їх об'єднує новаторський характер і спрямованість на зростання. Вони є рушієм розвитку інноваційної економіки, генеруючи нові ідеї та рішення, які здатні суттєво вплинути на економічне зростання країни.

В умовах багатогранної агресії, що одночасно охоплює військові дії та різноманітні невійськові засоби впливу (інформаційні, економічні,

[1] Ситник Н. І., Голюк В. Я. Менеджмент стартап проектів: навчальний посібник. КПІ ім. Ігоря Сікорського, 2019. 58 с.

кібератаки тощо) з метою послабити й дестабілізувати противника, що виходить за межі звичайного збройного протистояння й включає масовану пропаганду й дезінформацію, торговельно-економічний тиск, енергетичні блокади, терор і залякування мирного населення, кібератаки на критичну інфраструктуру, категоричне заперечення самого факту війни попри очевидні докази, використання проросійських сил та держав-сателітів, а також звинувачення України у діях, які насправді вчиняє сама росія. В таких умовах особливо страждає приватний сектор, включно з галуззю інформаційних технологій та стартап-екосистемою.

Повномасштабна війна і супутні гібридні атаки суттєво вплинули на українську ІТ-галузь. Багато технологічних компаній вимушено релокувалися або відкрили офіси за кордоном задля безпеки. Повномасштабна війна і супутні гібридні атаки суттєво вплинули на українську ІТ-галузь. Багато технологічних компаній вимушено релокувалися або відкрили офіси за кордоном задля безпеки[1]. Це свідчить, що багато українських стартапів та ІТ-бізнесів змогли перебудувати процеси (перехід на віддалену роботу, диверсифікація офісів, резервні інфраструктури) і підтримувати безперервність діяльності. Водночас негативні наслідки війни для бізнесу очевидні: скорочення інвестицій та платоспроможного попиту всередині країни, утрата персоналу (частина фахівців мобілізована або виїхала за кордон), порушення ланцюгів постачання обладнання, а також енергетична криза через обстріли інфраструктури.

Кіберпростір став одним із основних полів битви у гібридній війні. Російські хакерські групи систематично атакують українські державні органи, інфраструктуру та приватні компанії. Для стартапів, які зазвичай значною мірою покладаються на ІТ-інфраструктуру і хмарні сервіси, кіберзагрози особливо небезпечні. Злочинці можуть викрасти інтелектуальну власність (вихідний код, ноу-хау), порушити роботу онлайн-платформ або шантажувати витоком конфіденційних даних. Показовим є інцидент у грудні 2024 року, коли українські оборонні стартапи зазнали масованої

[1] Климчук О. Результати спільного дослідження Sayenko Kharenko та Асоціації "IT Ukraine" щодо стану і перспектив релокації ІТ-компаній «Релокація. Новий ІТ-ландшафт України». Sayenko Kharenko. Медіа, технології та комунікації. 05.09.2022. URL: https://sk.ua/uk/rezultati-spilnogo-doslidzhennja-sayenko-kharenko-ta-asociacii-it-ukraine-shhodo-stanu-i-perspektiv-relokacii-it-kompanij-relokacija-novij-it-landshaft-ukraini/

цільової кібератаки: хакерське угруповання «UAC-0185» розсилало фішингові листи начебто від Українського союзу промисловців і підприємців із запрошенням на захід, сподіваючись інфікувати комп'ютери співробітників оборонних компаній[1]. Метою було отримання несанкціонованого доступу та викрадення даних про новітні військові розробки. Цей випадок підтверджує, що стартапи оборонного та ІТ-сектору перебувають під прицілом кібершпигунства в умовах війни.

Попри те, що в Постанові КМУ № 430 юридично закріплено визначення «стартапу» як суб'єкта малого чи середнього підприємництва або авторського колективу (куди можуть входити здобувачі освіти, науковці, науково-педагогічні працівники та інші фізичні особи), діяльність якого спрямована на розроблення, створення, впровадження й реалізацію інноваційної продукції та пошук бізнес-моделі для подальшого масштабування й розвитку[2], чіткої регламентації таких компаній у законодавстві все ще немає. Відтак стартапи фактично керуються загальними нормативно-правовими актами, не маючи спеціалізованого правового режиму.

Фактично стартап діє як суб'єкт підприємництва (найчастіше як ТОВ або ФОП), тому на нього поширюються всі загальні вимоги господарського та цивільного законодавства. Засновники стартапу повинні обрати організаційно-правову форму відповідно до чинного права – зазвичай це фізична особа-підприємець або товариство з обмеженою відповідальністю.

Кожна форма має свої переваги й недоліки (наприклад, ФОП – простота реєстрації, ТОВ – кращі можливості для залучення інвесторів). Права та обов'язки учасників оформлюються установчими документами (статутом, корпоративним договором тощо). Діяльність стартапів підпадає під дію базових законів у сфері підприємництва, інвестицій та інновацій, зокрема: Закону України «Про підприємни-

[1] Кіберзлочинці здійснили спробу атакувати оборонні підприємства та українських захисників. Державна служба спеціального зв'язку та захисту інформації України. Новини. 09.12.2024. URL: https://cip.gov.ua/ua/news/cert-ua-warns-of-phishing-attacks-targeting-ukrainian-defense-sector

[2] Про реалізацію експериментального проекту щодо створення на базі закладів вищої освіти, наукових установ мережі стартап-шкіл – інкубаторів – акселераторів: Постанова Кабінету Міністрів України від 23.04.2024, № 430: станом на 23.04.2024. URL: https://zakononline.com.ua/documents/show/526645___768767

цтво»[1], Закону України «Про інвестиційну діяльність»[2], Закону України «Про режим іноземного інвестування»[3], Закону України «Про інноваційну діяльність»[4]. Ці акти визначають загальні засади ведення бізнесу, залучення інвестицій і державної підтримки інновацій відповідно. Спеціальні правові режими також використовуються для стимулювання стартап-екосистеми. Зокрема, з 2022 року в Україні діє режим «Дія City» – унікальна правова та податкова платформа для ІТ-індустрії. Режим запроваджено Законом України «Про стимулювання розвитку цифрової економіки»[5]. Метою є створення сприятливих умов для високотехнологічного бізнесу та залучення інвестицій у цю сферу. Резидентам «Дія City» пропонуються податкові пільги (знижений податок на доходи працівників, особливий податок на виведений капітал), гнучкі умови найму ІТ-спеціалістів через гіг-контракти, можливість опціонних програм для співробітників та інші стимули.

Окрім законів про бізнес та інвестиції, для стартапів дуже важливо національне законодавство у сфері інтелектуальної власності, цифрових технологій та кібербезпеки. Закони України про охорону інтелектуальної власності забезпечують правову охорону результатів творчої діяльності стартапів. Так, діють Закони України «Про авторське право і суміжні права»[6] та «Про охорону прав на винаходи і корисні моделі»[7], «Про охорону прав на знаки для товарів і послуг»[8]

[1] Закон України «Про підприємництво». Верховна Рада України від 26.02.1991, № 698-XII: станом на 11.02.2022. URL: https://zakon.rada.gov.ua/laws/show/698-12#Text

[2] Закон України «Про інвестиційну діяльність» Верховна Рада України від 18.09.1991, № 1560-XII: станом на 10.10.2022. URL: https://zakon.rada.gov.ua/laws/show/1560-12#Text

[3] Закон України «Про режим іноземного інвестування»: Верховна Рада України від 19.03.1996, № 93/96-ВР: станом на 03.09.2024. URL: https://zakon.rada.gov.ua/laws/show/93/96-%D0%B2%D1%80#Text

[4] Закон України «Про інноваційну діяльність»: Верховна Рада України від 26.12.2002, № 40-IV: станом на 31.03.2023. URL: https://zakon.rada.gov.ua/laws/show/40-15#Text.

[5] Закон України «Про стимулювання розвитку цифрової економіки в Україні»: Верховна Рада України від 01.12.2022. № 1667-IX: станом на 01.01.2025. URL: https://zakon.rada.gov.ua/laws/show/1667-20#Text.

[6] Закон України «Про авторське право і суміжні права»: Верховна Рада України від 01.12.2022, № 2811-IX: станом на 10.10.2024. URL: https://ips.ligazakon.net/document/T222811?an=3.

[7] Закон України «Про охорону прав на винаходи і корисні моделі»: Верховна Рада України від 23.12.1993, № 3687-XII: станом на 31.12.2023. URL: https://zakon.rada.gov.ua/laws/show/3687-12#Text.

[8] Закон України «Про охорону прав на знаки для товарів і послуг»: Верховна Рада України від 23.12.1993, № 3689-XII: станом на 29.12.2024. URL: https://zakon.rada.gov.ua/laws/show/3689-12#Text.

тощо. Вони дозволяють засновникам стартапу захистити свої ідеї: зареєструвати патент на винахід, отримати свідоцтво на торговельну марку, зареєструвати авторське право на програмне забезпечення.

В умовах війни зросло значення законодавства про кібербезпеку. Закон України «Про основні засади забезпечення кібербезпеки України»[1] визначає рамки захисту критичної інформаційної інфраструктури та координацію між державними органами у протидії кібератакам. Стартапи, як і інші суб'єкти, зобов'язані дотримуватися вимог кібербезпеки, особливо якщо вони є постачальниками ІТ-послуг для держави або володіють важливими даними. Держава під час війни приймає додаткові нормативні акти, спрямовані на захист кіберпростору, але на жаль, раніше правова система недостатньо враховувала виклики гібридної війни – ні концепції розвитку законодавства, ні доктрина не були адаптовані до феномену гібридної агресії, що триває з боку росії. Лише після 2014 р. окремі закони ухвалювалися з поправками на збройний конфлікт (статус окупованих територій, права внутрішньо переміщених осіб тощо), але цілісного концепту приватно-правового регулювання в умовах гібридної війни не розроблено. Ця прогалина наразі стає очевидною і спонукає до оновлення національного законодавства з урахуванням воєнних реалій.

Діяльність стартапів в Україні також підпадає під вплив міжнародного права та зобов'язань держави. По-перше, Україна є учасницею основних міжнародних договорів у сфері інтелектуальної власності (Паризька конвенція, Бернська конвенція, Договір СОІВ, Угода ТРІПС тощо), що забезпечує визнання прав українських стартапів на винаходи, торговельні марки і твори за кордоном. По-друге, у цифровій сфері Україна імплементує норми Європейського Союзу згідно з Угодою про асоціацію. Це стосується, зокрема, правил електронної комерції, захисту персональних даних, електронних довірчих послуг і телекомунікацій. Відповідно, українські стартапи мають орієнтуватися на європейські стандарти у своїй онлайн-діяльності. Так, Закон України «Про електронну комерцію», гармонізований з директивами ЄС, визначає організаційно-правові засади електронної торгівлі в Україні, встановлює порядок укладення електронних пра-

[1] Закон України «Про основні засади забезпечення кібербезпеки України»: Верховна Рада України від 05.10.2017, № 2163-VIII: станом на 28.06.2024. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

вочинів та права й обов'язки учасників e-commerce[1]. Цей закон закріплює юридичну силу електронного договору та електронного підпису, що особливо важливо в умовах воєнного часу, коли багато угод укладаються віддалено. По-третє, у царині кібербезпеки Україна співпрацює з міжнародною спільнотою: наша держава приєдналася до Будапештської конвенції про кіберзлочинність, що дозволяє ефективніше розслідувати хакерські атаки на бізнес спільно з іноземними правоохоронцями. Крім того, на глобальному рівні обговорюються ініціативи на кшталт «Цифрової Женевської конвенції» щодо заборони руйнівних кібератак на мирні об'єкт[2]. Цей проєкт, запропонований експертами, передбачає домовленості між державами та ІТ-корпораціями про невтручання в критичні цифрові системи одне одного. Хоча формально він не прийнятий, сама ідея відображає прагнення встановити міжнародні правила, які б захищали приватний сектор (у тому числі стартапи) від військових кібероперацій.

В умовах гібридної війни держава змушена коригувати регуляторні підходи. З початком воєнного стану було прийнято низку нормативних актів, спрямованих на підтримку бізнесу: спрощення податкового навантаження, мораторії на окремі перевірки, продовження строків подання звітності тощо. Стартапи могли скористатися цими полегшеннями для збереження діяльності. Також запроваджено програми державних грантів для стартапів навіть під час війни. Правова система адаптується і в частині судочинства, що дозволяє проведення судових засідань в режимі відеоконференції, продовжено процесуальні строки, призупинено виконання зобов'язань на окупованих територіях тощо. Однак, слід наголосити, що й досі відсутня цілісна концепція правового регулювання приватноправових відносин в умовах гібридної війни, яка б забезпечила системну реакцію права на нові виклики. На законодавчому рівні необхідно визначити особливі правові режими для бізнесу під час війни, механізми компенсації збитків від воєнних дій, гарантії для інвесторів, що працюють в Україні попри ризики.

Попри умови гібридної війни, запуск стартапу й без того лишається ризикованою справою з типовими проблемами, котрі в умовах

[1] Закон України «Про електронну комерцію»: Верховна Рада України від 03.09.2015, № 675-VIII: станом на 01.01.2024. URL: https://zakon.rada.gov.ua/laws/show/675-19#Text.

[2] Microsoft права: нам потрібна цифрова Женевська конвенція. 13 травня 2017. URL: https://www.imena.ua/blog/microsoft-digitalgeneva-convention/

воєнних дій лише посилюються. На початковому етапі засновники стикаються з вибором організаційно-правової форми та структуруванням бізнесу. Як згадувалось, стартап зазвичай реєструється як ТОВ або ФОП[1]. ТОВ надає змогу залучати співзасновників та інвесторів в обмін на частки, але вимагає розробки статуту, можливого укладення корпоративного договору між засновниками про розподіл часток, прибутку, опціонів тощо. Нерідко українські стартапи обирають реєстрацію за кордоном (у США, Естонії, Польщі) – це робиться для спрощення доступу до іноземних інвестицій і ринків[2]. Така практика створює додаткові юридичні виклики: потрібно враховувати вимоги як українського, так і іноземного законодавства, будувати структуру групи компаній, розподіляти права на інтелектуальну власність між українською командою та материнською компанією за кордоном тощо.

Отримання достатнього фінансування – один з найскладніших аспектів розвитку стартапу. В мирний час стартапи покладаються на кошти засновників, венчурні фонди, державні гранти (в Україні діє Український фонд стартапів, що надає грантове фінансування на ранніх стадіях)[3]. Але війна призвела до відтоку капіталу та обережності інвесторів. Багато міжнародних фондів взяли паузу у фінансуванні українських проєктів через високі ризики. Відповідно, стартапам стало складніше залучити seed-інвестиції або серію А. Інше питання – оцінка компанії: у кризовий час оцінки падають, і фаундерам доводиться погоджуватися на менш вигідні умови заради виживання. Проте системно питання інвестування стартапів у воєнний час потребує додаткових рішень – таких як державні гарантії інвестицій, страхування військових ризиків для інвесторів, податкове стимулювання венчурних вкладень.

Інтелектуальні активи – це серце більшості стартапів, адже саме унікальна ідея, технологія чи контент складають основну цінність

[1] Бояринова К. О., Копішинська К. О. Особливості законодавчого регулювання діяльності стартап-компаній в Україні. Економічний вісник НТУУ «Київський політехнічний інститут». 2017. № 17: Інноваційно-інвестиційні процеси. URL: https://ev.fmm.kpi.ua/article/view/108722/103670.

[2] Драпій В. Навіщо реєструвати компанію в іншій країні: 5 причин. MC. Today. 25.05.2021. URL: https://surl.li/ffvwtw.

[3] Фінансування та програми підтримки. Дія Бізнес. URL: https://business.diia.gov.ua/finance/programs/finance?filter=%7B%7D&order=%7B%22id%22:%22DESC%22%7D&currentPage=1&itemsPerPage=9&category=%5B2,5,9,10,11%5D.

компанії. Правовий захист інтелектуальної власності є критично важливим, особливо коли стартап залучає інвесторів або виходить на глобальний ринок. В Україні засновники мають можливість оформити права на свої напрацювання: отримати патенти на винаходи або корисні моделі (якщо стартап має технічні інновації), зареєструвати торговельну марку на бренд продукту, зареєструвати авторські права на програмне забезпечення, бази даних, дизайн тощо[1]. Вибір типу охорони залежить від характеру об'єкту: так, для унікального алгоритму може підійти патент на винахід, для мобільного додатку – авторське право на код та товарний знак на назву. Проблемою є те, що процедура патентування може тривати довго та вимагати витрат, а стартап часто обмежений у коштах та часі. В даному випадку міг би стати в нагоді механізм прискореної реєстрації інтелектуальної власності для критичних технологій чи компенсації витрат на патентування. Ще один виклик – забезпечити, щоб усі права належали саме компанії: якщо продукт створювався співзасновниками чи найманими працівниками, треба оформити договори про передачу прав. Інакше можливі конфлікти, коли, наприклад, звільнений програміст претендує на частку в продукті. Типовий спір у стартапах – це спір між співзасновниками за права на інтелектуальну власність: трапляється, що на старті не було письмових домовленостей, і коли проєкт починає приносити дохід, виникають претензії щодо того, кому належать розробки. Українські суди при розгляді таких спорів виходять із положень національного законодавства про інтелектуальну власність. Важливим є доказ фіксації вкладення кожного зі сторін та наявність договорів. Практика показує, що належне оформлення прав інтелектуальної власності на ранніх стадіях (реєстрація об'єктів, договори між співзасновниками) значно знижує ризик конфліктів у майбутньому. Крім того, війна підвищила ризики піратства та промислового шпигунства: відсутність належного захисту спрощує недобросовісним конкурентам копіювання українських розробок. Тому стартапам варто дбати не лише про юридичну охорону, а й про кіберзахист своїх ноу-хау (шифрування даних, контроль доступу,

[1] Бояринова К. О., Копішинська К. О. Особливості законодавчого регулювання діяльності стартап-компаній в Україні. Економічний вісник НТУУ «Київський політехнічний інститут». 2017. Т. 17: Інноваційно-інвестиційні процеси. URL: https://ev.fmm.kpi.ua/article/view/108722/103670.

договорів про нерозголошення з усіма, хто має доступ до коду). На міжнародному рівні українські інноватори можуть користуватися системою PCT (межнародна заявка на патент) та Мадридською системою для знаків, щоб забезпечити охорону своїх прав на інтелектуальну власність на ключових ринках[1].

Більшість стартапів оперує в онлайн-середовищі, тож велика частина їх договірних відносин укладається електронно: через веб-інтерфейси, мобільні додатки, обмін електронними документами. Українське законодавство достатньо добре пристосоване для цього. Закон України «Про електронну комерцію» чітко визнає, що електронні правочини є юридично чинними, якщо дотримано необхідних вимог (ідентифікація сторін, волевиявлення в електронній формі тощо)[2]. Такі угоди прирівняні до письмових договорів, тобто, стартап може укласти договір з клієнтом шляхом акцепту публічної оферти на сайті або обміну електронними підписами під скан-копією договору – і такий контракт буде легітимним. В Україні діє інфраструктура електронного підпису та печатки відповідно до Закону України «Про електронну ідентифікацію та електронні довірчі послуги», який імплементує регламент eIDAS[3]. Тож компанії можуть підписувати документи кваліфікованим електронним підписом (КЕП), що юридично рівнозначний власноручному. Пандемія COVID-19 привчила бізнес до дистанційного укладення угод, а війна зробила це часто єдино можливим. Цифрові транзакції – це не лише укладення договорів, а й розрахунки, облік, звітність. В цій сфері в Україні впроваджено чимало новацій: система електронного документообігу, електронні рахунки та інвойси, електронні податкові накладні тощо. Стартапи широко застосовують онлайн-платежі через платіжні сервіси. Правове регулювання платіжних послуг також змінюється – було ухвалено Закон України «Про платіжні послуги»[4] для гармонізації з європейською

[1] Інтелектуальна власність та патентознавство: підручник. За ред. П. М. Цибульова, А. С. Ромашко. Київ: КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. 374 с.

[2] Закон України «Про електронну комерцію»: Верховна Рада України від 03.09.2015, № 675-VIII: станом на 01.01.2024. URL: https://zakon.rada.gov.ua/laws/show/675-19#Text.

[3] Закон України «Про електронну ідентифікацію та електронні довірчі послуги»: Верховна Рада України від 05.10.2017, № 2155-VIII: станом на 18.12.2024. URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text

[4] Закон України Про платіжні послуги: Верховна Рада України від 30.06.2021, № 1591-IX: станом на 15.11.2024. URL: https://zakon.rada.gov.ua/laws/show/1591-20#Text.

директивою[1]. Це відкриває можливості для fintech-стартапів, зокрема в напрямку відкритого банкінгу. Щодо smart contracts (розумних контрактів на блокчейні) – поки що українське право не має прямих норм, але такі механізми можуть застосовуватися як особливий спосіб фіксації виконання зобов'язань, за умови, що базовий юридичний договір все ж існує.

Окремо варто згадати про правовий режим віртуальних активів, адже чимало стартапів працюють у сфері криптовалют, NFT, блокчейн-рішень. Незважаючи на проєкт спеціального Закону України «Про віртуальні активи»[2], який вводить правове поле для крипто-ринку, наявна відсутність повної регуляції, в Україні де-факто діє досить ліберальний режим для криптовалют, що дозволяє стартапам-обмінникам чи блокчейн-платформам працювати (на свій ризик) і взаємодіяти з банками. На фоні війни криптовалюти стали важливим інструментом – зокрема, для благодійних зборів. Для стартапів, залучених у крипто, важливо мати прозорі правила гри, аби легально залучати інвестиції через токенізацію, випуск NFT, проводити ICO/ITO в рамках закону.

Таким чином, створення та масштабування стартапу супроводжується комплексом правових завдань: обрання форми бізнесу, оформлення відносин між співзасновниками, залучення інвестицій, захист інтелектуальної власності, налаштування договорів з клієнтами і партнерами (все частіше – в електронній формі), забезпечення відповідності вимогам цифрового законодавства. У воєнний час до цього додаються нові виклики: необхідність враховувати форс-мажори у договорах, додатковий контроль кібербезпеки, побудова гнучких ланцюгів поставок. Правове поле поступово підлаштовується під ці виклики, забезпечуючи інструменти (е-договори, захист інтелектуальної власності, регулювання fintech) для розвитку інновацій навіть у складних умовах.

В рамках даного питання також слід розглянути міжнародний досвід регулювання діяльності стартапів під час криз і конфліктів та можливості його адаптації в Україні. Однією з країн, яка історично

[1] Цимбалюк Х. О. Порівняльно-правовий аналіз PSD2 та проєкта нової платіжної директиви PSD3 і регламентів. Юридично науковий журнал DeIure. 2024. Т. 1. URL: https://www.deiure.in.ua/index.php/journal/article/view/3.

[2] Проєкт Закону України Про віртуальні активи: Верховна Рада України від, № 2074-IX: станом на 15.11.2024. URL: https://zakon.rada.gov.ua/laws/show/2074-20#Text.

розвивала потужну стартап-екосистему на тлі тривалого конфлікту, є Ізраїль, який попри постійну військову напругу змогла створити сприятливі умови для інноваційного бізнесу. Ключову роль відіграє державна підтримка: Міністерство інновацій, науки та технології Ізраїлю надає гранти технологічним стартапам і стимулює комерціалізацію військових розробок у цивільному секторі. В результаті під час критичних ситуацій і терактів ізраїльське стартап середовище продовжувало зростати. Так, у 2024 році, попри безпекові виклики, ізраїльські технологічні компанії залучили рекордні $12,2 млрд фінансування, продемонструвавши 31% зростання порівняно з попереднім роком[1]. Водночас ізраїльська практика висвітлює й низку викликів, зокрема можливе відлякування інвесторів унаслідок конфліктів. Щоб підтримати бізнес, уряд Ізраїлю запроваджував надзвичайні програми, завдяки яким компанії отримували пряме фінансування для виплати зарплат і продовження проєктів у кризовий період[2].

У часи економічних криз багато урядів зверталися до стимулювання підприємництва як драйвера відновлення. Наприклад,після кризи доткомів та рецесії 2008 США спростив краудінвестинг, дозволивши стартапам залучати кошти від широкого кола інвесторів через онлайн-платформи[3]. Цей досвід може бути корисним Україні під час війни: вже зараз з'являються українські платформи на кшталт AngelsDeck чи фонди військових облігацій, де технологічні проєкти можуть отримати мікроінвестиції від громадян.

На підставі міжнародного досвіду доцільно запропонувати комплекс правових заходів для вдосконалення регулювання стартапів в Україні як у воєнний, так і в післявоєнний період. Зокрема, доцільним є запровадження спеціальних стимулів для інвесторів (наприклад, податкових пільг чи гарантій). В українському контексті це може реалізуватися у формі податкової знижки для ІТ-компаній, які інвестують у вітчизняні стартапи, або шляхом страхування воєнних

[1] Hennessey Z. Despite war and tension, Israeli high-tech had a great year. Israel21c. Innovation. 16.02.2025. URL: https://www.israel21c.org/despite-war-and-tension-israeli-high-tech-had-a-great-year/#:~:text=achieving%20significant%20growth%20despite%20significant,regional%20challenges.

[2] Wrobel S. Israel Innovation Authority extends $25 million lifeline to startups amid war. The Times of Israel. 10.10.2023. URL: https://www.timesofisrael.com/israel-innovation-authority-extends-25-million-lifeline-to-startups-amid-war/#:~:text=,in%20assistance%20grants.

[3] Jumpstart our business startups act: 112th Congress від 05.04.2012, № 112–106. URL: https://www.congress.gov/112/plaws/publ106/PLAW-112publ106.pdf.

ризиків за участі міжнародних організацій. Також доцільно впровадити механізми надання грантів чи створити Фонд відновлення стартапів із застосуванням надзвичайних програм, аналогічних ізраїльським, що покликані захистити інноваційні проєкти від згортання через тимчасові труднощі.

Окрім того, важливим є правове запровадження регуляторів у галузях, які є критичними для відбудови (наприклад, фінтех, енергетика, медичні технології), завдяки чому стартапи матимуть змогу впроваджувати новації в умовах часткового звільнення від жорстких ліцензійних обмежень, перебуваючи під наглядом відповідного регулятора. Як підтверджує британський досвід, це сприяє динамічному розвитку великої кількості інноваційних компаній. Також необхідно вжити заходів для полегшення виходу стартапів на глобальні ринки, уклавши двосторонні міжнародні угоди щодо взаємного визнання електронних транзакцій та посиленої співпраці в сфері стартап-ініціатив.

З огляду на шкоду, завдану війною інноваційній інфраструктурі (фізичне знищення чи переміщення стартап-хабів), доцільно задіяти чинний Закон України «Про наукові парки»[1] для розбудови мережі нових технопарків та інкубаторів у відносно безпечніших регіонах. Держава й міжнародні партнери мають можливість спільно стимулювати університети та дослідницькі центри створювати осередки підтримки стартапів, а компаніям-резидентам технопарків надавати певні податкові й адміністративні пільги. Практика зарубіжних країн свідчить, що в умовах кризи слід насамперед мінімізувати надмірні ризики для стартапів за допомогою прямої фінансової підтримки і правових гарантій, водночас забезпечуючи їм достатню свободу для запровадження новаторських рішень. Україна вже започаткувала низку ініціатив на кшталт унікального правового та податкового простору для ІТ-компаній в Україні «Дія City»[2], проте може активніше застосовувати успішні зарубіжні зразки, тим самим надаючи інноваторам не лише шанси вижити в умовах війни, а й стати рушійною силою економічного зростання у післявоєнний період.

[1] Закон України Про наукові парки: Верховна Рада України від 25.06.2009, № 1563-VI: станом на 15.11.2024. URL: https://zakon.rada.gov.ua/laws/show/1563-17#Text.

[2] Закон України Про стимулювання розвитку цифрової економіки в Україні: Верховна Рада України від 01.12.2022, № 1667-IX: станом на 01.01.2025. URL: https://zakon.rada.gov.ua/laws/show/1667-20#Text.

У контексті правозастосовної практики та судового захисту стартапів, які стикаються із типовими спорами, зумовленими швидким зростанням і притаманною їм невизначеністю, найчастіше виникають правові колізії, пов'язані з об'єктами інтелектуальної власності. Адже саме вони зазвичай становлять найцінніший актив більшості новостворених технологічних компаній. Типовий приклад – конфлікт між співзасновниками або співробітником і компанією щодо того, кому належать права на створений продукт (програмний код, дизайн, бренд тощо). Якщо на старті не було чітко оформлено передачу прав компанії, то автор може заявити претензії. Українські суди розглядають такі справи на основі норм цивільного законодавства про розпорядження майновими правами інтелектуальної власності. Важливим доказом є договірні умови: якщо є договір з працівником чи контрагентом, що всі результати робіт переходять замовнику, суд зазвичай стає на бік компанії. Інший різновид спорів – захист стартапом своїх прав проти сторонніх порушників. Наприклад, копіювання конкурентою унікального інтерфейсу чи технології. Стартап може позиватися про припинення порушення і відшкодування збитків, посилаючись на патент або авторське право. Однак судовий захист ІВ може бути утруднений, якщо право не було формально зареєстровано (особливо щодо патентів і торговельних марок). Тому практика підтверджує, що превентивна реєстрація інтелектуальної власності є найкращим способом підвищити шанси на успіх у суді[1].

Коли стартап залучає зовнішнього інвестора, між сторонами оформлюють інвестиційну угоду, де фіксуються права інвестора (частка у статутному капіталі, місце в раді директорів, право вето) та обов'язки засновників[2]. Спір виникає, якщо засновники порушують узгоджені показники або нецільово використовують кошти – тоді інвестор може судитися за повернення інвестицій чи відшкодування. Навпаки, стартап може пред'явити претензії за невиконання інвестором зобов'язань щодо фінансування. Типовий приклад – оскарження рішень загальних зборів у разі ймовірного зловживання сторонами своїми правами. Незважаючи на військові обставини, господарські

[1] Бояринова К. О., Копішинська К. О. Особливості законодавчого регулювання діяльності стартап-компаній в Україні. *Економічний вісник НТУУ «Київський політехнічний інститут».* 2017. Т. 17. URL: https://ev.fmm.kpi.ua/article/view/108722/103670.

[2] Andhov A. Start-up Law: монографія. Cheltenham: Edward Elgar, 2020. 328 с. URL: https://doi.org/10.4337/9781839108457.

суди в Україні продовжують розгляд таких справ, хоч і з можливим продовженням строків.

Стартапи як суб'єкти цивільно-правових відносин зазвичай укладають численні договори з клієнтами (щодо надання послуг або реалізації товарів), постачальниками, фрілансерами тощо, а будь-яке порушення чи неналежне виконання таких угод тягне за собою претензії, що регулюються нормами цивільного та господарського права. В умовах війни особливого значення набула категорія форс-мажору: воєнні дії, мобілізація та збої в постачанні кваліфікуються як обставини непереборної сили, які дають сторонам змогу посилатися на них для звільнення від відповідальності за невиконання або несвоєчасне виконання контрактів. Торгово-промислова палата України оперативно розпочала видачу сертифікатів про форс-мажорні обставини, зумовлені воєнними діями[1]. Судова практика з цих питань вже набула певної усталеності: зокрема, Верховний Суд у одній із справ вказав, що форс-мажор може впливати на виконання лише окремих зобов'язань і не поширюватися на інші, залежно від характеру конкретного зобов'язання та фактичних обставин щодо боржника[2]. Тобто наявність війни автоматично не звільняє від усіх зобов'язань, потрібен причинно-наслідковий зв'язок між подією війни і неможливістю виконати конкретний договір. Таким чином, стартапам при настанні форс-мажору потрібно належно повідомляти контрагентів, отримувати сертифікати Торгово-промислової палати України і, за можливості, шукати альтернативне виконання, щоб уникнути спорів.

Стартапи є невід'ємною частиною сучасної інноваційної економіки, генераторами технологічного прогресу та важливим чинником економічного зростання. В умовах гібридної війни розвиток стартап-екосистеми України набуває стратегічного значення: успішні стартапи не лише сприяють економічній стійкості під час конфлікту, а й закладають підвалини для післявоєнного відновлення країни. Як зазначалось раніше, правове поле стартапів в Україні

[1] Щодо засвідчення форс-мажорних обставин. Торгово-промислова палата України. 26.12.2024. URL: https://ucci.org.ua/press-center/ucci-news/protsedura-zasvidchennia-fors-mazhornikh-obstavin-z-28-02-2022.

[2] Кібенко О. Практика Верховного Суду щодо форсмажору та істотної зміни обставин. Міжнародний судово-правовий форум. 2024. Т. II. С. 30. URL: https://supreme.court.gov.ua/userfiles/media/new_folder_for_uploads/supreme/2024_prezent/Prezent_fors_major_14_06_2024.pdf.

складається з багатьох фрагментів законодавства – підприємництво, інвестиції, інтелектуальна власність, ІТ, кібербезпека – але досі не має єдиного комплексного акту, який би визначав спеціальний статус стартап-компаній. Гібридна війна створила нові виклики для стартапів: прямі загрози (фізичне знищення майна, кібератаки, відтік кадрів) і опосередковані проблеми (економічна криза, зменшення інвестицій).

Правове регулювання стартапів у контексті війни почало коригуватися: запроваджено спеціальні режими підтримки (Дія City) та антикризові заходи (податкові пільги, мораторії, підтвердження форс-мажору), проте ці кроки поки точкові. Національне законодавство потребує комплексної модернізації з урахуванням викликів гібридної агресії, адже ця форма війни засвідчила відсутність інтегрованої приватно-правової концепції реагування на воєнні загрози. Зокрема, виявилися проблеми із правовим режимом майна і зобов'язань на окупованих територіях, із захистом прав внутрішньо переміщених осіб, із застосуванням категорії форс-мажору тощо. У сфері стартапів це проявилось у питаннях: як забезпечити дотримання контрактів, якщо сторони розкидані по світу; як захистити ноу-хау компанії від ворожих кібератак; як зберегти інвестиції, якщо бізнес тимчасово не може працювати на повну силу. Українська судова практика вже виробляє правові механізми реагування, зокрема Верховний Суд уточнив критерії звільнення від відповідальності у зв'язку з воєнними діями[1].

З метою вдосконалення правового регулювання стартапів в умовах воєнного та післявоєнного періоду доцільно передбачити системні зміни в національному законодавстві. По-перше, варто ухвалити спеціальний закон або внести доповнення до чинних актів з метою визначення правового статусу стартап-компаній (наприклад, закріпивши чіткі критерії «інноваційного малого підприємства» та механізми державної підтримки). По-друге, необхідно розробити податкові стимули та фінансові пільги (тимчасове звільнення від сплати податку на прибуток за умови реінвестування, податковий кредит на дослідницькі і дослідно-конструкторські роботи, зниження ЄСВ у період військового стану тощо).

[1] Петрушина К. Судова практика щодо форс-мажору та виконання договірних зобов'язань. Li*ga Zakon*. Судова практика. 18.11.2024. URL:https://surl.li/gdkykp.

Також доцільно запровадити механізм державного страхування й гарантування інвестицій у стартапи, зокрема у співпраці з міжнародними фінансовими інституціями. У сфері кібербезпеки слід деталізувати вимоги до бізнесу, що працює з критичними даними або в оборонній галузі, і посилити відповідальність за кібершпигунство в умовах війни. Для захисту прав стартапів варто уніфікувати підхід судів до форс-мажору, впроваджувати медіацію та створити спеціалізований арбітраж при торгово-промисловій палаті, аби прискорити розгляд технічних спорів.

У контексті інтеграції на європейський ринок бажано гармонізувати законодавство з регуляціями Європейського Союзу, а також спростити митні процедури для ввезення та вивезення обладнання. Нарешті, слід передбачити полегшений доступ стартапів до державних замовлень і закупівель, щоб держава могла оперативно залучати інноваційні розробки (дрони, програмне забезпечення для військових потреб), тим самим стимулюючи становлення й розвиток українських інноваційних компаній.

Слід зазначити, що правове регулювання стартапів має бути динамічним і випереджувальним, особливо в умовах гібридних викликів. Сьогоднішня війна – це не лише битва танків і ракет, а й змагання технологій, економік і правових систем. Українські стартапи вже довели свою життєздатність під тиском агресії, тепер завдання держави – вдосконалити правове середовище так, щоб максимально сприяти їх появі, зростанню і захисту. Необхідні «гібридні відповіді» правовими засобами на гібридні загрози: гнучке законодавство, що враховує воєнні реалії, ефективні судові та альтернативні механізми захисту, а також інтеграція найкращих світових практик. У підсумку, це зміцнить економічний фронт країни і наблизить нашу перемогу не лише на полі бою, а й у глобальному конкурсі інновацій.

Ключові слова: стартап, інноваційна діяльність, інтелектуальна власність, ДіяCity, кібербезпека.

Розділ 17

Е-КРЕДИТУВАННЯ У ПЕРІОД ВОЄННОГО СТАНУ

DOI

Олена Берназ-Лукавецька
кандидатка юридичних наук, доцентка

Онлайн кредитування

Цивільний кодекс України містить визначення кредитного договору, за яким банк або інша фінансова установа (кредитодавець) зобов'язується надати грошові кошти (кредит) позичальникові у розмірі та на умовах, встановлених договором, а позичальник зобов'язується повернути кредит та сплатити проценти.

Згідно зі ст. 1 Закону України «Про фінансові послуги та фінансові компанії» від 14.12.2021 р. надавачем фінансових послуг може виступати фінансова установа, а у випадках, прямо визначених спеціальними законами, – інша юридична особа або філія іноземної юридичної особи, яка має право надавати фінансові послуги відповідно до цього Закону та спеціальних законів.[1]

Протягом останніх десятиліть світова банківська індустрія знаходиться в умовах жорсткої конкурентної боротьби, зокрема зараз у період дії воєнного стану. Поява нових інформаційних технологій чинить серйозний вплив на вироблення стратегічної політики банку. Нинішні зміни в банківській сфері пов'язані з впливом ряду факторів, в числі яких міжнародна тенденція до глобалізації ринку банківських послуг, зміна законодавства, а також розвиток інформаційних технологій.

Інформаційні технології (ІТ) кардинально змінюють кредитну сферу, підвищуючи ефективність, безпеку та доступність фінансових послуг. Вони охоплюють широкий спектр програмних та апаратних

[1] Про фінансові послуги та фінансові компанії: Закон України від 14 грудня 2021 р. № 953-IX. *Відомості Верховної Ради України.* 2023. № 3-4. Ст. 10.

засобів, які використовуються для обробки, зберігання, передачі та аналізу даних у кредитних операціях.

Можна з упевненістю говорити про те, що процес інформатизації банківської діяльності продовжиться і надалі. У банківському секторі в найближчому майбутньому будуть переважати тенденції до підвищення якості та надійності пропонованих продуктів і послуг, збільшення швидкості проведення розрахункових операцій, організації електронного доступу клієнтів до банківських продуктів. Це обумовлено, перш за все, прагненням банків до досягнення конкурентних переваг на фінансових ринках.

На даний час ринок програмних продуктів для кредитних організацій представлений широким спектром систем, що розрізняються як функціональною частиною, так і технічною реалізацією, апаратною платформою, рівнем системного сервісу, методами захисту інформації і т.д.

Однак, будь-яка банківська інформаційна система обов'язково повинна відповідати наступним вимогам: можливість мережевої роботи багатьох користувачів; реалізація всього комплексу банківських операцій з розрахунково-касового обслуговування; кредитно-депозитної діяльності, валютних операцій; гнучке налаштування для доступу кінцевих користувачів; підтримка декількох апаратних платформ; автоматизоване формування більшої частини звітних форм, можливість їх перенастроювання і т.д. Цим вимогам в даний час задовольняють більшість систем для фінансових організацій, представлених на ринку програмних продуктів.

Всі банківські інформаційні системи можна розділити на дві великі групи: розроблені на основі технології файл / сервер або клієнт / сервер. Остання стала фактично стандартом. Вона має такі очевидні переваги, як висока швидкість обробки інформації, слабо залежить від кількості користувачів і обсягу оброблюваних даних; розвинені можливості захисту інформації, що, в свою чергу, обумовлено обробкою основного її обсягу на сервері, доступ до якого може бути фізично обмежений; гнучкість щодо вибірки і аналізу даних. Хоча необхідно зазначити, що така технологія висуває підвищені вимоги до апаратно-технічного забезпечення кредитної організації, перш за все до серверного та мережевого обладнання, на які лягає велика частина навантаження при обробці даних. Переваги реалізації клієнт / сервер-

ної системи в повній мірі проявляються при обробці значних обсягів інформації великим числом одночасно працюючих користувачів.

Говорячи про Інтернет-технології необхідно зазначити, що вони є важливою частиною банківської системи, вони успішно використовуються при обслуговуванні фізичних осіб. Розглянемо різновиди інтернет-технологій, що можуть використовуватися у кредитуванні.

Основними напрямки застосування ІТ в кредитній сфері є:

– Автоматизація процесів: ІТ дозволяють автоматизувати процеси кредитування, починаючи від подачі заявки та перевірки кредитної історії, до видачі та погашення кредиту. Це значно скорочує час обробки заявок та зменшує витрати.
– Електронна комерція та онлайн-кредитування: Інтернет та мобільні додатки дозволяють клієнтам отримувати кредити онлайн, що значно спрощує процес та робить його більш доступним.
– Управління ризиками: за допомогою ІТ банки та кредитні організації аналізують великі обсяги даних для оцінки кредитоспроможності клієнтів та управління кредитними ризиками. Це дозволяє приймати більш обґрунтовані рішення та знижувати ймовірність неповернення кредитів.
– Кібербезпека: застосування сучасних технологій шифрування та захисту даних забезпечує безпеку транзакцій та захист конфіденційної інформації клієнтів. [1]
– Зручність та доступність: онлайн-банкінг та мобільні додатки роблять кредитні послуги більш доступними для широкого кола користувачів, у тому числі для тих, хто раніше не мав можливості користуватися традиційними банківськими послугами.

Інтернет відіграє важливу роль в сучасному світі, допомагаючи швидко знайти необхідну інформацію. Наприклад, людям, зацікавленим в пошуку житла, і все, що з ним пов'язано, – це і способи державної підтримки при купівлі житла, пошук кредитора та вибір кредитування. Цю інформацію можна отримати на сайтах банків-кредиторів. За допомогою онлайн-видань, що містять інформацію про нерухомість, можна ознайомитися з інтернет-каталогами, що допомагають з вибором іпотечних програм. Також нову інфор-

[1] Інформаційні технології в нашому житті. URL: https://surl.li/fyinzc

мацію завжди можна знайти на офіційних сайтах державних і муніципальних органів влади.

Ще одним видом інтернет-технологій є іпотечні онлайн-калькулятори. За допомогою такої системи громадянин може розрахувати суму іпотечного кредиту, визначитися з початковим внеском і графіком погашення заборгованості, розрахувати процентну ставку. Онлайн-калькулятори допомагають порівняти різні пропозиції та прийняти обґрунтоване рішення щодо вибору іпотечного кредиту.

В основному банки створюють онлайн-калькулятори, включаючи туди умови якоїсь певної іпотечної програми, для полегшення розрахунку різних витрат.

Деякі калькулятори стали дуже популярними саме у період воєнного стану, наприклад, для програми «єОселя». Вони дозволяють розрахувати умови кредитування з урахуванням пільгових ставок та інших умов. [1] Програма «єОселя» передбачає пільгове кредитування на придбання житла для певних категорій громадян України. Умови програми включають вік позичальника (від 18 до 70 років на момент погашення), платоспроможність, відсутність у власності надмірного житла (52,5 кв. м + 21 кв. м на кожного члена сім'ї) та не участь в інших державних програмах забезпечення житлом. Також існують обмеження щодо типу та площі житла, яке можна придбати за програмою.

Програмою можуть скористатися громадяни України, які належать до певних пільгових категорій, або ті, хто відповідає загальним умовам участі. Серед них : військовослужбовці (за контрактом ЗСУ), СБУ, служби зовнішньої розвідки, ГУР, Нацгвардії, Держприкордонслужби, Управління державної охорони, Держспецзв'язку, Держспецтрансслужби, педагогічні, медичні та наукові працівники, Ветерани війни та члени їхніх сімей, учасники бойових дій, особи з інвалідністю внаслідок війни, члени сімей загиблих (померлих) ветеранів війни та захисників України, внутрішньо переміщені особи (ВПО).

Існує такий вид технологій як інтернет-консультація, тобто надання консультацій та порад спеціалістами (лікарями, психологами, юристами, консультантами тощо) за допомогою інтернет-зв'язку, таких як відео- та аудіоконференції, чати, електронна пошта. Це зручний спосіб отримати консультацію, не виходячи з дому, особливо коли особиста зустріч неможлива або небажана.

[1] Калькулятор іпотеки єОселя. URL: https://riel.ua/calculator-mortgage-home

До видів інтернет-консультацій, які стали найбільш популярними у пірод воєнного стану можна віднести:

- Медичні онлайн-консультації:

Лікарі можуть проводити консультації, діагностувати захворювання, давати рекомендації щодо лікування та контролювати стан пацієнтів через відеозв'язок, аудіо-повідомлення або текстові чати.

- Психологічні онлайн-консультації:

Психологи надають психологічну підтримку, проводять терапію та консультують з питань психічного здоров'я через відеозв'язок, аудіо-повідомлення або текстові чати.

- Консультації з різних галузей:

Онлайн-консультації можуть охоплювати широкий спектр питань, наприклад, консультації з фінансів, освіти, кар'єри, бізнесу тощо.

- Консультації для підтримки клієнтів:

Онлайн-консультанти допомагають клієнтам на сайтах та в додатках розібратися з продуктами, послугами та вирішити проблеми.

- Юридичні онлайн-консультації:

Юристи можуть надавати юридичні консультації та поради з правових питань за допомогою онлайн-інструментів. Такоє такі послуги можуть надаватися з питань кредитування. Це дуже зручна послуга, яка дозволяє подати заявку на кредит не виходячи з дому. Ще одна перевага цієї функції – можна подавати заявку в кілька банків. Також і для банківських працівників зручне використання цієї системи, вони можуть дистанційно консультувати клієнтів з приводу нових послуг і контролювати їх заборгованість. У період кризи, для деяких клієнтів буде цікава інформація з рефінансування і реструктуризації кредитів.

Також зараз, у зв'язку з тим, що багато українців знаходяться за кордоном у період воєнного стану введеного в Україні, набирають попит онлайн консультації з приводу купівлі нерухомості в кредит у країні перебування. Деякі країни Європейського Союзу пропонують можливість отримати посвідку на проживання при купівлі нерухомості. Наприклад, у Португалії, Греції, Італії та Франції існують такі програми.

Щодо недоліків онлайн консультацій, то до них можна віднести:

Обмежений невербальний контакт: складніше оцінити невербальні сигнали клієнта, такі як мова тіла та міміка, що може вплинути на точність діагностики та оцінки його правоздатності.

Технічні проблеми: залежність від стабільного інтернет-з'єднання та наявності необхідного обладнання.

Обмеження у деяких випадках: не всі питання у сфері кредитування можна вирішити онлайн, іноді потрібна особиста присутність.

В цілому, інтернет-консультації є корисним інструментом для отримання допомоги та підтримки у різних сферах життя, але важливо враховувати їхні переваги та недоліки, щоб зробити правильний вибір.

Також одним з достатньо нових продуктів, що з'явилися на ринку, стала можливість оплати рахунків через Інтернет. Нові технології оплати рахунків через Інтернет включають в себе використання систем інтернет-еквайрингу, таких як Click to Pay та мобільних платіжних систем, на кшталт Google Pay та Apple Pay, які дозволяють оплачувати покупки онлайн за допомогою банківських карток, а також нові платіжні методи, що використовують API для інтеграції з різними сервісами.

Інтернет-еквайринг для інтернет-магазину чи іншого онлайн-бізнесу – це послуга, яка передбачає обробку безготівкових транзакцій на власному веб-сайті компанії або на іншій платформі, через яку працює підприємець (наприклад, веб-сайт електронної комерції або соціальні мережі). Це означає, що платежі через інтернет стають простішими та доступнішими.

Більше того, з кожним роком безготівковий розрахунок стає все більш популярним та ефективним (а також простішим). Суть еквайрингу полягає в процесі обробки транзакції, де покупець оплачує товар або послугу за допомогою своєї картки, а продавець отримує гроші на свій рахунок. Навіть не знаючи цієї складної назви, багато хто користується еквайрингом вже

Існує кілька основних типів еквайрингу для онлайн-бізнесу.

1) Банківський еквайринг. До переваг можна віднести високий рівень безпеки. Крім того, в транзакції бере участь менше посередників, ніж при роботі через сторонні системи, завдяки чому комісії можуть бути відносно низькими. Кількість способів оплати обмежена: як правило, лише картки.
2) Платіжна система. Використовується сторонній сервіс онлайн-платежів. Такі сервіси інтернет-еквайрингу зазвичай мають вищі комісії, ніж банківські, але набір функцій більший,

від поглибленої статистики до розрахунку податків. Список доступних варіантів оплати ширший, ніж у банківського еквайрингу.

3) Криптоеквайринг. Система для прийому платежів у криптовалюті. Багато користувачів підключають її як додаткову послугу. Вона дозволяє працювати з клієнтами з-за кордону та пропонує високу безпеку та низькі комісії. [1]

Також виділяють торговий еквайринг – це система, яка дозволяє приймати банківські картки в магазинах, кафе, ресторанах та інших торгових точках. Тобто, бізнес спрощує процес прийняття платежів і для себе.

Суть процесу полягає в тому, що під час оплати покупець проводить своєю карткою через спеціальний пристрій – POS-термінал. Термінал надсилає інформацію про оплату до банку, який перевіряє, чи достатньо коштів на рахунку покупця, і або схвалює, або відхиляє транзакцію. Вся процедура займає кілька хвилин. У магазинах цей вид оплати практикується поряд з готівковими платежами вже давно.

Приклад того, як відбувається придбання:

1. Отже, клієнт хоче оплатити свою покупку.
2. Продавець вводить необхідну суму та просить клієнта оплатити карткою.
3. Покупець проводить своєю карткою (через термінал).
4. Запит надходить з термінала до банку (цей банк обслуговує саме цей термінал).
5. Банк надсилає запит до банку, який видав картку.
6. Другий банк перевіряє, чи достатньо коштів на рахунку, і підтверджує або відхиляє запит.
7. Транзакція або підтверджена, або відхилена. Тобто, покупка або оплачена, або ні.

Іноді в цьому процесі можуть виникати збої, але такі випадки трапляються рідко.

Варто сказати кілька слів про переваги торгового еквайрінгу у період воєнного стану: зручність для клієнтів – можливість оплачувати товари та послуги карткою, що зменшує потребу у використанні готів-

[1] TOP-6 Internet Acquiring Platforms and Their Features Overviewed. URL: https://cryptocloud.plus/en/blog/internet-acquiring-services-compilation

ки; збільшення продажів – клієнти частіше здійснюватимуть покупки, якщо мають можливість розрахуватися карткою; безпека – мінімізація ризиків, пов'язаних зі зберіганням та транспортуванням готівки. Не слід забувати про таку перевагу, як автоматизація бухгалтерського обліку – еквайринг дозволяє автоматично фіксувати та обробляти платежі [1].

Також такі технології дозволяють оплатити рахунки не виходячи з дому. Через Інтернет можна оплатити не тільки іпотеку, а й комунальні платежі, платежі за телефон і багато іншого. Ця система дуже зручна в експлуатації. Але поки вона не зовсім безпечна, оскільки Інтернет володіє низьким рівнем надійності. Тому не рекомендується зберігати дані вашого рахунку на комп'ютері або телефоні.

Необхідно підкреслити, що основними перевагами технологій оплати є:

- Зручність – швидка та проста оплата онлайн без необхідності вводити дані картки кожного разу.
- Швидкість: здійснення платежів за лічені секунди.
- Безпека: захист даних карток за допомогою шифрування та інших технологій.
- Доступність: можливість оплати в будь-який час і в будь-якому місці.
- Збільшення конверсії: зручність оплати може призвести до збільшення продажів.

Ще однією зручною послугою є отримання своєї кредитної історії онлайн. Така онлайн перевірка кредитної історії дозволяє дізнатися про платіжну дисципліну та наявність поточних та минулих кредитів позичальника. Це важливо, оскільки кредитна історія впливає на можливість отримання нових кредитів, умови кредитування (процентна ставка, ліміти) та може використовуватися для захисту від шахрайства.

Кредитна історія показує, як особа позичальника вчасно погашає кредити та чи є у позичальника прострочення. Це важливий фактор для банків та фінансових установ при прийнятті рішення про надання кредиту. Позитивна кредитна історія збільшує шанси на отримання кредиту на вигідніших умовах, таких як нижча процентна ставка або вищий кредитний ліміт.

[1] Trading and internet acquiring: what it is in simple terms. URL: https://112.ua/en/torgovyj-i-internet-ekvajring-cto-eto-takoe-prostymi-slovami-39686

Тобто, особа може замовити кредитний звіт – це документ, в якому відображається його кредитна історія, тобто інформація про поточні та минулі кредити, заборгованість і прострочення. Для перегляду такого кредитного звіту необхідно зайти на офіційний сайт і в спеціальному розділі ввести свої персональні дані.

Так,наприклад, перевірити кредитну історію онлайн можна на **сайті Українського бюро кредитних історій (УБКІ):** ubki.ua, або за допомогою **чат-боту УБКІ в Viber та Telegram: УБКІ**, а також **окремі банки та фінансові установи** такі як ПриватБанк, пропонують перевірку кредитної історії через свої онлайн-сервіси (наприклад, Приват24)[1].

Зазвичай для такої перевірки потрібні лише паспорт та ідентифікаційний код. Варто пам'ятати, що кредитна історія – це важливий інструмент для управління фінансовими ризиками, як для позичальників, так і для кредиторів.

Також прикладами впровадження ІТ у кредитній сфері є: системи автоматизованої обробки заявок (SAO)[2], які дозволяють автоматизувати процес перевірки документів, оцінки кредитоспроможності та прийняття рішень; системи управління ризиками, що Використовують алгоритми машинного навчання для аналізу великих обсягів даних та виявлення шахрайства, а також для оцінки ризиків непогашення кредитів; та онлайн-платформи для кредитування, які Забезпечують можливість подачі заявок на кредит та отримання коштів онлайн, а також управління кредитами через інтернет.

В цілому, інформаційні технології відіграють ключову роль у трансформації кредитної сфери, роблячи її більш ефективною, безпечною та доступною для всіх учасників.

Таким чином ми бачимо, що наразі інформаційні технології охоплюють все більше сфер людської життєдіяльності та ведення бізнесу. Не є винятком і є сфера надання кредитних послуг, у якій серед основних видів кредиту (банківський, споживчий тощо) з'являється та використовується ще один, а саме кредит он-лайн.

---

[1] Як стати партенром УБКІ? URL: https://www.ubki.ua/partner

[2] Інформаційні системи та технології в банківській сфері: методичні рекомендації до самостійної роботи студентів спеціальності 072 «Фінанси, банківська справа та страхування» першого (бакалаврського) рівня. Харків: ХНЕУ ім. С. Кузнеця, 2021. URL: https://surl.li/rnofzp

У тому числі, нинішні технології зробили допустимими появу електронного глобального фінансового ринку, який базується на інтеграційних системах, таких як: Телефонний банк, Банк-Клієнт, Інтернет, Інтернет Банк-Клієнт, рекомендовані в якості основних курсів просування банківських послуг.

Передові банки, які вивчають досвід, накопичений країнами заходу по застосування комунікаційних електронних систем, стали користуватися ним в своїй практиці.

Щодо он-лайн кредитування, то воно є послугою, за допомогою якою позичальник може подати он-лайн заявку на отримання кредиту (у тому числі отримати кредитну картку) за допомогою заповнення спеціальної форми на сайті кредитної організації. Після цього позичальник або отримує попереднє рішення про можливість кредитування прямо на сайті, або з ним зв'язується представник кредитора для подальшого розгляду цього питання.

Завдяки такій можливості подати заявку на он-лайн кредит в банк або іншу кредитну організацію особа заощаджує свій час та може дізнатися про перспективи отримання кредиту в необхідній сумі, не відвідуючи при цьому ці установи особисто.

Онлайн-кредитування стосується різних методів, які споживачі використовують для позики грошей або відстрочки платежів за онлайн-покупки. Ці методи включають кредитні картки, цифрові гаманці, банківські перекази, послуги «купи зараз, плати пізніше» та навіть криптовалюту для деяких платформ. По суті, всі вони передбачають можливість здійснювати покупки або отримувати доступ до коштів онлайн, з розумінням того, що повернення коштів відбудеться пізніше, або негайно, або з часом.

Можна виділити основні різновиди онлайн-кредитів:

1. Кредитні картки. Вони дозволяють користувачам позичати гроші для покупок та повертати залишок пізніше, часто з відсотками. Використовуються онлайн. Широко приймаються для онлайн-транзакцій через платіжні шлюзи. Прикладами є: Visa, Mastercard, American Express.

2. Цифрові гаманці. Вони зберігають платіжну інформацію (кредитні картки, банківські рахунки) для швидких онлайн-покупок. Сприяють швидшому оформленню замовлення шляхом безпеч-

ного зберігання платіжних даних. Приклади: PayPal, Apple Pay, Google Pay [1].

3. Банківські перекази. Прямий переказ коштів з одного банківського рахунку на інший. Поширені для великих покупок і можуть бути здійснені через платформи або додатки онлайн-банкінгу. Приклади: SEPA (для європейських банківських переказів), онлайн-банківські перекази.

4. Купуй зараз, плати пізніше (BNPL). Даний різновид дозволяє клієнтам купувати товари негайно та оплачувати їх пізніше, часто частинами, з відсотками або без них. Він стає дедалі популярнішим для онлайн-торгівлі. Приклади: Klarna, Afterpay.

5. Криптовалюта. Цифрові або віртуальні валюти, які можна використовувати для онлайн-транзакцій. Деякі онлайн-платформи та продавці приймають криптовалюту як спосіб оплати. Приклади: Bitcoin, Ethereum.

6. Передплачені картки. Картки, завантажені певною сумою грошей, яку можна використовувати для онлайн-покупок. Надають спосіб управління витратами та корисні для людей без традиційних банківських рахунків.

7. Платіжні шлюзи. Платформи, що обробляють онлайн-платежі, діючи як місток між клієнтом, продавцем та платіжними мережами. Вони сприяють безпечному переказу коштів для різних способів онлайн-платежів. Приклади: Stripe, Razorpay.[2]

Прикладом онлайн кредитування є також дистанційне оформлення товару в кредит в Інтернет магазинах (кредит на онлайн покупки). Найчастіше такими товарами є телефони, смартфони, побутова техніка. Особа може розраховувати на надання такого кредиту у розмірі від 1000 до 100 000,00 гривень, в залежності від строку надання кредиту, віку позичальника, початкового внеску, приблизного графіку погашення кредиту та ідентифікуючих документів позичальника (паспорта, ІНН, пенсійного посвідчення, тощо).[3]

---

[1] Different Types of Electronic Payment Systems with Advantages and Disadvantages. URL: https://razorpay.com/blog/types-of-electronic-payment-system/

[2] Accept Online Payments Seamlessly in India with Razorpay Payment Gateway- URL: https://razorpay.com/payment-gateway/

[3] Кредити на онлайн покупки фізичним особам. URL: https://sensebank.ua/privat-nim-osobam

Ще одним цікавим прикладом онлайн кредитування є отримання кредиту на короткий термін (наприклад, до моменту отримання заробітної плати). Деякі організації пропонують таку послугу як онлайн позика. Так, у Республіці Казахстан позичальник повинен виконати наступні дії для отримання позики он-лайн:

Подати заявку на отримання позики. Заявник (позичальник) повинен бути громадянином Республіки Казахстан або іноземним громадянином з видом на проживання, який проживає на території Республіки Казахстан та досяг віку 20 років, має постійну реєстрацію на території Республіки Казахстан.

При заповненні Заявником Заявки, Заявник надає Товариству (кредитору) наступну інформацію, включаючи, але не обмежуючись: розмір суми і термін видачі позики, який не може перевищувати 30 (тридцяти) календарних днів; фото документа, що посвідчує особу, отримані через Сайт або Мобільний додаток; фотографії Заявника, отримані через Сайт або Мобільний додаток; індивідуальний ідентифікаційний номер (ІІН); адреса проживання заявника; адреса електронної пошти; номер мобільного телефону.

Вказати суму Договору в Оферті при виборі суми позики на Сайті або в Мобільному додатку.

Позичальник зобов'язується повернути надану суму Позики і сплатити Винагороду за користування позикою в порядку і в терміни, обумовлені Договором.

1. Заявник, який має намір отримати Позику, повинен зареєструватися на Сайті або в Мобільному додатку шляхом заповнення Анкети, викладеної на Сайті і в Мобільному додатку. При цьому Заявник погоджується надати Товариству усю необхідну інформацію (див. п.2)
2. Після отримання необхідної інформації Товариство приймає рішення про видачу або відмову у видачі позики в розмірі та на умовах, зазначених Заявником в Оферті, не пізніше 1 (одного) робочого дня з дати направлення Заявником Заявки. Товариство повідомляє Заявника про прийняте рішення про надання Позики або відмову від укладення Договору з Заявником будь-яким доступним способом.
3. Заявник до прийняття позитивного рішення про видачу позики зобов'язаний на вимогу Товариства пройти процес ідентифіка-

ції на Сайті або в Мобільному додатку, шляхом: фотографування документа, що посвідчує особу (лицьовий та зворотний бік); фотографування особи.

4. У разі прийняття Товариством позитивного рішення про видачу Заявнику Позики, Товариство надає Позику Позичальнику у вигляді одноразового перерахування Суми Позики, вказаною в Оферті, на Гаманець Позичальника. [1]

Характеризуючи використання онлайн кредитування, слід згадати його широке застосування у Польщі. Таким видом кредитування є соціальний кредит – позика он-лайн. Звичайно, для того аби надати або отримати соціальну позику необхідно мати при собі посвідчення особи (такі як водійські права або паспорт) і невелику суму грошей, яка буде впливати на субрахунок на сайті. Крім того, можна перевірити номер телефону або місце розташування позичальника – це збільшить авторитет і можливість отримати позику, особливо на самому початку своєї діяльності на сайті.

Після успішного створення облікового запису, особа може виступати як кредитором, так і позичальником. У цих системах є деякі служби безпеки, які захищають інтереси бажаючих інвестувати. Відсотки за позиками оподатковуються як дохід капіталу, а не як дохід від підприємницької діяльності.

Дана компанія підтримує веб-портал, який дозволяє особі зв'язатися з людьми, які мають потребу у кредиті – позичальниками, а також з людьми, у яких є кошти, щоб знайти – кредитора. Позичальник беручі кредит повинен заздалегідь вказати суму кредиту, приблизний термін погашення і процентну ставку на яку він розраховує. Це клієнт робить через офіційний сайт. Також йому необхідно вказати на сайті особисті дані, включаючи інформацію про щомісячний дохід та кількість осіб, що проживають разом з ним. Дана інформація необхідна для перевірки позичальника в інформаційному бюро кредитів. Якщо у позичальника немає проблем з погашенням інших кредитів така кредитна заявка буде мати позитивний результат.

Щодо самого договору позики, то він направляється замовнику після того, як позичальник проходить процедуру подачі заявки на отримання кредиту та починає діяти після передачі плати за перевірку в розмірі 1 злотих, а також затвердження його умов.

[1] Правила надання позик. URL: https://finance.kz/zaimy

Крім того, позичальник повинен поставити свій електронний підпис на договорі і відправити його через Мережу. Якщо у нього немає цифрового підпису, необхідно надрукувати весь договір з додатками та підписати його. Підпис має бути чітким і складатися з імені та прізвища. Далі система генерує електронний контракт і передає кошти, депоновані усіма кредиторами на рахунок позичальника. Щомісячний платіж відсотків є відповідною частиною капіталу, яку отримає кредитор. Ці відсотки є його єдиною нагородою.[1]

Таким чином, перевагою он-лайн кредитування, позика мають перевагами спрощений спосіб отримання грошових коштів, що дозволяє позичальникам заощадити час.

Підсумовуючи, можна визначити онлайн кредитування, як процес оформлення і надання клієнтом в Банк документів на отримання кредиту по інтернет-заявці, підписання сторонами інформації про умови кредитування та процентній ставці, укладення кредитного договору за допомогою системи «Інтернет-Банк».

Але, як у кожному кредитному договорі, актуальною є проблема забезпечення інтересів учасників договору, передусім, інтересів кредитора (кредитодавця), який ризикує, надаючи кредит у період воєнного стану. Разом із тим, при такому кредитуванні кредитні ризики можуть виявитися вищими, оскільки кредитодавець не завжди має можливості достатньо ретельно перевірити платоспроможність потенційного боржника, його кредитну історію тощо.

У зв'язку з цим суттєво зростає значення правових засобів забезпечення виконання кредитного договору, найбільш прийнятними з яких при онлайн кредитуванні є застава і гарантія. Тому далі доцільно докладніше зупинитися на розгляді особливостей їхнього застосування у ІТ-сфері.

Застава ІТ-об'єктів у період воєнного стану

Застава є цивільним правовідношенням, в якому одна сторона (боржник) зобов'язана вчинити на користь іншої сторони (кредитора) певну дію (наприклад, сплатити гроші, передати майно, виконати

[1] Nikt nie daje gwarancji dla pożyczek w sieci. URL: https://prawo.gazetaprawna.pl/artykuly/415270,nikt-nie-daje-gwarancji-dla-pozyczek-w-sieci.html

певну роботу, тощо) або утриматись від виконання певної дії, а кредитор має право вимагати від боржника виконання його обов'язку.

Сторона, яка виступає боржником за зобов'язанням, повинна виконати зобов'язання належним чином відповідно до умов договору та вимог Цивільного кодексу України, інших актів цивільного законодавства, а за відсутності таких умов та вимог – відповідно до звичаїв ділового обороту та інших вимог, що звичайно ставляться (ст. 526 ЦК).

Безумовно, боржник може при бажанні додатково забезпечити виконання свого обов'язку одним із способів забезпечення виконання зобов'язання, передбачених цивільним законодавством, серед яких гарантія, неустойка, порука, притримання, завдаток і в тому числі застава.

Щодо застосування застави, то нею, як вбачається зі ч. 1 ст. 3 Закону України «Про заставу», може бути забезпечене виконання лише таких зобов'язань, за якими вимога кредитора є дійсною або майбутня вимога, яка не суперечить законодавству України. У згаданій нормі міститься окремі види вимог, які можуть бути забезпечені заставою, зокрема такі, що випливають з договорів купівлі-продажу, перевезення позики, оренди тощо. Оскільки ця норма не дає визначення дійсності вимоги, логічно припустити, що заставою можуть забезпечуватись й інші дійсні вимоги, які не згадуються прямо в Законі «Про заставу» та ті вимоги, що перелічуються в цьому законі, не завжди можуть бути забезпечені заставою, а лише у тому випадку, коли вони мають ознаки дійсності.

Предметом застави може виступати майно та майнові права, які відповідно до законодавства України можуть бути відчужені заставодавцем та на які може бути звернено стягнення. Крім того, предметом застави може бути майно, яке стане власністю заставодавця після укладення договору застави, в тому числі продукція, плоди та інші прибутки (майбутній урожай, приплід худоби тощо), якщо це передбачено договором.

Зазвичай у міжнародній практиці, розглядаючи варіанти кредитування, позичальнику, можливо, доведеться вибирати між забезпеченим та незабезпеченим кредитом. Забезпечені кредити вимагають надання позичальником чогось цінного як застави на випадок, якщо він не зможе погасити кредит, тоді як незабезпечені кредити дозволяють

позичальнику позичити гроші одразу. Обидва типи кредиту мають свої плюси та мінуси, тому перш ніж приймати будь-яке рішення, краще зрозуміти пов'язані з ними умови.

Розглянемо детальніше ці види. Так, забезпечений кредит – це кредит, забезпечений заставою. Найпоширенішими типами забезпечених кредитів, зокрема, у період воєнного стану, є іпотека та автокредити, і у випадку цих кредитів заставою є будинок або автомобіль позичальника. Але насправді заставою може бути будь-який фінансовий актив, яким володіє позичлаьник. І якщо ви не погасите кредит, банк може вилучити ваше забезпечення як платіж. Наприклад, у США, інформація про вилучення майна залишається у кредитній історії позичальника до 7 років.

У більшості країн Європи, коли позичальник бере кредит, що є забезпеченим, кредитор накладає заставу на актив, який він пропонує як заставу. Після погашення кредиту кредитор знімає заставу, і позичальник повністю володіє обома активами.

Оскільки активи позичальника можуть бути конфісковані, якщо він не погасить забезпечений кредит, вони, можливо, ризикованіші, ніж незабезпечені кредити.

Ось види активів, які можна використовувати як предмет "забезпеченого" кредиту, наприклад, у США:

- Нерухомість. Іпотека використовується для придбання житла, при цьому нерухомість виступає в якості застави. Типові терміни кредиту становлять 15 або 30 років.
- Банківські рахунки (поточні рахунки, ощадні рахунки, депозитні сертифікати та рахунки грошового ринку)
- Транспортні засоби (легкові автомобілі, вантажівки, позашляховики, мотоцикли, човни тощо). Автокредит використовується для придбання транспортного засобу (наприклад, автомобіля), який служить заставою. У разі невиконання зобов'язань кредитор може вилучити транспортний засіб.
- Акції, пайові фонди або інвестиції в облігації
- Страхові поліси, включаючи страхування життя. Кредит на страхування життя : береться під грошову вартість поліса страхування життя, причому поліс виступає в якості забезпечення. Боржник може погасити кредит або отримати залишок відрахування з виплати страхової суми у разі смерті бенефіціара.

- Колекційні предмети високого класу та інші цінності (дорогоцінні метали, антикваріат тощо)
- Кредитні картки, такі як Capital One Platinum Secured Credit Card та Platinum Secured Mastercard® від First Tech Federal Credit Union . У цьому випадку заставою є готівка, яку позичальник вносить (часто це повертається депозит у розмірі 200 доларів США), яка діє як його початковий кредитний ліміт. Позичальник отримує свій депозит назад, коли закриває рахунок.
- Результати творчої діяльності в сфері IT, такі як програмний код, алгоритми, бази даних, а також винаходи, торгові марки, дизайн програмного забезпечення та інше.
- Апаратне забезпечення (наприклад, комп'ютери, сервери, мережеве обладнання), програмне забезпечення (операційні системи, програми, бази даних), дані (інформація, що обробляється).

Також останнім часом стали непоодинокими випадки оформлення таких різновидів кредиту як кредит, забезпечений акціями : забезпечений ощадним рахунком або депозитним сертифікатом (CD) часто з нижчими процентними ставками, ніж незабезпечені позики.

Депозитний сертифікат (CD) – це тип ощадного рахунку, який виплачує фіксовану процентну ставку за кошти, що зберігаються протягом узгодженого періоду. Найкращі ставки за депозитними сертифікатами зазвичай вищі, ніж за ощадними рахунками, але позичальник втрачає гнучкість зняття коштів. Якщо він зніме кошти з депозитного сертифіката достроково, з нього буде стягнуто штраф.

Депозитні сертифікати бувають на різні терміни, від 3-, 6- та 12-місячних до 4-, 5- та навіть 10-річних. Вони є безпечнішою та консервативнішою інвестицією, ніж акції та облігації, але пропонують менші можливості для зростання.[1]

Як ми вже говорили вище, для позичальника при отриманні кредиту важливо мати позитивну кредитну історію. Однак, цікавим моментом є те, що кредити з «поганою кредитною історією» також мають місце на практиці при отриманні кредиту, але зазвичай розміри позик невеликі, терміни погашення короткі, а ставки високі.

Погана кредитна історія – це термін, який часто використовується для опису низького кредитного рейтингу.

[1] What is a certificate of deposit (CD)? Pros and Cons. URL: https://www.investopedia.com/terms/c/certificateofdeposit.asp

Низький кредитний рейтинг часто пов'язаний із пропущеними або несвоєчасними платежами за кредитними картками, позиками чи іншими позиками, а також із регулярним перевищенням кредитного ліміту. Це також може включати людей, які повністю порушили умови кредитної угоди, тобто порушили її.

Кожен кредитор має власні критерії, вирішуючи, кому він схвалить кредитну картку чи позику. Не існує конкретного кредитного рейтингу, який кредитори використовують для прийняття рішень щодо схвалення. Це означає, що позичальник може мати право на одну кредитну картку, але не на іншу від іншого кредитора.

На сьогоднішній момент, у період воєнного стану, банки все частіше стикається не з вчасним погашенням кредиту. Однак, все одно, навіть якщо позичальник порушував неодноразово умови кредитних договорів, краще намагатися їх укладати знов, наприклад, оформлення кредитної картки на незначну суму.

Кредитна картка, розроблена для людей з поганою кредитною історією, працює так само, як і стандартна кредитна картка, але часто з іншими умовами. Наприклад, кредитні ліміти зазвичай нижчі та мають вищу процентну ставку.

Хоча процентна ставка за цими картками може бути вищою, своєчасне здійснення платежів покаже, що позичальник здатен керувати кредитною угодою. Це може покращити його кредитний рейтинг з часом.

Ось деякі важливі речі, які слід враховувати під час подання заявки на отримання та використання кредитної картки для людей з поганою кредитною історією, а також деякі речі, про які слід знати:

- Позичальник може використовувати картку, щоб покращити свій кредитний рейтинг;
- Будь-які покупки, здійснені за допомогою кредитної картки, захищені, як і стандартна кредитна картка;
- Позичальник все ще можете мати право на отримання цих карток, якщо у нього є CCJ або він раніше був оголошений банкрутом;
- Якщо позичальник ніде не працює або не зареєстрований за адресою, подання заявки на отримання кредитної картки може бути складнішим.

Наприклад, у Великій Британії є навіть спеціальні види кредитних карток, щоб покращити кредитну історію, зокрема кредитна картка Vanquis Credit Builder.[1]

Деякі важливі моменти, які слід пам'ятати, подаючи заявку на отримання картки з поганою кредитною історією:

По-перше, це то, що багато кредиторів пропонують позичальнику можливість початкової перевірки відповідності вимогам. Це може допомогти з'ясувати, чи буде заявка позичальника схвалена без залишення «жорсткої перевірки кредитної історії» у його кредитному досьє.

По-друге, перевірка відповідності вимогам дає уявлення позичальнику про те, чи буде йому надано кредит. Але це не завжди гарантовано. Також, часто потрібно проводити додаткові перевірки на шахрайство, дані про особу та платоспроможність. Це означає перехресну перевірку інформації у заявці позичальника з його кредитною історією. Необхідно розуміти, що кредитори проведуть повну перевірку кредитної історії потенціального позичальника, що буде зазначено у його кредитній історії. Тож треба бути уважним, вибираючи найкращі кредитні картки.

Щодо незабезпеченого кредиту, то він не вимагає застави, хоча з позичальника все одно стягуються відсотки, а іноді й комісії. Студентські позики, особисті позики та кредитні картки – все це приклади незабезпечених кредитів.

Оскільки застави немає, фінансові установи видають незабезпечені позики значною мірою на основі кредитного рейтингу чи кредитної історії погашення минулих боргів (див. попередній розділ). З цієї причини незабезпечені позики можуть мати вищі процентні ставки (але не завжди), ніж забезпечені позики.

Незабезпечені особисті набирають популярності. За даними онайн-ринку кредитування Lending Tree, у США налічується приблизно 20,2 мільйона позичальників особистих позик. Особа може взяти особисту позику практично для будь-якої мети, будь то ремонт кухні, оплата весілля, відпустка мрії чи погашення боргу за кредитною карткою.

Більшість людей беруть особисті позики для консолідації боргів, і оскільки особисті позики, як правило, мають нижчу річну процентну

[1] Credit Builder Credit Card. URL: https://www.vanquis.com/credit-cards/credit-builder-card/\

ставку, ніж кредитні картки, позичальники часто можуть заощадити гроші на відсотках.

Консолідація боргів об'єднує кілька боргів, зазвичай боргів з високими відсотками, таких як рахунки за кредитними картками, в один платіж. Консолідація боргів – гарна ідея, якщо позичальник може отримати нижчу процентну ставку, ніж він сплачує зараз. Це допоможе йому зменшити загальну суму боргу та реорганізувати її, щоб він міг швидше її погасити. Якщо позичальник має справу з керованою сумою боргу та хоче спростити сплату кількох рахунків з різними процентними ставками, платежами та термінами погашення, консолідація боргу – це розумний підхід, який він може реалізувати самостійно.

Існує два основні способи консолідації боргу, обидва з яких зосереджують боргові платежі позичальника в одному щомісячному рахунку. Найкращий варіант для боржника залежатиме від його кредитного рейтингу та співвідношення боргу до доходу.

Наприклад, можна отримати кредитну картку з 0% відсотками та переказом балансу. З такою кредитною карткою з боржник переводить залишки коштів з своєї існуючої кредитної картки на нову картку, а потім погашає її з нульовими відсотками протягом акційного періоду, який може тривати від 15 до 21 місяця. Це заощаджує гроші на відсотках і навіть може допомогти боржнику швидше позбутися боргів, оскільки він може використати ці додаткові заощадження для погашення боргу. Щоб претендувати на участь, йому знадобиться хороший або відмінний кредитний рейтинг (кредитний рейтинг 690 або вище).

Або можливо отримати кредит на консолідацію боргу з фіксованою ставкою. За допомогою кредиту на консолідацію боргів боржник використовує кошти кредиту для погашення боргів, а потім повертає його частинами протягом встановленого терміну, зазвичай від одного до семи років. Оскільки процентні ставки за кредитом на консолідацію боргів фіксовані, він сплачуватимете однакову суму щомісяця, доки кредит не буде погашено. Боржник може отримати кредит на консолідацію боргів з поганою кредитною історією (кредитний рейтинг 629 або нижче), але позичальники з вищими рейтингами, ймовірно, матимуть право на найнижчі процентні ставки.

Коли варто розглянути консолідацію боргів?

Успішна стратегія консолідації вимагає наступного:

– щомісячні платежі за боргами не перевищують 50% щомісячного валового доходу позичальника.
– кредитна історія позичальника достатньо хороша, щоб претендувати на отримання картки з 0% ставкою на переказ балансу або кредиту на консолідацію боргу з нижчою процентною ставкою, ніж його існуючий борг.
– грошовий потік позичальника може стабільно покривати регулярні платежі за його боргом.

Якщо ви оберете картку з переказом балансу, ви зможете погасити її протягом акційного періоду.

Якщо ви оберете консолідований кредит, ви зможете погасити його протягом одного-семи років.

Ось приклад, коли консолідація має сенс: скажімо, у вас є дві або три кредитні картки з процентними ставками від 23% до 28%, і ваша кредитна історія хороша. Ви можете претендувати на отримання необезпеченого кредиту на консолідацію боргу під 15% – значно нижча процентна ставка. Завдяки меншим відсоткам, що нараховуються щомісяця, ви швидше досягнете успіху в позбавленні від боргів.

Для багатьох людей консолідація відкриває світло в кінці тунелю. Якщо позичальник бере кредит із трирічним терміном та знає, що його буде погашено за три роки – за умови, що він вчасно сплачує платежі та контролює свої витрати. І навпаки, здійснення мінімальних платежів за кредитними картками може означати місяці або роки до їх погашення, і все це при нарахуванні більших відсотків, ніж початкова основна сума.

Консолідація боргів, як правило, є гарною ідеєю, оскільки вона спрощує погашення боргів з високими відсотками, таких як кредитні картки. Якщо позичальник має право на низьку процентну ставку за кредитом на консолідацію боргів або переведе свої борги на кредитну картку з 0% переказом балансу, він заощадите гроші на відсотках, які потім зможе використати для погашення боргу.

Тільки необхідно переконатися, що у боржника не накопичуються нові залишки на консолідованих картках, оскільки це може призвести до подальшого заборгованості, тому потрібно враховувати всі пе-

реваги та недоліки, перш ніж подавати заявку на позику або картку з переказом балансу.[1]

Як зазначалося у попередніх розділах посібника, об'єктами майнових прав у ІТ-сфері, можуть бути певні майнові блага, які є проявом інформаційних технологій. Зокрема, предметом застави можуть виступати: програмне забезпечення, комп'ютерна програма, база даних, доменне ім'я, веб-сайт, кредитні картки.

Останнім часом у Інтернет-просторі все більше використовуються система електронних розрахунків. Однією з таким систем миттєвих інтернет-розрахунків є система WEBMONEY, яка була створена ще в 1998 році.Кожний користувач даної системи має свій особовий рахунок, що називається WMID (складається з 12 цифр, кожний WMID у системі унікальний). Усередині нього може бути відкрито декілька гаманців — спеціальних облікових записів, на яких ведеться облік «титульних знаків», що номіновані у різних валютах: гривня, долар США, євро та інші. [2]

Користувачі даної системи можуть за їх бажанням отримати також і кредитні кошти під заставу або без. Заставою може бути, наприклад, право власності на доменне ім'я, контент сайту, права на програмне забезпечення, що використовуються на сайті, або навіть сам сайт як цілісний об'єкт.

Одним з прикладів надання кредиту може бути кредит під заставу домен. Так, прикладом використання застави у Інтернет просторі може слугувати кредит під заставу webсайту. (Web-сайти за своєю природою є близькими до баз даних. Тексти, розміщені на Web-сайті, зазвичай містять посилання на інші інформаційні ресурси, розміщені на тому самому або іншому сайті. Таким чином, Web-сайти є механізмами доступу до систематизованої інформації та, будучи оригінальними, підлягають охороні.[3]

Так, вже непоодинокими є випадки надання оголошень щодо надання кредиту під заставу сайту. Наприклад, позичальнику пропонується отримати кредит за передання в управління кредитора сайту позичальника. Сторони домовляються про розмір відсотків та суму

[1] What Is Debt Consolidation, and Should I Consolidate? URL: https://www.nerdwallet.com/article/loans/personal-loans/what-is-debt-consolidation

[2] Опис системи Web money. URL: https://webmoney.ua/ukrainian/about/aboutukr

[3] ІТ-право та інформаційна безпека: моногр. За ред. О. І. Харитонової, Є. О. Харитонова. Одеса. Фенікс, 2017. С. 94.

кредиту та про дату повернення грошей після детального аналізу сайту. Зазвичай кредитором виступають кредитні спілки або кооперативи.

Досить новим предметом застави у Інтернет-просторі є застава комп'ютерної гри. Наприклад, нещодавно, користувачі NeoGAF виявили в мережі документ, згідно з яким студія Cloud Imperium Games взяла кредит в банку Coutts & Co під заставу всього, що пов'язано з їх грою Star Citizen. Йдеться про всі ассети, коди, права на IP та поширення проекту. Скільки саме автори Star Citizen взяли в кредит, в документі не видно. Відомо, що банк Coutts & Co дав студії Cloud Imperium Games ліцензію на подальшу розробку гри, і, якщо у розробників щось піде не так, це може обернутися заморожуванням проекту. Зараз бюджет Star Citizen вже перевищує 150 мільйонів доларів. Саме стільки творцям вдалося зібрати за допомогою краудфандінга. (Краудфандинг (Crowdfunding, crowd — «громада, гурт, юрба», funding - «фінансування»), тобто «Громадське фінансування», «Фінансування громадою» - це співпраця людей, які добровільно об'єднують свої гроші чи інші ресурси разом, як правило через Інтернет, аби підтримати зусилля інших людей або організацій. [1]

Корисним є досвід Польщі у цій галузі, де застава досить активно використовується при укладанні договорів у електронному вигляді. Так, не пізніше, ніж в момент вираження споживачем волі за договором, укладеним на відстані або поза межами підприємства, торговець зобов'язаний повідомити споживача ясно і зрозуміло про: розмір та спосіб складання застави, або ж про надання інших фінансових гарантій, які необхідно виконати споживачу на вимогу підприємця. Якщо підприємець вимагає від споживача надання будь-яких забезпечень, фінансових гарантій або ж застави, існує обов'язок підприємця проінформувати про це споживача.

Така інформація повинна вказувати на тип забезпечення (готівка, вексель, банківська гарантія) та його розмір і порядок подання. Наприклад, під час здачі в оренду кімнати в пансіонаті через веб-сайт, орендодавець повинен проінформувати споживача про те, що оренда пов'язана з необхідністю сплати30 злотих застави.[2]

[1] Визначення краудфандингу. Вікіпедія. URL: https://uk.wikipedia.org/wiki/%D0%9A%D1%80%D0%B0%D1%83%D0%B4%D1%84%D0%B0%D0%BD%D0%B4%D0%B8%D0%BD%D0%B3

[2] Obowiązek nr. 18 – kaucja – Prawo Konsumenckie. URL: https://www.prawokonsumenckie.pl/pl/a/obowiazek-informacyjny-nr-18-kaucja).

Таким чином, ми бачимо, що інститут кредитування в Інтернет просторі тісно пов'язаний з засобами забезпечення виконання зобов'язань, серед яких центральне місце займає застава ІТ-об'єктів. Тобто, можна констатувати, що застава є досить надійним засобом забезпечення інтересів кредитодавця при електронному кредитуванні.

При цьому варто зауважити, що відповідно до потреб бурхливого розвитку інформаційних технологій та виникненням нових ІТ-об'єктів, усе більше стає прикладів передання у заставу ІТ-об'єктів.

Таким чином, особливості застави у ІТ- сфері у період воєнного стану проявляються у двох аспектах: з одного боку застава є забезпечення електронного кредитування, з іншого, ІТ-об'єкти можуть бути предметом застави.

Гарантія як засіб забезпечення виконання зобов'язань у період воєнного стану

Ще одним ефективним видом забезпечення виконання кредитних зобов'язань є гарантія. Згідно ч.1. ст. 560 ЦК України за гарантією банк, інша фінансова установа, страхова організація (гарант) гарантує перед кредитором (бенефіціаром) виконання боржником (принципалом) свого обов'язку. У цій же статті міститься перелік учасників даних відносин, серед них: гарант, принципал та бенефіціар, однак їх коло може бути більш розширене.

Більш детальне визначення гарантії міститься у постанові Правління НБУ від 15.12.2004 р. «Про затвердження Положення про порядок здійснення банками операцій за гарантіями в національній та іноземних валютах». П.1. розділу 1 даного Положення визначає, що гарантія – це спосіб забезпечення виконання зобов'язань, відповідно до якого банк гарант приймає на себе грошове зобов'язання перед бенефіціаром (оформлене в письмовій формі або у формі повідомлення) сплатити кошти за принципала в разі не виконання останнім своїх зобов'язань у повному обсязі або їх частину в разі пред'явлення бенефіціаром вимоги та дотримання всіх вимог,передбачених умовами гарантії.

Зобов'язання банку-гаранта перед бенефіціаром не залежить від основного зобов'язання принципала (його припинення або недійсно-

сті),зокрема і тоді, коли посилання на таке зобов'язання безпосередньо міститься у тексті гарантії.[1]

Щодо міжнародної практики використання гарантії, то гарантія як вид забезпечення виконання зобов'язання представляє собою досить широке поняття і може видаватись не тільки банком. Вона може поєднувати ознаки, як властиві нашому праву, так і іншим способам забезпечення виконання вимог кредиторів, таких як:

- гарантія виплати заборгованості по орендній платі, за несплату якої майно підлягає арешту;
- гарантія виплати боргу частковими платежами, беручи до уваги, що кредитор все ще відмовляється від судового переслідування ;
- гарантія зі сторони декількох осіб з надання обмеження сум;
- гарантія зі сторони декількох поручителів з виплати суми заставної з обмеженням відповідальності кожного поручителя. [2]

Ведучи мову про банківську гарантію необхідно виділити її види, які активно застосовуються у період воєнного стану. До них можна віднести:

- відклична гарантія – така, що може бути відкликана, або така, умови якої можуть бути змінені без попереднього повідомлення (кредитора) бенефіціара
- безвідклична, тобто така, що не може бути відкликана, а її умови не можуть бути змінені без погодження з (кредитором) бенефіціаром.
- умовна, тобто така, що забезпечує виконання платежу та інших зобов'язань банком-гарантом перед бенефіціаром за його першою вимогою (також в письмовому вигляді), але вже з деякими умовами. Тут потрібні також документи, які стануть підтвердженням невиконання принципалом його зобов'язань.
- безумовна, тобто за такою гарантією банкна першу вимогу кредитора (бенефіціара) здійснює платіж. Такий тип гарантії вигідний, головним чином, бенефіціару, тому як він захищає саме

[1] Про затвердження Положення про порядок здійснення банками операцій за гарантіями в національній та іноземних валютах: Постанова Національного банку України від 15.12.2004 р. № 639. *Офіційний вісник України.* 2005. № 3. ст. 156.

[2] Види гарантій у цивільному праві. В. М. Слома. URL: file:///C:/Documents%20and%20Settings/Admin/%D0%9C%D0%BE%D0%B8%20%D0%B4%D0%BE%D0%BA%D1%83%D0%BC%D0%B5%D0%BD%D1%82%D1%8B/Downloads/Unzap_2008_3_18.pdf

його інтереси і зовсім не вигідний протилежному боці, задіяної в угоді.

Зараз доволі актуальним стає такий різновид гарантії як банківська електрона гарантія, тобто це є зобов'язання банку перед замовником (організатором тендеру) виплатити в його користь зазначені суми в разі, якщо постачальник (учасник тендеру) не виконує зобов'язання перед замовником.

Так, наприклад, банківська гарантія, яка зазвичай використовується за межами Сполучених Штатів, дозволяє клієнту банку купувати товари, обладнання або здійснювати міжнародну торгівлю. Якщо клієнт не погашає борг або не доставляє обіцяні товари, банк покриває його.

Банківські гарантії широко використовуються за межами США та схожі на американські резервні акредитиви. Вони здебільшого використовуються в міжнародних ділових операціях, хоча в деяких країнах також можуть знадобитися гарантії для оренди нерухомості фізичним особам. Різні типи гарантій включають гарантію виконання контракту, гарантію авансового платежу, гарантію одержувача гарантійного обслуговування та гарантію оренди.

Ось кілька видів банківських гарантій у США, які покривають різні ризики, зокрема:

1. Гарантія виконання договору : служить забезпеченням витрат покупця, якщо послуги або товари не надаються, як узгоджено в договорі.

2. Гарантія авансового платежу: виступає забезпеченням відшкодування авансового платежу покупця, якщо продавець не постачає зазначені товар згідно з договором.

3. Гарантійне забезпечення: служить забезпеченням, що гарантує доставку замовлених товарів згідно з домовленістю.

4. Гарантія оплати: гарантує продавцю сплату ціни покупки у встановлений термін.

5. Гарантія оренди: служить забезпеченням для платежів за договором оренди.

Наприклад, Світовий банк пропонує програму банківських гарантій для проєктів. Ці гарантії забезпечують комерційних кредиторів захистом від невиконання зобов'язань щодо платежів або невиконання урядами зобов'язань щодо виконання.

Гарантії допомагають захистити міжнародні торговельні відносини, зменшуючи ризики, якщо контракт зірветься, постачальники не виконають його умови або покупець не оплатить товари. Хоча банківські гарантії не є поширеними в США, можна отримати аналогічну гарантію через резервний акредитив.

Резервний акредитив (SLOC) – це юридичний документ, який гарантує зобов'язання банку здійснити платіж продавцю у випадку, якщо покупець – або клієнт банку – не виконає умови угоди. Резервний акредитив допомагає сприяти міжнародній торгівлі між компаніями, які не знають одна одну та мають різні закони та правила. Хоча покупець гарантовано отримає товар, а продавець гарантовано отримає платіж, SLOC не гарантує, що покупець буде задоволений товаром. Резервний акредитив також може скорочено називатися SBLC.

Найчастіше бізнес звертається до SLOC, щоб отримати контракт. Контракт є «резервною» угодою, оскільки банк повинен буде платити лише у найгіршому випадку. Хоча SBLC гарантує оплату продавцю, угода має бути точно дотримана. Наприклад, затримка доставки або неправильне написання назви компанії може призвести до відмови банку у здійсненні платежу.

Існує два основних типи резервних акредитивів:

- Фінансовий SLOC гарантує оплату за товари або послуги, як це визначено в угоді. Наприклад, нафтопереробна компанія може організувати такий лист, щоб запевнити продавця сирої нафти, що вона може оплатити велику поставку сирої нафти.
- Договір про виконання проекту (SLOC), який зустрічається рідше, гарантує, що клієнт завершить проєкт, викладений у договорі. Банк погоджується відшкодувати третій стороні витрати у випадку, якщо його клієнт не завершить проєкт.

Процедура отримання SLOC схожа на заявку на отримання кредиту. Банк видає його лише після оцінки кредитоспроможності заявника.

У найгіршому випадку, якщо компанія стане банкрутом компанія або припинить свою діяльність, банк, що видає SLOC, виконає зобов'язання свого клієнта. Клієнт сплачує комісію за кожен рік дії листа. Зазвичай комісія становить від 1% до 10% від загальної суми зобов'язання на рік.

Резервні акредитиви (SBLC) зазвичай пропонуються комерційними банками та кредиторами. Банк оцінює кредитоспроможність заявника так само, як і заявку на отримання кредиту.

Підсумовуючи, хотілося б підкреслити, що SBLC – це потужний інструмент для компаній, які ведуть переговори щодо великих угод на товари чи послуги. За підтримки комерційного банку SBLC гарантує, що угода буде укладена навіть за найгіршого сценарію. Але SBLC не обійдеться без витрат – є комісії, і буде оцінена кредитоспроможність позичальника[1].

Банківські гарантії тендерної пропозиції (тендерна гарантія або конкурсна). Це свого роду страховка організатора торгів, у разі, коли учасник не виконує умови поставлені замовником в процесі проведення торгів (змінює ціну пропозиції або відмовляється від підписання договору).

Також, як ми бачимо у період дії воєнного стану, в Україні банки пропонують такі види гарантій, зокрема Ощадбанк та Райффайзен Банк:

1. Документ надається в електронному вигляді з накладанням електронного цифрового підпису (ЕЦП), який використовується, наприклад, для забезпечення участі замовника в електроних тендерах закупівель ProZorro.

2. Електронна тендерна гарантія – електронний документ, який містить всі умови гарантії, а також електронно-цифровий підпис уповноваженої особи та електронно-цифровий друк банку. Після підписання електронна гарантія направляється клієнту – учаснику тендера. Клієнт долучає її до своєї тендерної пропозиції та розміщує на авторизованому електронному майданчику, через який проводиться процедура закупівлі. Клієнт може перевірити достовірність електронно-цифрового підпису та печатки Ощадбанку на гарантії на офіційному сайті Центрального засвідчувального центру Міністерства юстиції України.

Тобто така гарантія забезпечує зобов'язання учасника торгів (постачальника) перед організатором торгів (замовником, бенефіціаром). Його цільове призначення полягає в зобов'язанні гаранта (банку) компенсувати замовнику суму втраченої вигоди, якщо заявник

[1] What Is a Standby Letter of Credit (SLOC), and How Does It Work? URL: https://www.investopedia.com/terms/s/standbyletterofcredit.asp

порушить умови тендеру та відмовиться від укладання договору на постачання товарів або виконання робіт.

3. Банківська гарантія виконання договору (зобов'язань). Вона служить гарантією на поставку товару або послуг відповідно до умов договору. На підставі такої гарантії виконання банк, за вказівкою продавця, зобов'язаний виплатити замовнику зазначену гарантовану суму у разі невиконання або неналежного виконання підрядником своїх зобов'язань за договором із замовником. Таким чином, замовник повністю захищений від ризиків порушення договору підрядником, що безумовно підвищує ступінь довіри до нього та є його додатковою перевагою серед конкурентів.

4. Гарантія для туризму. Гарантія для туризму в Україні, зокрема банківська гарантія, є обов'язковою умовою для туроператорів та турагентів, що передбачено Законом України «Про туризм». Вона забезпечує захист прав туристів у разі невиконання туроператором або турагентом своїх зобов'язань, зокрема, у випадках неплатоспроможності, ліквідації або банкрутства. Розмір фінансового забезпечення, а отже, і сума гарантії, залежить від виду діяльності (внутрішній, в'їзний чи міжнародний туризм).

5. Банківська гарантія повернення авансового платежу. Тобто це зобов'язання банку виплатити покупцю певну суму, якщо продавець не виконає свої зобов'язання за договором, зокрема не поверне авансовий платіж. Це захищає покупця від ризику втрати авансу у випадку невиконання продавцем умов договору [1].

6. Банківська гарантія платежу. Вона служить гарантією зобов'язання по своєчасній оплаті поставлених товарів або наданих послуг і зазвичай використовується при роботі з «відкритим рахунком».

Підсумовуючи зазначимо, що у зв'язку зі стрімким розвитком інформаційно-технологічних відносин та переходу звичайних відносин у площину«віртуальних»,окрім вище охарактеризованих різновидів гарантій,можуть також виникати і інші її різновиди.

Однак, одною з основних проблем з якою стикаються правознавці – це недостатнє правове регулювання засобів забезпечення виконання зобов'язання, які використовуються у ІТ-сфері у період воєн-

[1] Види банківських гарантій. URL: https://raiffeisen.ua/en/korporativnim-kliyentam/finansuvannya/garantijni-operaciyi/bankivski-garantiji

ного стану. Сподіваємось, що найближчим часом дане питання буде вирішено, завдяки прийняття спеціальних законів у даній сфері.

Також до основні проблеми е-кредитування у період воєнного стану включають збільшення ризиків неплатежів через втрату працездатності, зниження платоспроможності, пошкодження або втрату заставного майна, а також складнощі з оцінкою кредитоспроможності позичальників в умовах невизначеності.

Ключові слова: зобов'язання, засоби забезпечення виконання зобов'язань, застава, гарантія, договір, правовідносини, кредитний договір, позика, інформаційні технології, Інтернет, воєнний стан, виконання договору, ІТ-об'єкти, кредитор, боржник.

Розділ 18

ЦИВІЛЬНО-ПРАВОВА ВІДПОВІДАЛЬНІСТЬ ЗА ШКОДУ, ЗАВДАНУ КІБЕРАТАКАМИ

DOI

Богдан Фасій
кандидат юридичних наук, доцент

У сучасному інформаційному суспільстві, яке характеризується стрімким розвитком цифрових технологій та їх глибокою інтеграцією у усі сфери суспільного життя, питання цивільно-правової відповідальності за шкоду, завдану кібератаками набуває особливої актуальності. Масштабність та складність кіберзагроз, які охоплюють як фізичних особі, так і юридичних осіб та державні інституції, зумовлюють необхідність вироблення ефективних механізмів притягнення до відповідальності, здатних забезпечити належний рівень правового захисту та мінімізувати негативні наслідки для правопорядку.

Кібератаки можуть завдавати значної матеріальної та моральної шкоди, що зумовлює потребу у встановленні чітких правових критеріїв щодо відшкодування збитків та визначення суб'єктного складу відповідальних осіб. Особливості вчинення правопорушення у кіберпросторі, зокрема складність ідентифікації правопорушника, транскордонний характер кіберзлочинності, а також використання новітніх технологій для приховування слідів злочину, створюють значні виклики для правозастосування практики.

Проблематика цивільно-правової відповідальності за шкоду, завдану кібератаками, займає важливе місце в сучасному правовому полі, оскільки цифровізація суспільних відносин створює нові загрози правам та законним інтересам фізичних та юридичних осіб. Наукова доктрина пропонує низку концептуальних підходів до визначення правової природи та механізмів реалізації відповідальності в умовах кіберпростору, однак єдиного узгодженого підходу в межах цивільного права наразі не вироблено, що обумовлює необхідність подальшого наукового дискурсу[1].

[1] Підопригора О. А. Цивільно-правова відповідальність: теорія та практика. Київ: Юрінком Інтер, 2020. С. 15.

Одним із домінантних підходів у цивілістиці є концепція деліктної відповідальності, що ґрунтується на традиційних юридичних конструкціях, які передбачають наявність шкоди, протиправні діяння, причинно-наслідковий зв'язок та вину правопорушника[1]. Однак у випадку кібератак застосування загальних положень деліктного права стикається з труднощами, зокрема у зв'язку з анонімністю суб'єкта правопорушень, складністю ідентифікації джерела кібератаки та встановлення причинного зв'язку між конкретними діями порушника та заподіяною шкодою[2]. Додатковою проблемою є питання про можливість притягнення до відповідальності суб'єктів, які не є безпосереднім ініціаторами атаки, але створили передумови для її реалізації, зокрема власників вразливих інформаційних систем чи операторів цифрових платформ, які не забезпечують належний рівень кібербезпеки.

Альтернативний науковий підхід до цієї проблематики передбачає застосування концепції об'єктивної відповідальності у випадках, коли шкода є наслідком недотримання стандартів інформаційної безпеки[3]. Така модель відповідальності є поширеною в правових системах, що ґрунтуються на ризик-орієнтованому регулюванні, і передбачає, що суб'єкти господарювання, які здійснюють обробку великих масивів персональних даних або забезпечують функціонування критичної цифрової інфраструктури, несуть відповідальність незалежно від їхньої вини у разі порушення безпеки, якщо не доведуть, що вжили всіх необхідних заходів для запобігання настання шкоди[4]. Вказаний підхід є характерним для правового регулювання ЄС, де відповідальність за витік даних чи порушення кібербезпеки покладається на контролерів та операторів інформаційних систем навіть у разі, якщо зловмисники діяли автономно.

Наукова дискусія також охоплює питання про можливість застосування договірних механізмів відповідальності у випадку, коли

---

1 Штефан М. Й. Деліктне право України: сучасний стан та перспективи розвитку. Харків: Право, 2019. С. 92

2 Хом'як В. В. Інформаційна безпека та правові аспекти її забезпечення. Львів: Галицький інститут, 2021. С. 47.

3 Вдовиченко П. А. Цивільно-правові аспекти відповідальності у сфері цифрових технологій. Одеса: Фенікс, 2022. С. 61.

4 European Union Agency for Cybersecurity (ENISA). *Cybersecurity Act and its implications.* Luxembourg: Publications Office of the European Union. 2020. P.73.

правовідносини між потерпілим та потенційним відповідачем мають контрактний характер[1]. В умовах цифрової економіки значна частина кібератак завдає шкоди суб'єктам, які перебувають у договірних відносинах із операторами цифрових послуг, фінансових платформ чи хмарних сервісів, що ускладнює кваліфікацію відповідних правопорушень виключно як деліктів[2]. Деякі науковці обґрунтовують необхідність закріплення презумпції договірної відповідальності у випадках порушення безпеки даних або неналежного виконання зобов'язань щодо захисту інформації, що уможливлює застосування жорсткіших санкцій до постачальників цифрових послуг, які не забезпечили належний рівень кіберзахисту.

Важливим аспектом проблематики є транскордонний характер кібератак, що зумовлює необхідність міжнародно-правової координації механізмів цивільно-правової відповідальності. Відсутність єдиних міжнародних стандартів щодо юрисдикції, застосовного права та механізмів правового захисту потерпілих створює ситуацію правової невизначеності, що перешкоджає ефективному притягненню до відповідальності осіб, які здійснюють кібератаки[3]. У зв'язку з цим у доктрині висловлюється необхідність розроблення спеціальних міжнародних угод, які б передавали єдині підходи до визначення юрисдикції у справах, пов'язаних із кібератаками, а також процедурні механізми співпраці між державами у сфері судового захисту прав потерпілих.

Окремого розгляду в науковій літературі заслуговує концепція орієнтованого регулювання кібербезпеки, яка передбачає впровадження превентивних заходів для мінімізації ризиків правопорушень у кіберпросторі. Відповідно до цього підходу, цивільно-правова відповідальність має заповнюватись механізмами кіберстрахування, корпоративного комплаєнсу та аудиту інформаційної безпеки, що дозволяє мінімізувати ймовірність завдання шкоди та покласти частину фінансових ризиків на спеціалізовані інститути страхування кіберзагроз.

---

1 Kuner C. Data Protection Law and International Jurisdiction on the Internet. *International Journal of Law and Information Technology*. 2018. Vol. 26. №. 2. P. 1-20.

2 Koops B. J. The Trouble with European Data Protection Law. *International Data Privacy Law*. 2019. Vol. 9. №. 1. P. 5-12.

3 Hartzog W. Privacy's Blueprint: The Battle to Control the Design of New Technologies. Harvard University Press, 2018. 312 p.

Кіберстрахування є порівняно, новим явищем у правовому просторі, тому потребує ґрунтовного дослідження питання використання його як механізму захисту від ризиків, що виникають (можуть виникнути) внаслідок кібератак.

Кіберстрахування – це спеціалізований вид страхування, спрямований на захист організацій та фізичних осіб від фінансових втрат, пов'язаних з інцидентами в кіберпросторі, такими як кібератаки, витоки даних або збої в інформаційних системах. Це інструмент управління ризиками, який дозволяє передати фінансову відповідальності за можливі кіберінциденти страховій компанії, забезпечуючи тим самим фінансову стабільність та безпеку суб'єктів господарювання[1].

Кіберстрахування є новим явищем не лише для України, а й для всього світу. За даними Munich Re за 2018 рік, такий вид захисту надається лише 60 страховими компаніями у різних країнах, причому охоплення кіберризиків поки що залишається обмеженим – застраховано лише 5% таких ризиків[2]. Однак стрімке зростання кіберзагроз, викликаних діяльністю хакерів, сприяє активному розвитку цього сектора. За оцінками страхової групи Allianz, ринок кіберстрахування щорічно демонструє приріст на 25-50%[3].

США по праву можна вважати лідером у сфері кіберстрахування завдяки розвиненій IT-інфраструктурі, першому виявленню серйозних кіберзагроз для бізнесу та жорсткому законодавчому регулюванню захисту персональних електронних даних. Кіберстрахування є одним із найдинамічніших сегментів глобального ринку страхових послуг і розглядається як ефективний інструмент управління ризиками та захисту бізнесу від загроз, що супроводжують електронну комерцію.

До ключових ризиків, які покривають кіберстрахування, належать:

- викрадення конфіденційної інформації співробітниками компанії;
- викрадення відомостей щодо кредитних карт;
- незаконне виведення коштів із рахунків;
- втрата носіїв інформації;

[1] Нагайчук Н. Страхування в системі управління кібер-ризиками підприємства в умовах цифрової економіки. URL: https://www.academia.edu/116320960/Страхування_в_системі_управління_кібер_ризиками_підприємства_в_умовах_цифрової_економіки

[2] Підсумки 2018. URL: https://cyberpolice.gov.ua/results/2018/

[3] Селіверстова Л. С., Трухан Д. А. Підходи до розвитку кіберстрахування як сегменту глобального страхового ринку. *Економіка та держава.* 2020. № 1. С. 23-26.

- фішинг-атаки;
- кібервимагання;
- збої в роботі комп'ютерних мереж через хакерські атаки.

Основною метою кіберстрахування залишається захист від масштабних хакерських атак, здатних завдати значної фінансової та репутаційної шкоди.

Популярність цього виду страхування у розвинених країнах пояснюється розумінням того, що навіть за умови впровадження передових технологій кібербезпеки та регулярного навчання персоналу завжди залишається мінімальний ризик компрометації системи, який складно передбачити чи оцінити[1].

Основними механізми кіберстрахування є процеси андеррайтингу, оцінки ризиків, встановлення страхових премій та врегулювання претензій. Андеррайтинг включає в себе оцінку кіберизиків конкретної організації, аналіз її інформаційної безпеки та визначення відповідних умов страхування[2]. Цей процес є важливим, оскільки правильна оцінка ризиків дозволяє страховикам встановлювати адекватні страхові премії та умови покриття. Встановлення страхових премій базується на аналізі ймовірності настання кіберінцидентів та потенційних збитків. Страхові компанії використовують статистичні дані, моделі ризиків та інформацію про попередні інциденти для визначення розміру премій. Це дозволяє забезпечити фінансову стійкість страховика та адекватне покриття страховика.

Врегулювання претензій є ключовим етапом у механізмі кіберстрахування. Після настання кіберінциденту страхувальник подає претензію до страхової компанії, яка проводить розслідування, оцінює збитки та здійснює відповідні виплати. Цей процес вимагає тісної співпраці між страховиком та страхувальником для забезпечення швидкого відновлення бізнес-процесів та мінімізації негативних наслідків інциденту[3].

---

[1] Shaun S. Wang. Integrated Framework for Information Security. Investment and Cyber Insurance. Wang, Shaun, Integrated Framework for Information Security Investment and Cyber Insurance (September 15, 2017). URL: https://ssrn.com/abstract=2918674

[2] Jason R. C. Nurse. The Data that Drives Cyber Insurance: *A Study into the Underwriting and Claims Processes* / Jason R. C. Nurse, Louise Axon, Arnau Erola, Ioannis Agrafiotis, Michael Goldsmith, Sadie Creese. URL: https://arxiv.org/pdf/2008.04713

[3] Ruperto P. Majuca. The Evolution of Cyberinsurance / Ruperto P. Majuca, William Yurcik, Jay P. Kesan. URL: https://arxiv.org/pdf/cs/0601020

Важливим аспектом кіберстрахування є управління моральним ризиком та проблеми асиметрії інформації. Страхові компанії розробляють спеціальні умови та вимоги до страхувальників, такі як впровадження політик кібербезпеки, регулярні аудити та навчання персоналу, щоб знизити ймовірність настання інцидентів та забезпечити прозорість у відносинах зі страхувальником[1].

Кіберстрахування також стимулює організації до підвищення рівня кібербезпеки. Наявність страхового покриття спонукає компанії впроваджувати кращі практики та стандарти захисту інформації, оскільки це впливає на умови страхування та розмір премій. Таким чином кіберстрахування відіграє важливу роль у загальному підвищенні кіберстійкості суб'єктів господарювання та суспільства в цілому.

Розвиток кіберстрахування в Україні знаходиться на початковому етапі. На нашу думку, основними перешкодами для впровадження кіберстрахування є низька обізнаність бізнесу про кіберризики, відсутність статистичних даних та недостатній рівень кібербезпеки в організаціях. Однак, з огляду на зростання кількості кіберінцидентів та цифровізацією економіки, потреба в кіберстрахуванні стає все більш актуальною.

Для стимулювання розвитку кіберстрахування в Україні необхідно розробити нормативно-правову базу, що регулює цей вид страхування, а також підвищувати обізнаність бізнесу про важливість кібербезпеки та можливості страхового захисту. Крім того, необхідним є співпраця між страховими компаніями, державними органами та експертними організаціями у сфері кібербезпеки може стати ефективним механізмом успішного впровадження кіберстрахування[2].

Таким чином, кіберстрахування є важливим елементом сучасної системи управління ризиками, який забезпечує фінансовий захист від кіберзагроз. Розвиток цього інструменту в Україні вимагає комплексного підходу, включаючи вдосконалення законодавства, підвищення рівня кібербезпеки та обізнаності бізнесу про переваги кіберстрахування. Це сприятиме підвищенню стійкості національної економіки до кіберзагроз та забезпечить захист інтересів як юридичних, так і фізичних осіб у цифровому середовищі.

[1] Галатюк К. О., Лозова В. О. Явище інформаційної асиметрії на ринку страхування. URL: https://conf.ztu.edu.ua/wp-content/uploads/2021/11/259.pdf

[2] Приказюк Н. В., Гуменюк Л. С. Дорожня карта впровадження кібер-страхування в Україні. *Innovation and Sustainability.* 2021. № 1. С. 68.

На сьогоднішній день, підходи до питань цивільно-правової відповідальності за шкоду завдану кібератаками засвідчують відсутність єдиного підходу до визначеної проблематики. Очевидно, що традиційні конструкції цивільного права потребують адаптації до нових технологічних реалій, що передбачає формування гібридних правових механізмів, які поєднують елементи деліктної, договірної та об'єктивної відповідальності, а також забезпечують ефективні механізми міжнародного співробітництва у сфері захисту прав осіб, які постраждали внаслідок кібератак.

Для ґрунтовного дослідження питань відповідальності за шкоду завдану кібератаками, необхідно визначити правову природу поняття «кібератаки». У міжнародному праві термін «кібератака» немає єдиного загальноприйнятого визначення, що пов'язано з різними концептуальними підходами держав та міжнародних організацій до кваліфікації протиправних дій у кіберпросторі. Одним із перших міжнародних документів, що визначає основи регулювання кіберзагроз, є Конвенція Ради Європи про кіберзлочинність (Будапештська конвенція, 2001 р.)[1]. Вона не містить безпосереднього визначення поняття «кібератака», однак описує категорію комп'ютерних злочинів, зокрема несанкціонований доступ до комп'ютерних систем, втручання в дані та систему, а також комп'ютерне шахрайство та підробку[2].

Іншим ключовим документом є Талліннський посібник із застосування міжнародного права до кібероперацій (Tallinn Manual 2.0, 2017), який визначає кібератаку як «дію або серію пов'язаних дій, спрямованих на цілеспрямоване порушення конфіденційності, цілісності або доступності інформації, інформаційних систем і мереж»[3]. При цьому, у рамках міжнародного гуманітарного права кібератаки можуть кваліфікуватися як «напади» відповідно до ст. 49 Додаткового протоколу I до Женевських конвенцій, якщо вони завдають шкоди об'єктам або людям[4].

[1] Конвенція Ради Європи про кіберзлочинність. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text

[2] Convention on Cybercrime (Budapest Convention). Council of Europe. 23 November 2001. URL: https://www.coe.int/en/web/cybercrime/the-budapest-convention

[3] Schmitt M. N. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press, 2017. P. 23.

[4] Додатковий протокол до Женевських конвенцій від 12 серпня 1949 року, що стосується захисту жертв міжнародних збройних конфліктів (Протокол I), від 8 червня 1977 року. URL: https://zakon.rada.gov.ua/laws/show/995_199#o315

Окремі міжнародні організації також формулюють власні визначення. Наприклад, НАТО розглядає кібератаку як «навмисне використання комп'ютерних технологій для створення руйнівного впливу на інформаційні системи», а Європейський Союз у Директиві 2013/40/EU визнає «незаконний доступ, втручання та перехоплення даних» як ключові форми кібератак[1].

Таким чином, міжнародно-правові підходи до визначення кібератаки відзначаються відсутністю уніфікованого визначення, але в загальному сенсі охоплюють умисні дії, спрямовані на порушення роботи інформаційних систем, завдання шкоди інфраструктурі або отримання неправомірного доступу до даних.

На національному рівні визначення кібератак також варіюються залежно від правової традиції на рівні регулювання кіберпростору. В українському законодавстві термін «кібератака» прямо не визначений, проте Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 р. № 2163-VIII визначає «кіберінцидент» як подію, яка може призвести до порушення кібербезпеки, а «кіберзагрозу» як сукупність умов та чинників, що створюють небезпеку в кіберпросторі[2]. Таким чином, на рівні законодавства кібератаки можуть розглядатись через призму кіберзагроз та інцидентів. Для повного та всебічного розуміння специфіки даних понять необхідно визначити їх співвідношення та черговість проявів в цифровому просторі. Так, поняття «кіберінцидент», «кіберзагроза» та «кібератака» є ключовими в сфері кібербезпеки, кожне з яких відображає різні аспекти взаємодії з інформаційними системами та мережами. Розуміння їх співвідношення є важливими для ефективного управління ризиками та забезпечення захисту інформаційних ресурсів.

Кіберзагроза (англ. cyber threat) – це потенційно можливі явища або чинники, які можуть створювати небезпеку для інформаційних систем, мереж або даних. Вони включають у себе вразливості, які можуть бути використані зловмисниками для несанкціонованого доступу або пошкодження інформації. Загрози можуть бути як внутрішніми (наприклад, недбалість працівників), так і зовнішніми (наприклад, дії хакерів).

[1] Directive 2013/40/EU on attacks against information systems. Official Journal of the European Union. 2013. L218. P. 8-14.

[2] Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. *Відомості Верховної Ради України.* 2017. № 45. Ст. 403.

Кібератака (англ. cyber attack) – це цілеспрямовано дія, спрямована на реалізацію кіберзагрози. Вона передбачає використання вразливостей в інформаційних системах для досягнення певних цілей, таких як крадіжка даних, порушення роботи систем або їх знищення. Прикладом кібератаки є використання шкідливого програмного забезпечення для отримання несанкціонованого доступу до системи.

Кіберінцидент (англ. cyber incident) – це подія або сукупність подій, які ставлять під загрозу цілісність, конфіденційність або доступність інформаційних систем, мереж або даних. Кіберінцидент може бути результатом як навмисних дій (кібератак), так і ненавмисних подій (технічні збої, посилки користувачів). Він є фактичним проявом кіберзагрози, яка може або не може бути результатом кібератаки.

Отже, співвідношення між цими поняттями можна представити наступним чином: кіберзагроза є потенційною можливістю виникнення небезпеки для інформаційних систем. Коли ця загроза реалізується через цілеспрямовані дії зловмисників, ми маємо справу з кібератакою. Якщо внаслідок кібератаки або інших факторів відбувається подія, яка порушує нормальне функціонування інформаційних систем, це вважається кіберінциндентом.

Таким чином, кіберзагроза є потенційною небезпекою, кібератака – це реалізація цієї небезпеки через навмисні дії, а кіберінцидент – це результат, який може виникнути внаслідок кібератаки або інших подій, що впливають на інформаційну безпеку.

У Кримінальному кодексі України поняття кібератаки також прямо не закріплено, проте його можна розглядати через такі склади злочинів:

– несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж (ст. 361 КК України);
– Створення, розповсюдження або збут шкідливих програмних чи технічних засобів, а також несанкціоноване збирання, зберігання та передача інформації з обмеженим доступом (ст. 361-1, 362 КК України)[1].

[1] Кримінальний кодекс України: Закон України. *Відомості Верховної Ради України.* 2001. № 25-26. Ст. 131.

Щодо зарубіжних країни, то у США згідно із Законом про комп'ютерне шахрайство та зловживання (Computer Fraud and Abuse Act, 1986) кібератака визначається як «несанкціоноване проникнення або пошкодження інформаційної системи, що призводить до значних фінансових втрат або загрози національній безпеці»[1]. У Німеччині Закон про безпеку інформаційних технологій (IT-Sicherheitsgesetz, 2015) визначає кібератаку як «навмисне використання шкідливих програм або інших технічних засобів для порушення функціонування цифрових інфраструктур»[2].

Зіставлення національних та міжнародних нормативних актів, які містять згадку про кібератаки, дає можливість виокремити такі основні підходи до розуміння даного явища:

1. Функціональний підхід – робить акцент на наслідках кібератаки (порушення конфіденційності, цілісності даних, того).

2. Суб'єктний підхід – визначення відповідальності держав, приватних осіб або транснаціональних організацій за проведення кібератак.

3. Технологічний підхід – увага до технічних аспектів атак, таких як використання шкідливого програмного забезпечення, DDoS-атаки тощо.

4. Правовий підхід – кваліфікація кібератак в межах національного кримінального, цивільного або адміністративного права.

З точки зору цивільного права, кібератака може бути визначена як протиправне посягання на інформаційні системи, електронні комунікаційні мережі чи дані з метою завдання шкоди фізичній особі, юридичній особі чи державі, що може спричинити майнову та немайнову шкоду, порушення договірних зобов'язань або іншим чином вплинути на приватно-правові відносини. Таким чином, у цивільному праві кібератака розглядається не лише як технологічний злочин, а й як юридичний факт, що тягне за собою правові наслідки, зокрема відшкодування збитків та відновлення порушених прав.

Загалом, проблема визначення кібератак залишається дискусійною, і сучасні тенденції вказують на необхідність розробки єдиного міжнародного підходу, який би врахував транскордонний характер кіберзагроз та встановлював уніфіковані критерії відповідальності за

[1] Computer Fraud and Abuse Act (CFAA). U. S. Code, Title 18, Section 1030, 1986.

[2] IT-Sicherheitsgesetz. Bundesministerium des Innern, 2015. URL: https://www.bmi.bund.de

їх вчинення. Наприклад, лише в листопаді та грудні 2016 року Україна зазнала 6500 кібератак. Окрім інформаційної пропаганди та викрадення важливих даних, російські хакери атакували й енергетичну інфраструктуру столиці. 17 грудня 2016 року в Києві на короткий час зникло електропостачання. Розслідування показало, що ця атака була пов'язана з іншими зломами – систем «Укрзалізниці», Міністерства фінансів і Пенсійного фонду України. Подібні втручання траплялися й раніше. У грудні 2015 року без світла тимчасово залишилися 230 тисяч жителів Києва. Експерти з Information Systems Security Partners (ISSP), які досліджували ситуацію для «Укренерго», вважають, що ці атаки були взаємопов'язаними. Хоча їхні наслідки вдалося швидко ліквідувати, фахівці припускають, що вони мали на меті продемонструвати можливості зловмисників. Україна стала випробувальним майданчиком для російських хакерів. Ще одна масштабна кібератака, відома як BugDrop, відбулася в лютому 2017 року. Її організатори залишаються невідомими. Загрозу виявила міжнародна компанія CyberX, яка оприлюднила офіційне розслідування на своєму сайті[1].

Відомий український дослідник у сфері кібербезпеки, професор В. Л. Бурячок, визначає поняття «кібератака» як комплекс узгоджених за метою, змістом і часом дій (кіберакцій), спрямованих на певний об'єкт впливу. Метою таких атак є порушення конфіденційності, цілісності, доступності, спостережуваності або авторства інформації, що в ньому циркулює, враховуючи її вразливість. Також кібератаки можуть призводити до збоїв у роботі ІТ-систем і мереж цього об'єкта[2].

Як влучно зазначають Бондаренко І. Д. та Шестаков В. І. більшість кібератак, спрямовані на Україну, не спричинили безпосереднього фізичного руйнування обладнання чи загибелі людей, однак під час розробки Tallinn Manual 2.0 його автори розглядали саме ці фактори як визначальні для набуття кібератакою правового статусу «атаки» відповідно до норм міжнародного гуманітарного права, адже здійснення таких дій проти цивільних об'єктів і населення є воєнним злочином. Попри це, кібератаки, подібно до застосування кінетичної зброї, виводили з ладу критично важливі інфраструктурні об'єкти

[1] Всесвітній огляд економічних злочинів. *Кіберзлочини в центрі уваги.* URL: https://www.pwc.com/ua/en/services/forensic/assets/gecs_2011_report_ukraine_ukr.pdf

[2] Бурячок В. Л. Основи формування державної системи кібернетичної безпеки: монографія. Київ: НАУ, 2013. 432 с.

шляхом знищення або пошкодження їхнього штатного програмного забезпечення, що призводило до порушення основних функцій цих об'єктів, включно з життєво необхідними для цивільного населення[1]. Наприклад, відключення електропостачання значної кількості споживачів, а також систем теплогенерації та лікарень у зимовий період створювало безпосередню загрозу життю та здоров'ю населення.

Реальне усвідомлення критичної небезпеки наслідків кібератак упродовж останніх років зумовило значний перегляд підходів європейських і американських науковців до так званого «порогу серйозності» (gravity threshold), який визначає, чи може певний кіберінцидент бути кваліфікований як «атака» за нормами міжнародного гуманітарного права. Зокрема, у науковій спільноті посилюється позиція щодо того, що самі комп'ютерні дані, особливо в системах управління критичною інфраструктурою, можуть розглядатися як об'єкт атаки, навіть за відсутності фізичних руйнувань чи людських жертв[2].

На основі вищезазначеного, може стверджувати, що кібератака є складним і багатогранним явищем, що потребує міждисциплінарного дослідження, оскільки вона має широкий вплив на суспільство, державу, економіку та міжнародну безпеку. З технічної точки зору кібератаки пов'язані з використанням шкідливого програмного забезпечення, фішингових атак, DDoS-атак та інших методів, що спрямовані на компрометацію інформаційних систем. Правовий підхід до дослідження кібератак дає можливість вивчити межі відповідальності, правові наслідки та способи правового реагування. Кібератаки також розглядаються у військовому та геополітичному контексті, оскільки вони стали інструментом гібридної війни, інформаційних конфліктів та дипломатичного тиску. З економічної точки зору кібератаки досліджують як дії, що завдають значних фінансових втрат підприємствам, банківським установам і державним органам, що порушує економічну стабільність та підриває довіру до цифрових технологій. З соціальної точки зору, кібератаки вивчають механізми впливу на суспільні настрої, породжують страх, дестабілізують громадську думку та сприяють поширенню дезінформації.

[1] Бондаренко І. Д. Шестаков В. І. Кібератаки РФ на Україну – воєнний злочин. *Юридичний науковий електронний журнал.* 2023. № 11. С. 614-619. URL: http://www.lsej.org.ua/11_2023/152.pdf

[2] The Gravity of Russia's Cyberwar against Ukraine. OpinioJuris: веб-сайт. URL: https://opiniojuris.org/2023/04/19/the-gravity-of-russias-cyberwar-against-ukraine/

Кібератаки як форма неправомірного впливу на інформаційні системи та цифрові ресурси можуть бути класифіковані за різними критеріями, включаючи мету атаки, методи реалізації, рівень завданої шкоди та правові наслідки.

1. Залежно від мети, кібератаки можуть бути спрямовані на:
- порушення доступності інформаційних систем (наприклад, DDoS-атаки);
- несанкціоноване отримання доступу до інформаційних ресурсів (хакерські атаки, фішинг);
- модифікацію або знищення даних (ransomware, дефейсинг);
- шахрайство та маніпулювання даними (спуфінг, соціальна інженерія);
- підрив національної або корпоративної безпеки (APT-атаки, кібершпигунство).

2. Залежно від методів здійснення розрізняють наступні види кібератаки:
- *DDoS-атаки (Distributed Denial of Service).* DDoS-атаки є найбільш поширеним видом кібератак, які мають на меті перевантаження інформаційної системи великою кількістю запитів. Юридична кваліфікація таких дій може ґрунтуватися на нормах кримінального права, зокрема як несанкціоноване втручання в роботу комп'ютерних мереж (ст. 361 КК України, аналогічні норми передбачені в CFAA у США та в Директиві 2013/40/EU в ЄС)[1].
- *фішингові атаки (Phishing).* Фішинг є однією з найбільш небезпечних форм соціальної інженерії, яка спрямована на обманне отримання доступу до конфіденційної інформації (логінів, паролів, банківських реквізитів). З точки зору правового регулювання фішинг може кваліфікуватися як шахрайство (ст. 190 КК України) або як Несанкціоновані дії з інформацією, яка обробляється в електронно-обчислювальних машинах (комп'ютерах) (ст. 362 КК України)[2].
- *програмне забезпечення – здирник (Ransomware*). Ransomware є формою шкідливого програмного забезпечення, яке блокує

[1] Directive 2013/40/EU on attacks against information systems. Official Journal of the European Union. 2013. URL: https://eur-lex.europa.eu/eli/dir/2013/40/oj/eng

[2] Кримінальний кодекс України: Закон України. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text

доступ до даних або пристроїв, вимагаючи викуп за відновлення доступу. Правові аспекти таких атак охоплюють кримінальну відповідальність за вимагання (ст. 189 КК України) та несанкціоноване втручання в комп'ютерні системи (ст. 361 КК України). Також, з міжнародно-правової точки зору, ransomware – кодифікація міститься у Будапештській конвенції про кіберзлочинність[1].

– *хакерські атаки (Hacking, SQL-injection, Brute-force).* Хакерські атаки охоплюють широкий спектр методів несанкціонованого доступу до інформаційних систем. SQL-ін'єкції та brute-force атаки використовуються для отримання контролю над базами даних, викрадення інформації або саботажу цифрової інфраструктури. Вони підпадають під дію законодавчих норм щодо комп'ютерного саботажу та кіберзлочинності (ст. 361-1 КК України, CFAA у США)[2].
– *атаки типу «Людина посередині» (Man-in-the-Middle, MitM).* MitM-атаки передбачають перехоплення та модифікацію даних між двома сторонами, які не підозрюють про втручання. Використовуються переважно для крадіжки конфіденційної інформації або змінення фінансових транзакцій.
– *кібершпигунство (Cyber Espionage, APT-атаки).* Кібершпигунство є однією з найсерйозніших загроз на рівні національної безпеки та корпоративного сектору. Атаки цього типу передбачають таємний, довготривалий доступ до інформаційних систем для отримання державних або комерційних таємниць. Юридично можуть кваліфікуватися як державна зрада (ст. 111 КК України), промислове шпигунство або незаконне розголошення комерційної таємниці.
– *шкідливе програмне забезпечення (Malware, Trojans, Worms, Spyware).* Категорія шкідливого програмного забезпечення охоплює віруси, трояни, черв'яки та програми-шпигуни, які можуть бути використані для викрадення даних, саботажу або несанкціонованого контролю над пристроями. В Україні такі дії можуть кваліфікуватися як розповсюдження шкідливого програмного забезпечення (ст. 361-1 КК Украї-

[1] Конвенція про кіберзлочинність. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text
[2] Computer Fraud and Abuse Act (CFAA). U. S. Code, Title 18, Section 1030, 1986.

ни), а в міжнародному праві – підпадати під Будапештську конвенцію[1].

Кібератаки є одним із найнебезпечніших викликів сучасного інформаційного суспільства, що можуть спричинити суттєві порушення цивільних прав фізичних та юридичних осіб. У правовій доктрині кібератаки розглядаються як протиправні діяння, що порушують принцип непорушності прав суб'єктів цивільних правовідносин, завдають шкоди їх майновому та немайновому становищу, а також підривають засади правового регулювання кіберпростору.

Кібератаки можуть спричинити безпосереднє або опосередковане *порушення права власності*, зокрема через:

– несанкціоноване заволодіння цифровими активами (крадіжка криптовалюти, цифрових сертифікатів, електронних грошей тощо);
– знищення, модифікацію або блокування доступу до майнових об'єктів (наприклад, ransomware – атаки, які обмежують доступ до інформаційних ресурсів та вимагають викуп);
– несанкціоноване використання програмного забезпечення або баз даних, що може призвести до економічних збитків.

Правова кваліфікація таких порушень ґрунтується на положеннях ст. 316-319 ЦК України щодо здійснення права власності та його захисту, а також міжнародних норм щодо захисту цифрових активів.

Кібератаки можуть спричинити несанкціоноване *втручання в приватне життя*, що проявляється в:

– перехопленні, викраденні або розголошенні персональних даних (зокрема, внаслідок фішингових атак, атак типу Man-in-the-Middle);
– несанкціонованому доступі до електронної пошти, соціальних мереж, цифрових профілів;
– розповсюдженні чутливих даних, що може мати репутаційні, економічні або психологічні наслідки для потерпілої особи.

Правовий захист таких прав ґрунтується на положеннях ст. 32 Конституції України, ст. 270 ЦК України, а також на міжнародних нормах, зокрема GDPR (Regulation (EU) 2016/679), що встановлює жорсткі вимоги щодо обробки та захисту персональних даних.

[1] IT-Sicherheitsgesetz 2.0. URL: https://www.openkritis.de/it-sicherheitsgesetz/ausblick-it-sicherheitsgesetz-2-0.html#:~:text=Das%20IT%2DSicherheitsgesetz%202.0%20ist,Neue%20KRITIS%2DPflichten.

Деструктивні кібератаки, спрямовані на компрометацію осіб або компаній, можуть порушувати п*раво на недоторканність честі, гідності та ділової репутації.* До таких дій можна віднести:

– дифамаційні кампанії, поширення неправдивої інформації, маніпулятивні вкиди в медіа та соціальних мережах;
– несанкціоноване розповсюдження компрометуючих матеріалів (відредагованих зображень, особистої переписки тощо);
– фальсифікацію комунікацій та цифрових слідів, зокрема через дипфейки та інші технології обману.

Ці аспекти регулюються ст. 277-299 ЦК України, а також міжнародними стандартами щодо боротьби з кібербулінгом та онлайн-наклепом.

Кібератаки можуть спричинити *порушення договірних відносин* та заподіяння шкоди господарській діяльності через:

– підрив комерційної діяльності шляхом атак на сайти, електронні платформи, фінансові системи (DDoS-атаки, хакерські зломи, маніпуляції з фінансовими транзакціями);
– фальсифікацію комерційних даних, що призводить до втрати довіри контрагентів та клієнтів;
– несанкціонований доступ до комерційної таємниці та використання конфіденційної інформації в конкурентних цілях (промислове шпигунство, кібершпигунство).

Охорона прав гарантується на основі ст.ст. 6, 627-629 ЦК України (щодо свободи договору), Закону України «Про захист від недобросовісної конкуренції».

У разі завдання шкоди фізичним або юридичним особам унаслідок кібератак потерпілі мають право вимагати відшкодування завданих збитків. Цивільно-правова відповідальність за кібератаки охоплює:

– відшкодування майнової шкоди (ст. 22, 1166 ЦК України);
– відшкодування моральної шкоди (ст. 23, 1167 ЦК України);
– відшкодування шкоди, завданої незаконним розповсюдженням персональних даних або компрометуючої інформації (ст. 277, 280 ЦК України).

Кібератаки можуть завдавати шкоди як фізичним, так і юридичним особам, порушуючи їхні майнові та немайнові права. Хоча деякі права є спільними для обох категорій суб'єктів, є й специфічні аспек-

ти, що відрізняють порушення прав фізичних осіб та порушення прав юридичних осіб.

Фізичні особи можуть зазнати порушення права власності та інших речових прав внаслідок несанкціонованого вилучення або блокування доступу до цифрових активів, викрадення криптовалюти, електронних грошей, цінних цифрових документів, знищення або модифікації особистих файлів і даних внаслідок атак типу ransomware, а також у разі несанкціонованого контролю над пристроями та акаунтами особи, що може мати наслідком як матеріальні збитки, так і втрату важливої особистої інформації. Крім того, кібератаки можуть посягати на право фізичної особи на приватність та захист персональних даних, зокрема шляхом несанкціонованого збирання, використання або розповсюдження персональних даних, перехоплення особистої кореспонденції, а також використання персональних даних для шахрайських схем, таких як оформлення кредитів або продаж чужих даних у Darknet. Порушенням немайнових прав є також посягання на честь, гідність і ділову репутацію фізичної особи через поширення неправдивої інформації, створення фейкових акаунтів, використання дипфейків, а також розголошення приватного життя. Окрему загрозу становлять фішингові схеми та соціальна інженерія, що вводять особу в оману та можуть спричинити серйозні фінансові втрати. Також порушується право на безпечне користування цифровими платформами, адже особа може втратити доступ до власних ресурсів або стати жертвою нав'язування шкідливого програмного забезпечення, що ставить під загрозу її цифрову безпеку. Важливим аспектом є також право на відшкодування завданої шкоди, оскільки фізична особа має право вимагати компенсації матеріальних збитків, зокрема у разі викрадення коштів або пошкодження особистого майна, а також моральної шкоди у випадках, коли кібератака спричинила серйозний психологічний стрес, шантаж або публікацію конфіденційної інформації.

Юридичні особи, у свою чергу, зазнають порушень права власності та інших майнових прав унаслідок несанкціонованого проникнення в корпоративні системи, крадіжки комерційної інформації, знищення або модифікації баз даних підприємства, зокрема клієнтських баз або бухгалтерських записів, а також через несанкціонований доступ до фінансових рахунків компанії, що може спричинити

значні економічні втрати. Важливим є також право на комерційну таємницю та захист конфіденційної інформації, адже кібершпигунство, незаконне отримання стратегічної інформації компанії, витік корпоративної інформації та використання викрадених даних для недобросовісної конкуренції можуть мати катастрофічні наслідки для підприємств, зокрема підрив довіри клієнтів і партнерів. Юридичні особи також стикаються з порушенням права на ділову репутацію через кампанії з дезінформації, поширення фейкових відгуків, наклепів, дискредитацію в інформаційному просторі, а також використання шахрайських схем, наприклад, фішингових атак від імені компанії, що завдає шкоди її іміджу. Окремим аспектом є порушення права на договірну діяльність та ведення господарської діяльності, адже кібератаки можуть призвести до зриву контрактів через блокування серверів або корпоративних систем, фальсифікації договірних відносин, маніпуляції цифровими підписами та підробки електронних контрактів, а також до несанкціонованого втручання в бізнес-процеси, що може паралізувати діяльність онлайн-магазинів, банківських установ, біржових платформ. У зв'язку з цим юридичні особи мають право на судовий захист та відшкодування завданих збитків, включаючи вимоги про компенсацію матеріальних втрат, зокрема недоотриманого прибутку, додаткових витрат на кібербезпеку, а також про відшкодування репутаційної шкоди, якщо через кібератаки було зруйновано довіру клієнтів та партнерів.

Таким чином, кібератаки завдають суттєвої шкоди як фізичним, так і юридичним особам, однак характер цих порушень відрізняється. Фізичні особи зазнають переважно порушень приватності, викрадення особистих даних, шахрайства, тоді як юридичні особи стикаються з економічними загрозами, витоком комерційної інформації, порушенням договірних зобов'язань.

Цивільно-правова відповідальність за шкоду, завдану кібератаками, ґрунтується на загальних положеннях деліктного права, що передбачають наявність правопорушення, шкоди, причинно-наслідкового зв'язку та вини заподіювача шкоди. Проте особливості кіберпростору, зокрема анонімність правопорушників, складність ідентифікації джерела атаки та глобальний характер правопорушень, зумовлюють специфічні підходи до встановлення відповідальності. Основою для притягнення до цивільно-правової відповідальності є

норми Цивільного кодексу України, міжнародні конвенції у сфері кіберзлочинності, а також спеціальне законодавство щодо захисту персональних даних та інформаційної безпеки.

Однією з ключових підстав цивільно-правової відповідальності за шкоду, завдану кібератаками, є неправомірне втручання в інформаційні системи, що порушує право власності на цифрові активи. Таке втручання може включати несанкціонований доступ до баз даних, знищення, модифікацію або шифрування інформації, блокування доступу до цифрових ресурсів, що спричиняє значні матеріальні та нематеріальні збитки потерпілим особам. Згідно зі ст. 1166 ЦК України, шкода, заподіяна неправомірними діями, підлягає відшкодуванню в повному обсязі, що передбачає компенсацію витрат на відновлення даних, втрачений прибуток та інші фінансові втрати.

Підставою цивільно-правової відповідальності є також порушення права особи на конфіденційність та захист персональних даних. Внаслідок кібератак часто відбувається неправомірне збирання, обробка або поширення персональної інформації, що суперечить Закону України «Про захист персональних даних» та Регламенту ЄС 2016/679 (GDPR). Витік конфіденційної інформації може спричинити фінансові втрати, порушення права на недоторканність приватного життя, репутаційні ризики. У таких випадках відповідальними можуть бути як безпосередні ініціатори кібератаки, так і володільці баз даних, які не забезпечили належного рівня кіберзахисту.

Окрему категорію правопорушень становлять кібератаки, що спричиняють шкоду корпоративним правам, зокрема порушують комерційну таємницю або завдають шкоди діловій репутації. Несанкціоноване оприлюднення бізнес-стратегій, фінансових звітів, що може суттєво підірвати конкурентні позиції компаній та завдати значних збитків. Відповідно до ст. 22 ЦК України, юридичні особи мають право на відшкодування реальних збитків та упущеної вигоди, якщо доведено, що розголошення комерційної інформації або її модифікація внаслідок кібератаки призвели до фінансових втрат.

Ще однією підставою для цивільно-правової відповідальності є шкода, заподіяна внаслідок використання соціальної інженерії та маніпулятивних кіберметодів, таких як фішинг, ransomware або DDoS-атаки. Такі дії можуть призвести до прямого фінансового збитку, оскільки жертви, введені в оману, здійснюють неправомірні платежі

або передають доступ до своїх фінансових ресурсів. У таких випадках судова практика визнає можливість відшкодування шкоди за рахунок винних осіб, а також відповідальність третіх осіб (наприклад, власників цифрових платформ), які не вжили належних заходів для запобігання шахрайським схемам.

Встановлення причинно-наслідкового зв'язку у випадках кібератак є складним процесом, що вимагає комплексного підходу та залучення різних спеціалістів. Особливо важливим є визначення, чи є кібератака форс – мажорною обставиною, що може звільнити сторону від відповідальності за невиконання зобов'язань[1].

Форс-мажорні обставини – це надзвичайні, непередбачувані та невідворотні події, які унеможливлюють виконання зобов'язань. Кібератака може бути визнана форс-мажором, якщо вона відповідає цим критеріям і безпосередньо впливає на здатність виконати зобов'язання. Наприклад, якщо компанія не може провести розрахунки через відсутність доступу до клієнт-банку внаслідок кібератаки, це може бути підставою для визнання форс-мажору[2].

Для встановлення причинно-наслідкового зв'язку необхідно підтвердити факт кібератаки. Це можна зробити шляхом звернення до правоохоронних органів, залучення експертів у сфері IT-технологій або аналізу документів досудового розслідування. Зокрема, протоколи огляду місця події можуть зафіксувати факт кібератаки та перелік уражених комп'ютерів та обладнання.

Для підтвердження факту кібератаки необхідно встановити, що вона безпосередньо призвела до неможливості виконання зобов'язань. Для цього слід аналізувати документи та звіти, оцінити вплив на діяльність та у разі необхідності, залучити фахівців для детального аналізу.

Всі етапи встановлення причинно-наслідкового зв'язку повинні бути належним чином задокументовані. Це включає підготовку звітів та забезпечення належного зберігання всіх доказів, включаючи електронні дані, протоколи та висновки експертів.

---

[1] Подоляка Н. В. Інтеграція методів причинно-наслідкового зв'язку та SWOT-аналізу щодо визначення інформаційних ризиків: пояснювальна записка до атестаційної роботи здобувача вищої освіти на другому (магістерському) рівні, спеціальність 125 Кібербезпека. Харків, 2020. 69 с.

[2] Висіцька І. Кібератака як форс-мажор: особливості визнання. URL: https://vysitska.com/2017/12/03/кібератака-як-форс-мажор-особливості/?utm_source=chatgpt.com

Встановлення причинно-наслідкового зв'язку у випадках кібератак є важливим етапом у визначенні відповідальності та можливості застосування форс-мажору. Врахування всіх вищезазначених аспектів дозволяє забезпечити об'єктивність та достовірність процесу.

Ідентифікація правопорушника та визначення суб'єкта відповідальності в контексті кіберзлочинності є надзвичайно складним завданням, що зумовлені низкою специфічних факторів.

По-перше, анонімність та глобальний характер Інтернету ускладнюють встановлення особи правопорушника. Зловмисники можуть використовувати технології для приховування своєї особистості, що ускладнює процес ідентифікації. Наприклад, використання проксі-серверів або VPN дозволяє маскувати реальне місцезнаходження та особисті дані зловмисника.

По-друге, відсутність фізичних слідів та традиційних доказів, характерних для злочинів у реальному світі, ускладнює процес доказування. Цифрові докази можуть бути легко змінені або знищені, що ставить перед правоохоронними органами додаткові виклики.

Щодо суб'єкта відповідальності, то відповідно до законодавства, суб'єктами кіберзлочинів можуть бути фізичні осудні особи, які до моменту вчинення злочину досягли шістнадцятирічного віку. Водночас, спеціальний суб'єкт має місце у двох випадках: коли особа є посадовою особою або коли злочин вчинено з використанням спеціальних технічних засобів або програмного забезпечення[1].

З точки зору цивільного права, питання вини та безвинної відповідальності набувають особливої актуальності при розгляді випадків кібератак. Цивільно-правова відповідальність за шкоду, заподіяну внаслідок кібератак, може бути заснована як на вині, так і на шкоді, що була завдана без умислу, залежно від обставин конкретної справи.

Вина в цивільному праві розглядається як психічне ставлення особи до своєї протиправної поведінки та її наслідків. Вона може бути у формі умислу або необережності. У випадку кібератак, якщо особа свідомо та навмисно вчиняє дії, що призводять до шкоди іншій особі, така поведінка кваліфікується як умисел. Якщо ж особа не передба-

[1] Савчук Н. В. Кіберзлочинність: зміст та методи боротьби. *Теоретичні та прикладні питання економіки*: зб. наук. пр. К.: Київ. ун-т, 2009. Вип. 19. С. 338-342

чала можливості настання шкоди, але повинна була і могла її передбачити, то відповідальність настає за необережність[1].

У цивільному праві, відповідальність за шкоду завдану внаслідок необережності може бути встановлена у випадках, коли закон прямо передбачає таку відповідальність, наприклад, за шкоду, заподіяну внаслідок діяльності, що створює підвищену небезпеку для оточуючих. Щодо кібератак, відповідальність за шкоду завдану необережними діями може бути застосована, якщо особа здійснює діяльність, пов'язану з підвищеним ризиком виникнення кібератак, і навіть при відсутності вини з її боку, шкода все одно повинна бути відшкодована. При розгляді справ про кібератаки необхідно ретельно аналізувати обставини, що призвели до шкоди. Важливо встановити, чи діяла особа умисно або з необережності, а також чи здійснювала вона діяльність, пов'язану з підвищеним ризиком виникнення кібератак. У разі встановлення умислу або необережності, особа несе відповідальність за заподіяну шкоду. Якщо ж шкода була заподіяна внаслідок діяльності, що створює підвищену небезпеку, і навіть при відсутності вини, відповідальність настає без вини.

Що стосується юридичних осіб, то вони несуть відповідальність за неналежний рівень кібербезпеки у випадках, коли їх дії або бездіяльність призводять до порушення законодавства у сфері кібербезпеки. Основним нормативно-правовим актом, що регулює ці питання, є Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII. Згідно з цим законом, особи, винні у порушенні законодавства у сферах національної безпеки, оборони, захисту державної таємниці, несуть відповідальність відповідно до закону.

Відповідальність може наставати у випадках, коли юридична особа не забезпечила належний захист інформаційних систем, що призвело до несанкціонованого доступу, витоку конфіденційної інформації або інших кіберінцидентів. Також відповідальність може бути застосована, якщо організація не виконала законних вимог посадових осіб Служби безпеки України або Державної служби спеціального зв'язку та захисту інформації України щодо забезпечення кібербезпеки.[2]

---

[1] Тихомиров О. О. Інформаційний делікт як підстава «інформаційної» юридичної відповідальності: відмітні ознаки. *Інформація і право.* 2019. № 1. С. 37-44.

[2] Доронін І. М. Правове регулювання забезпечення кібербезпеки у реалізації окремих функцій держави. *Інформація і право.* 2017. № 1(20). С. 107. URL: https://ippi.org.ua/sites/default/files/13_3.pdf

Крім того, міжнародні стандарти, такі як Конвенція Ради Європи про кіберзлочинність, передбачають відповідальність юридичних осіб за кримінальні правопорушення, вчинені на їх користь особами, які займають керівні посади. Це означає, що організація може бути притягнута до відповідальності, якщо її керівництво не забезпечило належний рівень кібербезпеки, що призвело до правопорушення[1].

Кібератаки становлять серйозну загрозу для сучасних організацій, завдаючи різноманітних видів шкоди, серед яких матеріальна, моральна та репутаційна. Розуміння природи та наслідків кожного з цих типів шкоди є сьогодні важливим для розробки ефективних стратегій захисту та відшкодування.

Матеріальна шкода внаслідок кібератак проявляється у прямих фінансових втратах, які можуть включати витрати на відновлення систем, втрату прибутку через простої. Наприклад, атаки типу «відмова в обслуговуванні» (DDoS) можуть призвести до тривалих простоїв веб-сайтів або сервісів, що безпосередньо впливає на доходи компанії. Крім того, витрати на залучення експертів з кібербезпеки для усунення наслідків атаки та впровадження додаткових заходів захисту також складають значну частину матеріальних збитків.

Матеріальна шкода, завдана кібератаками, є суттєвою проблемою сучасного інформаційного суспільства, оскільки такі атаки можуть призвести до значних фінансових втрат, порушення бізнес-процесів та зниження довіри до цифрових технологій.

Фінансові втрати внаслідок кібератак можуть включати прямі витрати, такі як витрати на відновлення систем, виплату викупу при атаках типу ransomware, а також непрямі втрати, пов'язані з простоєм бізнесу та втратою клієнтів. Наприклад, у січні 2024 року повідомлялося про зростання активності хакерських груп, що займаються програмами-вимагачами, які все частіше атакують медичні заклади, завдаючи їм значних фінансових збитків. До прикладу, колишнього розробника Trickbot Володимира Дунаєва було притягнуто до відповідальності за злочин, який полягав у зараженні американських лікарень і підприємств ransomware Trickbot, що коштувало жертвам збитків у десятки мільйонів доларів. За даними Національного агент-

[1] Правова база української кібербезпеки: загальний огляд і аналіз. *Міжнародна фундація виборчих систем в Україні.* 2019. URL: https://ifesukraine.org/wp-content/uploads/2019/10/IFES-Ukraine-Ukrainian-Cybersecurity-Legal-Framework-Overview-and-Analysis-2019-10-07-Ukr.pdf

ства зі злочинності Великобританії, зловмисники виманили щонайменше 180 мільйонів доларів США (145 мільйонів фунтів стерлінгів) у людей і організацій по всьому світу[1].

Порушення бізнес-процесів є ще одним наслідком кібератак. Збої в роботі інформаційних систем можуть призвести до тимчасової недоступності послуг або продуктів, що негативно впливає на репутацію компанії та її конкурентоспроможність. Наприклад, атака програми-вимагача на компанію TietoEVRY у Швеції вплинула на послуги для деяких клієнтів, що підкреслює вразливість бізнесу до кібератак.

Витрати на відновлення та посилення систем безпеки після кібератак також є значними. Компанії змушені інвестувати в оновлення інфраструктури, навчання персоналу та впровадження нових заходів безпеки, щоб запобігти майбутнім інцидентам.

Окрім прямих фінансових втрат, кібератаки можуть спричинити моральну шкоду, яка стосується психологічного впливу на постраждалих осіб. Це може включати стрес, тривогу та інші негативні емоційні реакції, пов'язані з втратою конфіденційної інформації або порушенням приватності. Особливо це стосується випадків, коли особисті дані співробітників або клієнтів стають доступними зловмисникам, що може призвести до відчуття небезпеки та вразливості серед постраждалих. Оцінка моральної шкоди внаслідок кібератак є складним завданням через нематеріальний характер таких втрат[2]. Відсутність чітких критеріїв оцінки та стандартизованих методик може призводити до суб'єктивності в судових рішеннях.

Репутаційна шкода є ще одним критичним аспектом наслідків кібератак. Публічне розголошення фактів про успішні атаки на компанію може суттєво підірвати довіру клієнтів, партнерів та інвесторів. Втрата репутації часто має довгострокові наслідки, які важко піддаються кількісній оцінці, але безпосередньо впливають на конкурентоспроможність та ринкову позицію організації. Відновлення довіри після таких інцидентів вимагає значних зусиль та ресурсів, включаючи проведення PR-кампаній та впровадження додаткових заходів безпеки. Особливо небезпечними є атаки, пов'язані з розголошенням

[1] Cyber Digest: Огляд подій в сфері кібербезпеки, січень 2024 С. 20. URL: https://www.rnbo.gov.ua/files/2024/NATIONAL_CYBER_SCC/Cyber%20digest/Cyber%20digest_Jan_2024_UA.pdf

[2] Особливості відшкодування моральної шкоди. URL: https://legalaid.gov.ua/novyny/osoblyvosti-vidshkoduvannya-moralnoyi-shkody/

персональних даних, оскільки вони можуть викликати скандали та судові позови. Публічне висвітлення таких інцидентів у засобах масової інформації часто погіршує ситуацію, формуючи негативний імідж компанії або особи. Це, у свою чергу, може спричинити фінансові втрати, оскільки клієнти починають уникати співпраці з організацією, яка не змогла забезпечити належний рівень захисту інформації. Багато компаній після масштабних кібератак стикаються зі зниженням вартості акцій, оскільки інвестори втрачають довіру до їхньої здатності захистити свої активи. У деяких випадках, особливо якщо йдеться про державні установи або великі корпорації, наслідки можуть бути ще серйознішими, адже кібератаки можуть підривати національну безпеку або довіру громадськості до ключових інституцій. Часто постраждалі компанії намагаються мінімізувати наслідки шляхом кризових комунікацій, але відновлення довіри може тривати роками. Захист від таких загроз потребує не лише впровадження сучасних технологій кібербезпеки, а й продуманої стратегії управління репутаційними ризиками. Відкритість та оперативне інформування клієнтів про заходи, яких вжито для усунення загроз, може допомогти пом'якшити удар по репутації. Однак навіть швидка реакція не завжди може компенсувати репутаційні втрати, особливо якщо атака була масштабною або сталася повторно. У цифрову епоху, коли будь-яка інформація швидко поширюється мережею, репутація стає одним із найцінніших активів, і її пошкодження через кібератаки може мати довгострокові наслідки.

Важливо зазначити, що ці види шкоди взаємопов'язані та можуть посилювати один одного. Наприклад, матеріальні втрати через кібератаку можуть призвести до моральної шкоди серед співробітників, які переживають за своє майбутнє, а репутаційні втрати можуть спричинити додаткові фінансові збитки через відтік клієнтів. Тому комплексний підхід до оцінки та управління ризиками кібератак є необхідним для мінімізації потенційних збитків.

Крім безпосередніх втрат, кібератаки можуть мати довгострокові наслідки для інноваційного потенціалу компанії. Витік конфіденційної інформації, такої як комерційні таємниці або дані про розробки, може призвести до втрати конкурентних переваг. Це, в свою чергу, впливає на здатність компанії впроваджувати нові продукти або послуги, що негативно позначається на її позиції на ринку.

Крім того, кібератаки можуть призвести до штрафів та інших санкцій з боку регуляторних органів. Це додає додатковий фінансовий тягар та може ще більше погіршити репутацію компанії. Тому дотримання нормативних вимог у сфері кібербезпеки є критично важливим для мінімізації таких ризиків. У контексті глобалізації бізнесу, кібератаки можуть мати міжнародні наслідки, впливаючи на партнерські відносини та ринки збуту в інших країнах. Витік даних або компрометація систем може призвести до втрати довіри з боку міжнародних партнерів, що ускладнює вихід на нові ринки або підтримку існуючих бізнес-зв'язків.

Отже, кібератаки можуть завдавати багатогранної шкоди організаціям, охоплюючи матеріальні, моральні та репутаційні аспекти. Розуміння та оцінка кожного з цих видів шкоди є необхідними для розробки ефективних стратегій захисту та відшкодування, що дозволить мінімізувати негативні наслідки та забезпечити стійкість організації в умовах сучасних кіберзагроз.

Складним є процес доведення шкоди та її розміру після кібератаки, адже це вимагає системного підходу та залучення різних фахівців. Цей процес включає кілька ключових етапів:

1. Виявлення та документування інциденту – це є першим кроком задля фіксації факту кібератаки, що включає збереження скріншотів та інших доказів. Важливо забезпечити цілісність цих даних для подальшого аналізу.

2. Оцінка обсягу та характеру втрат – після виявлення атаки необхідно визначити, які системи та дані були скомпрометовані, а також оцінити тривалість та інтенсивність впливу. Це дозволяє встановити масштаби шкоди.

3. Визначення фінансових втрат – оцінка матеріальних збитків включає підрахунок витрат на відновлення систем, втрати доходів через простої, витрати на юридичні послуги та можливі штрафи. Цей етап вимагає залучення фінансових експертів для точного розрахунку.

4. Оцінка моральної та репутаційної шкоди – визначення впливу на моральний стан співробітників та клієнтів, а також на репутацію компанії, є складним завданням. Для цього можуть використовуватися опитування, аналіз відгуків та моніторинг медіа.

5. Залучення експертів з кібербезпеки – фахівці з кібербезпеки проводять технічний аналіз інциденту, визначають вразливості та

оцінюють ефективність існуючих заходів захисту. Їхні висновки є важливими для розуміння причин та наслідків атаки.

7. Використання методичних рекомендацій – згідно з Методичними рекомендаціями щодо визначення ризиків та оцінки їхнього впливу, для визначення ризику застосовуються дані щодо загроз, вразливостей, їх ймовірностей та рівня шкоди. Це дозволяє системно підходити до оцінки потенційних втрат[1].

Загалом, процес доведення шкоди та її розміру після кібератаки вимагає комплексного підходу, залучення різних фахівців та використання спеціалізованих методик для точного визначення масштабів втрат та розробки ефективної стратегії відшкодування[2].

Відшкодування шкоди, завданої кібератаками, здійснюється відповідно до загальних принципів цивільного права України, з урахуванням специфіки кіберзлочинів. Основними способами відшкодування є грошова компенсація та відновлення порушених прав у натурі.

Грошова компенсація передбачає виплату потерпілому суми, еквівалентної завданим збиткам. Згідно зі ст. 22 ЦК України, збитками визнаються:

1. втрати, яких особа зазнала у зв'язку зі знищенням або пошкодженням майна;

2. витрати, які особа зробила або мусить зробити для відновлення свого порушеного права;

3. неодержані доходи, які особа могла б реально одержати за звичайних обставин, якби її право не було порушене.

Відновлення порушених прав у натурі полягає в реальному відновленні стану, який існував до порушення. Це може включати повернення викрадених даних або відновлення працездатності інформаційних систем. Стаття 1192 ЦК України передбачає, що за вибором потерпілого особа, яка завдала шкоди майну, може бути зобов'язана відшкодувати її в натурі або компенсувати завдані збитки у повному обсязі.

---

[1] Правова база української кібербезпеки: загальний огляд і аналіз. *Міжнародна фундація виборчих систем в Україні.* 2019. URL: https://ifesukraine.org/wp-content/uploads/2019/10/IFES-Ukraine-Ukrainian-Cybersecurity-Legal-Framework-Overview-and-Analysis-2019-10-07-Ukr.pdf?utm_source=chatgpt.com

[2] Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест. Відп. ред. О. Довгань; Державна наукова установа «Інститут інформації, безпеки і права НАПрН України»; Національна бібліотека України ім. В. І. Вернадського. К., 2024. № 6. 364 с.

У випадках, коли кібератака призвела до витоку конфіденційної інформації, що спричинило моральну шкоду, потерпілий має право на її компенсацію. Розмір такої компенсації визначається судом з урахуванням характеру правопорушення та глибини моральних страждань.

Варто зазначити, що відшкодування шкоди, завданої кібератаками, може бути ускладнене через труднощі в ідентифікації винних осіб та міжнародний характер таких злочинів. Тому важливу роль відіграє співпраця з правоохоронними органами та міжнародними організаціями для встановлення винних та притягнення їх до відповідальності.

Таким чином, відшкодування шкоди, завданої кібератаками, базується на загальних принципах цивільного права України, але потребує врахування специфіки кіберзлочинів та можливих труднощів у притягненні винних до відповідальності.

Страхування кіберризиків є важливим інструментом управління ризиками в умовах цифровізації, забезпечуючи фінансовий захист від наслідків кібератак та інших кіберзагроз. Цей вид страхування спрямований на компенсацію збитків, завданих порушенням інформаційної безпеки, та допомагає підприємствам швидко відновити свою діяльність після інцидентів.

Основною метою кіберстрахування є забезпечення фінансового механізму відновлення після значних збитків, допомагаючи підприємствам повернутися до нормального функціонування, зберегти стабільність, платоспроможність та знизити втрати в результаті перерви у виробництві[1].

Кіберстрахування покриває широкий спектр ризиків, включаючи втрату даних, зниження репутації, відшкодування збитків клієнтам та інші опції[2]. Це дозволяє підприємствам ефективно управляти потенційними загрозами та мінімізувати фінансові втрати від кібератак.

В Україні розвиток кіберстрахування стикається з певними проблемами, такими як відсутність цього виду страхування у більшості страхових компаній та недостатня обізнаність підприємств про його

[1] Розвиток кіберстрахування як сегменту глобального страхового ринку. URL: https://kon-insurance.mnau.edu.ua/files/work_2020/6.pdf

[2] Попович Д. В., Бундз Н. Б., Іванків В. О. Проблеми та перспективи розвитку страхування кіберризиків на національному ринку. *Молодий вчений.* № 4 (116). 2023. С. 864-867.

переваги[1]. Однак, з огляду на зростання кіберзлочинності та впровадження цифрових технологій, потреба в кіберстрахуванні стає все більш актуальною.

Важливим аспектом кіберстрахування є необхідність оцінки кіберризиків та визначення умов страхування, розміру страхового покриття і премій. Це вимагає від страхових компаній глибокого розуміння специфіки кіберзагроз та здатності проводити незалежну фахову експертизу кіберризиків.

Таким чином, страхування кіберризиків виступає ефективним механізмом компенсації шкоди, завданої кібератаками, та є невід'ємною частиною сучасної системи управління ризиками в умовах цифрової економіки.

Правове регулювання відповідальності за шкоду, завдану кібератаками, в Україні стикається з низкою прогалин, що ускладнюють ефективну боротьбу з кіберзлочинністю та захист прав потерпілих. Основні проблеми включають недостатню деталізацію законодавства, відсутність чітких визначень ключових термінів та неузгодженість між нормативно-правовими актами.

По-перше, в українському законодавстві відсутні чіткі та загальновизнані визначення таких понять, як «кібератака», «кіберзагроза», «кіберзлочин» тощо. Це призводить до неоднозначного тлумачення та застосування норм права на практиці. Запропоновано законодавчо закріпити основні терміни кібербезпеки, що сприятиме уніфікації підходів до їх розуміння та застосування.

По-друге, існує проблема неузгодженості між різними нормативно-правовими актами, що регулюють сферу кібербезпеки. Це створює труднощі у визначенні відповідальності за кіберзлочини та механізмів компенсації шкоди. Необхідно провести комплексний аналіз чинного законодавства з метою виявлення та усунення суперечностей, а також розробити єдину стратегію кібербезпеки, яка б враховувала сучасні виклики та загрози[2].

По-третє, наявні прогалини у визначенні відповідальності за кіберзлочини, вчинені в умовах війни. Запровадження відповідально-

[1] Іванова Т. Г. Перспективи розвитку ринку кіберстрахування в Україні. URL: https://ir.kneu.edu.ua/server/api/core/bitstreams/f44303d4-aa69-42bb-b043-5519e3394df6/content

[2] Федорін М., Заєць Я. Про особливості правового забезпечення кібернетичної безпеки (кібербезпеки) в Україні. URL: http://lawdrafting.org/pro-osoblivosti-pravovogo-zabezpechennya-kibernetichnoyi-bezpeki-kiberbezpeki-v-ukrayini/

сті за такі дії є необхідним для забезпечення національної безпеки та захисту суспільних інтересів України.

Для усунення зазначених прогалин, на нашу думку, необхідно:

1. Розробити та впровадити спеціалізоване законодавство у сфері кібербезпеки, яке б чітко визначало правовий статус суб'єктів кіберпростору, їх права та обов'язки, а також встановлювало відповідальність за порушення у цій сфері.

2. Гармонізувати національне законодавство з міжнародними стандартами та практиками у сфері кібербезпеки. Це сприятиме ефективній міжнародній співпраці у боротьбі з кіберзлочинністю та забезпечить належний рівень захисту прав потерпілих.

3. Підвищити кваліфікацію правоохоронних органів та суддівського корпусу у сфері кібербезпеки. Це забезпечить ефективне застосування законодавства та належний захист прав потерпілих від кібератак.

Таким чином, усунення прогалин у правовому регулюванні відповідальності за шкоду, завдану кібератаками, вимагає комплексного підходу, який включає вдосконалення законодавства, гармонізацію його з міжнародними стандартами та підвищення професійного рівня фахівців у сфері кібербезпеки.

Цивільно-правова відповідальність за шкоду, завдану кібератаками – це встановлений законом обов'язок особи, яка вчинила неправомірне втручання в інформаційні системи, електронні комунікаційні мережі або дані, відшкодувати матеріальні збитки та/або моральну шкоду, заподіяну потерпілій особі чи організації. Вона ґрунтується на загальних принципах деліктного та договірного права, передбачаючи можливість відшкодування матеріальних збитків, компенсації моральної шкоди та відновлення порушених прав.

Важливим аспектом є складність ідентифікації порушників у кіберпросторі, що ускладнює процес притягнення їх до відповідальності. Відсутність чітких правових механізмів для боротьби з міжнародними кіберзлочинцями також є серйозною проблемою. Основними способами відшкодування шкоди виступають грошова компенсація, відновлення в натурі та компенсація моральної шкоди. Проте правозастосовна практика щодо таких справ в Україні ще не є достатньо розвиненою, що потребує додаткового законодавчого врегулювання та роз'яснень. Необхідно вдосконалювати правові механізми,

зокрема гармонізувати українське законодавство з міжнародними стандартами, забезпечити ефективне страхування кіберризиків і розробити спеціалізовані процедури для розгляду справ про кібератаки в судовому порядку. Державі слід активізувати міжнародну співпрацю у сфері кібербезпеки для ефективного розслідування злочинів, а також розвивати спеціалізовані підрозділи, що займаються кіберзлочинністю.

Важливим напрямом є підвищення обізнаності бізнесу та громадян щодо засобів захисту від кіберзагроз, а також впровадження обов'язкових стандартів кібербезпеки для підприємств, що працюють із конфіденційними даними.

Отже, цивільно-правова відповідальність за кібератаки потребує подальшого розвитку та адаптації до сучасних викликів. Створення дієвої системи правового захисту потерпілих сприятиме підвищенню рівня безпеки у цифровому середовищі та зміцненню довіри до правових механізмів відшкодування шкоди.

Ключові слова: цивільно-правова відповідальність, відшкодування шкоди, майнові права, немайнові права, ділова репутація, кібератака, кібербезпека, кіберстрахування, методи цивільно-правового регулювання, національна безпека, кіберзагроза, гібридна війна, інформаційна війна.

Розділ 19

СІМЕЙНІ ПРАВОВІДНОСИНИ В СФЕРІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

DOI

Оксана Сафончик
докторка юридичних наук, професорка

Укладання шлюбу та ІТ в умовах гібридної війни

Сімейний Кодекс України у ст. 21 дає визначення шлюбу як сімейного союзу чоловіка і жінки, який зареєстрований у державному органі РАЦС. Крім того, певна норма закріплена й Конституцією України (ч.1 ст. 51). Звідси шлюб, у правовому аспекті, регулює відносини між чоловіком і жінкою щодо створення сім'ї, адже саме сім'я є головним інститутом сучасного суспільства.

Шлюб як союз чоловіка і жінки, що має соціальне значення, визначає правове становище дітей, народжених у цьому союзі, майнові відносини між подружжям та їхні спадкові права. Щодо цих прав шлюб є юридичним фактом, однак укладення такого союзу залежить від волі майбутнього подружжя і є юридичним правочином[1].

У сучасному правничому світі деякі вчені країн ЄС наголошують на тому, що шлюбні відносини можуть виникати й між особами однієї статі, які можуть укласти шлюб як партнери. Пояснюють вони це тим, що шлюб – це союз між двома особами, які мають бажання створити сім'ю та разом виховувати дитину.

А от українське сімейне законодавство не дозволяє укладення шлюбу між одностатевими партнерами, бо закріплює основні ознаки шлюбу: це союз саме жінки і чоловіка, тобто осіб різної статі[2]; це сімейний союз, який припускає спільне проживання, ведення спільного

[1] Шимон С. І. Майнові права як об'єкти цивільних правовідносин (теоретичні та практичні аспекти): автореф. дис.... д-ра юрид. наук. Київ, 2014. 40 с.

[2] Муравйов В. Гармонізація законодавства і європейська інтеграція. *Право України.* 2013. № 6. С. 12–50.

побуту, наявність взаємних прав і обов'язків (ч. 2 ст. 3 СК України)[1]; це рівноправний союз між чоловіком і жінкою, який зареєстрований в органі РАЦС та укладається на невизначений строк.

Звідси випливає, що при проживанні жінки і чоловіка однією сім'єю без державної реєстрації шлюбу в них не виникає прав і обов'язків подружжя, хоч сімейний союз існує. Не змінює цього становища навіть і той факт, що вони укладають певний шлюбний обряд за звичаями тієї чи іншої народності або шлюбний релігійний обряд (вінчання)[2]. Хоч у випадках, передбачених законом, шлюбу, що укладений за релігійним обрядом, надається юридичне значення. Це стосується шлюбів, які укладені за релігійними обрядами до створення або відновлення державних органів РАЦС (ч.ч. 2, 3 ст. 21 СК України)[3].

У сімейному законодавстві України закріплено порядок укладення шлюбів. Порядок укладення шлюбу – це прямо регламентована чинним законодавством процедура, що включає в себе дії органу РАЦС і осіб, які вступають у шлюб, спрямовані на вчинення державної реєстрації створення сім'ї як акту цивільного стану. До цього порядку належать умови, за яких шлюб уважатиметься укладеним. Отже, шлюб за сімейним законодавством України укладається на умовах добровільності між чоловіком і жінкою (в Україні примушення жінки і чоловіка до шлюбу не допускається) (ст. 24 СК України), які досягли шлюбного віку (ст. 22 СК України), мають сімейну правоздатність (ст. 25 СК України), не є між собою родичами прямої лінії чи братами і сестрами, не перебувають у іншому не припиненому шлюбі.

Відповідно положень СК України укладення шлюбу зводиться до наступних етапів:

1. Звернення до державного органу РАЦСу жінки та чоловіка, які виявили бажання укласти шлюб (ч. 2 ст. 28 СК України).

2 Ознайомлення осіб, які бажають зареєструвати шлюб, з їхніми правами та обов'язками (ст. 29 СК України).

3. Прийняття державними органами РАЦСу заяви за наявності всіх необхідних документів.

---

[1] Сімейне право України: підручник. За заг ред. Дзера О. В. Бондар Т. В. К.:ЮрІнком Інтер. 2023. 520 с.

[2] Сімейне право України: підручник. Суми: Юрінком Інтер, 2020. 520 с

[3] Сімейний Кодекс України: наук.-практ. Коментар/Станом на 01.01.2025/за заг. ред. Харитонова Є. О., Сафончик О. І. 432с.

4. Реєстрація шлюбу (ст. 34 СК України).

СК України передбачає досягнення шлюбного віку (ст. 23)[1], встановлюючи особливе шлюбне повноліття тільки для жінок. Відповідно до ч. 1 ст. 22, шлюбний вік для жінки і для чоловіка настає у вісімнадцять років. Установлення шлюбного віку є однією з умов отримання права на укладення шлюбу[2], бо особа, яка прагне укласти шлюб, має досягти статевої зрілості (тобто бути фізично зрілою) та відповідного стану розумового, психічного, морального і соціального розвитку. Досягнення шлюбного віку має відбутися на день реєстрації шлюбу (ч. 2 ст. 22 СК України), а це означає, що подати заяву може й особа, яка ще не досягла шлюбного віку, але досягне його не пізніше як протягом одного місяця з дня подачі заяви.

Деякі інші правники, зокрема Ю. С. Червоний, наполягають, що в ч. 2 ст. 23 СК України йдеться про зниження шлюбного віку[3], бо СК України передбачає можливість надання права на шлюб особі, яка ще не досягла шлюбного віку. Відповідно до ч. 2 ст. 23 СК України, за заявою особи, яка досягла шістнадцяти років, за рішенням суду їй може бути надано таке право, якщо буде встановлено, що це відповідає її інтересам. Отже, з позицією Ю. С. Червоного можна не погодитись, бо в зазначеній нормі сімейного права України йдеться саме про надання права на шлюб неповнолітній особі, а не про зниження шлюбного віку. Останній лише надається право на шлюб, якщо буде встановлено, що таким чином захищаються її інтереси (фактичне утворення сім'ї, вагітність, народження дитини, тяжке захворювання тощо). Передбачено, що з такою заявою може звернутися до суду лише особа, яка досягла віку шістнадцяти років. У свою чергу, суд розглядає заяву за правилами окремого провадження, повідомивши про це батьків і піклувальників неповнолітньої особи.

Одночасно з цим, ураховуючи аспекти розвитку й інтеграції українського законодавства до міжнародно-правових актів сімейного права країн ЄС, СК України передбачає можливість пред'явлення відповідної заяви про укладення шлюбу не лише за особи-

[1] Сімейний Кодекс України: наук.-практ. Коментар/Станом на 01.01.2025/за заг. ред. Харитонова Є. О., Сафончик О. І. 432с.

[2] Сімейне право України: підручник. За заг ред. Дзери, О. В. Бондар Т. В. К.:ЮрІнком Інтер. 2023. С. 87.

[3] Червоний Ю. С. Цивільний процес України: підручник. Київ: Істина, 2007. С.311

стою присутністю, а й через представників за умов засвідчення такої заяви нотаріально, за наявності нотаріально посвідченої довіреності. Однак зробити це можна лише за наявності поважних причин, що перешкоджають особистим зверненням. СК України не дає переліку причин неможливості подати заяву про укладення шлюбу особисто, але можна припустити, що ними можуть бути хвороба чи відрядження.

Акти цивільного стану визначаються у ст. 49 ЦК України як події та дії, що нерозривно пов'язані з фізичною особою і започатковують, змінюють, доповнюють або припиняють її можливість бути суб'єктом цивільних прав і обов'язків. До таких подій і дій ЦК України вважає належним, зокрема: народження фізичної особи, встановлення її походження, набуття та вихід з громадянства, досягнення відповідного віку, надання повної цивільної дієздатності, обмеження цивільної дієздатності, визнання особи недієздатною, укладення шлюбу, розірвання шлюбу, усиновлення, зміну імені, інвалідність, смерть тощо. Деякі з них, відповідно до Закону України «Про державну реєстрацію актів цивільного стану»[1], підлягають державній реєстрації. Це стосується народження фізичної особи та її походження, укладення шлюбу, розірвання шлюбу у випадках, передбаченим законом, зміни імені, смерті.

Державна реєстрація актів цивільного стану проводиться відділами ДРАЦС, виконавчими органами сільських, селищних і міських (крім міст обласного значення) рад. Акти цивільного стану стосовно громадян України, що проживають за кордоном, реєструються консульськими установами України.

Державна реєстрація актів цивільного стану здійснюється шляхом створення двох ідентичних екземплярів записів на бланку відповідної форми, куди включаються необхідні відомості про громадянина і про сам акт цивільного стану.

Крім того, останнім часом у зв'язку з розвитком ІТ-технологій[2] Українська держава розробила пілотний проект, який надає українцям можливість звернутися із заявою на укладення шлюбу on-line на

[1] Про державну реєстрацію актів цивільного стану: Закон України від 01.07.2010 р. Відомості Верховної Ради України. 2010. № 38. Ст. 509 URL: https://zakon.rada.gov.ua/laws/show/2398-17#Text

[2] Ожеван М. А., Гнатюк С. Л., Ісакова Т. О. Інформаційні технології як фактор суспільних перетворень в Україні: зб. аналіт. доп. /за заг. ред. Д. В. Дубова. Київ: НІСД, 2011. 96 с.

веб-порталі у сфері Державної реєстрації актів цивільного стану на сайті: http://dracs.minjust.gov.ua.[1]

Користувач Веб-порталу – будь-яка фізична особа, яка бажає подати до відділу ДРАЦС заяву або звернення, зареєструвалась на Веб-порталі та звертається з питань у сфері державної реєстрації актів цивільного стану або за інформаційно-консультаційною підтримкою.

З використанням цього Веб-порталу громадяни можуть подати до відділів РАЦС такі заяви про: державну реєстрацію шлюбу; державну реєстрацію розірвання шлюбу на підставі рішення суду; розірвання шлюбу подружжя, яке не має дітей; розірвання шлюбу відповідно до ст. 107 СК України; зміну імені; повторну видачу свідоцтв про державну реєстрацію актів цивільного стану; надання витягів з Державного реєстру актів цивільного стану громадян та про внесення змін до актових записів цивільного стану, їх поновлення й анулювання.

Електронна послуга – передача до відділів ДРАЦС заяв користувачів у сфері ДРАЦС з накладенням електронного цифрового підпису (електронний цифровий підпис – вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних відомостей, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача. Електронний цифровий підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа[2]) користувача або звернень з інформацією, необхідною для формування таких заяв, що підписуються під час особистого звернення фізичної особи до відділу, отримання повідомлень про результати їх розгляду.

Особистий кабінет – розділ Веб-порталу, доступ до якого має тільки зареєстрований користувач, що авторизується за допомогою особистих ідентифікаторів доступу до особистого кабінету (логін та пароль), у якому розміщуються інформаційні повідомлення, елек-

[1] Про запровадження пілотного проекту щодо подання заяв у сфері державної реєстрації актів цивільного стану через мережу Інтернет: затв. наказом М-ва юстиції України від 09.07.2015 р. № 1187/5. URL: http://законодавство.com/minyust-ukrajini/nakaz-vid-09072015-1187-pro-zaprovadjennya302198.html

[2] Про електронну ідентифікацію та електронні довірчі послуги: Закон України від 05.10. 2017 р. № 2155-VIII URL: https://zakon.rada.gov.ua/laws/show/2155-19#n534

тронні заяви або звернення, подані до відділу ДРАЦСу, результати їх розгляду та інша інформація.

Технічний адміністратор Веб-порталу – державне підприємство «Інформаційний центр» Міністерства юстиції України, яке здійснює заходи з технічного та технологічного створення та супроводження програмного забезпечення Веб-порталу, забезпечує захист інформації, що міститься на Веб-порталі, від несанкціонованого доступу відповідно до встановлених вимог до захисту оброблюваної в інформаційних системах інформації, надає щоденно відділам державної реєстрації актів цивільного стану відомості щодо проведених за попередній день платежів за заявами (зверненнями) фізичних осіб з використанням платіжних систем (прізвище, ім'я, по батькові платника, сума платежу, дата проведення платежу, призначення платежу, найменування кредитно-фінансової установи, якою проведено платіж, відомості про отримувача коштів); здійснює інші заходи, спрямовані на забезпечення його функціонування.

Увесь складний процес вдалось реалізувати відповідно до розпорядження Кабінету Міністрів України «Про реалізацію пілотного проекту у сфері державної реєстрації актів цивільного стану» від 26.06.2015 року № 669-р, п. 10 Положення про Міністерство юстиції України, затвердженого Постановою Кабінету Міністрів України від 02.07.2014 року № 228, та з метою оптимізації процесу надання адміністративних послуг у сфері державної реєстрації актів цивільного стану і створення сприятливих умов для їх отримання наказом Міністерства юстиції України від 09.07.2015 року № 1187/5.

Відповідно до Порядку роботи веб-порталу «Звернення у сфері державної реєстрації актів цивільного стану», затвердженого наказом Міністерства юстиції України від 09.07.2015 № 1187/5, з використанням функціональних можливостей Веб-порталу користувач може:

1) заповнити заяву, передбачену Правилами державної реєстрації актів цивільного стану в Україні, затвердженими наказом Міністерства юстиції України від 18.10.2000 року № 52/5 , Правилами внесення змін до актових записів цивільного стану, їх поновлення та анулювання, затвердженими наказом Міністерства юстиції України від 12.01.2011 року № 96/5 , Інструкцією з ведення Державного реєстру актів цивільного стану громадян, затвердженою наказом Міністерства юстиції України від 24.07.2008 року № 1269/5 , звернення для

їх подальшого надсилання безпосередньо засобами Веб-порталу до відділів державної реєстрації актів цивільного стану;

2) надіслати до відділів ДРАЦу скан-копії документів, необхідних для державної реєстрації актів цивільного стану, внесення змін до актових записів цивільного стану, їх поновлення та анулювання, у форматі, придатному для роздрукування або зчитування цих документів в електронному вигляді;

3) здійснити попередній запис на відвідування відділу ДРАЦСу із зазначенням зручних дати і часу;

4) оплатити з використанням платіжних систем послуги відділів ДРАЦСу;

5) отримати консультації працівників відділу ДРАЦСу щодо надісланих через Веб-портал заяв або звернень.

Отже, щоб подати заяву на реєстрацію шлюбу онлайн, необхідно виконати всього чотири пункти: зареєструватися на Веб-порталі, вибрати відділення РАЦС, дату, час і тип церемонії, сплатити державне мито за надання послуг та заповнити форму заяви (повні анкетні дані нареченого і нареченої, громадянство). За достовірність відомостей, поданих до відділів державної реєстрації актів цивільного стану через Веб-портал, відповідає користувач.

За результатами розгляду звернення щодо запису на попередній прийом через Веб-портал до особистого кабінету користувача надсилається повідомлення, у якому зазначаються прізвище, ім'я, по батькові, посада та контактний телефон особи, яка буде здійснювати прийом, а також дата і час прийому. Пошук заяв або звернень на Веб-порталі здійснюється за реєстраційним номером. Засобами Веб-порталу надається інформація про перелік необхідних документів та відомостей, а також інформація про необхідність особистого звернення заявника до відповідного відділу державної реєстрації актів цивільного стану. В особистому кабінеті користувача відображається інформація про стан розгляду заяв або звернень, поданих через Веб-портал.

Оплата вартості послуг зв'язку (послуг операторів телефонного зв'язку, Інтернет-провайдерів тощо) та інших послуг, пов'язаних із забезпеченням їхніх технічних можливостей для користування Веб-порталом, здійснюється користувачами на загальних підставах.

Слід звернути увагу, що електронна заява має подаватися з накладенням цифрового підпису. У разі його відсутності, для підпи-

сання заяви на весілля доведеться відвідати обраний вами РАЦС не пізніше 3-х робочих днів з моменту отримання повідомлення про результати розгляду заяви. Це важливо, оскільки місячний строк (хоча зазначений вище пілотний проект дозволяє знизити час очікування укладення шлюбу до декількох годин) до реєстрації шлюбу почне обчислюватися тільки з моменту належного підписання заяви.

Отже, підсумовуючи викладене вище, подання до відділів державної реєстрації актів цивільного стану звернень щодо заяв у сфері ДРАЦС через мережу Інтернет, тобто використовуючи ІТ технології, не звільняє від необхідності особистого звернення користувача до відділу та подання ним документів, передбачених законодавством для укладання шлюбу.

Проте, гібридна війна, що триває з 2014 року, суттєво змінила соціальну та правову реальність в Україні. Зміни у демографічній ситуації, міграційних процесах та доступі до державних послуг вплинули на можливості громадян вступати у шлюб.

На територіях, непідконтрольних українській владі, виник правовий вакуум. Там запроваджувалися нелегітимні норми та процедури, що не визнаються Україною та міжнародною спільнотою. Це створило проблеми з визнанням шлюбів, укладених у цих регіонах, на підконтрольній Україні території.

У відповідь на виклики війни, український уряд запровадив спрощені процедури реєстрації шлюбів для військовослужбовців та ВПО. Це дозволило швидше укладати шлюби в умовах невизначеності та підвищеного ризику.

Україна відреагувала на виклики війни та внесла зміни у законодавство, щоб полегшити процес одруження для військовослужбовців та громадян, які перебувають у небезпечних умовах.

Серед основних законодавчих змін слід відзначити такі:

Постанова Кабінету Міністрів України № 1024 від 2022 року дозволила військовослужбовцям укладати шлюб без фізичної присутності. Військові, які перебувають у зоні бойових дій, можуть реєструвати шлюб через довірену особу або за допомогою відеозв'язку.[1]

[1] Деякі питання державної реєстрації шлюбу в умовах воєнного стану: Постанова Кабінету Міністрів України від 7 березня 2022 р. № 213. URL: https://zakon.rada.gov.ua/laws/show/213-2022-%D0%BF#Text (втрата чинності 30.10.2024)

Пілотний проєкт «Шлюб за добу», запущений ще у 2016 році, цей проєкт набув популярності серед військових і переселенців у зв'язку з війною. Дає змогу зареєструвати шлюб без дотримання стандартного місячного терміну очікування.[1]

Бойові дії змусили багатьох переглянути пріоритети у житті, що призвело до збільшення кількості шлюбів серед військовослужбовців. Одруження може надавати додаткові соціальні гарантії, наприклад, право на отримання виплат у разі загибелі військового.

Війна підвищила рівень стресу та невизначеності, що в деяких випадках стимулює швидке укладення шлюбів. Експерти зазначають, що в умовах війни люди схильні прагнути стабільності у вигляді створення сім'ї.

Гібридна війна створила нові умови для виникнення шлюбних правовідносин в Україні. Вплив війни проявляється у збільшеній кількості шлюбів серед військових, міграційних викликах, спрощених процедурах укладення шлюбу, а також проблемах із визнанням шлюбів, зареєстрованих на окупованих територіях. Український уряд адаптував законодавство до нових умов, що сприяло збереженню інституту шлюбу навіть в умовах триваючої війни.

Отже, підсумовуючи викладене вище, подання до відділів державної реєстрації актів цивільного стану звернень щодо заяв у сфері ДРАЦС через мережу Інтернет, тобто використовуючи ІТ-технології, не звільняє від необхідності особистого звернення користувача до відділу та подання ним документів, передбачених законодавством для укладення шлюбу. Використання ІТ-технологій дійсно полегшує громадянам України забезпечити своє бажання укласти шлюб і створити сім'ю.

Припинення шлюбних правовідносин та ІТ в умовах гібридної війни

Сімейним законодавством передбачено припинення шлюбних відносин, тобто припинення шлюбу. Припинення шлюбу слід розуміти як викликане окремими видами юридичних фактів припинення право-

[1] Шлюб за добу. Центральне міжрегіональне управління Міністерства юстиції України. URL: https://centraljust.gov.ua/dergavna_reestracia_aktiv_civil_stanu/shlyub_za_dobu

відносин між чоловіком і дружиною, тобто припинення виконання подружжям обов'язків, які виникли при укладенні та реєстрації шлюбу[1].

Під припиненням шлюбу слід розуміти припинення в майбутньому правовідносин між подружжям, що виникли із зареєстрованого дійсного шлюбу, викликане певними юридичними фактами. Сутність припинення шлюбу полягає в тому, що внаслідок певних об'єктивних причин (наприклад, смерть одного з подружжя, оголошення одного з подружжя померлим у встановленому законом порядку) або суб'єктивних причин (наприклад, розпад сімейних зв'язків, небажання одного з подружжя перебувати в шлюбних відносинах тощо) існування шлюбу як союзу двох осіб, поєднаних спільністю подружнього життя, припиняється. Інакше кажучи, можна визначити, що припинення шлюбу є припинення в майбутньому правовідносин між подружжям, які виникли із зареєстрованого дійсного шлюбу, викликаних певними юридичними фактами.

У науковій літературі розрізняються два поняття, а саме «визнання шлюбу недійсним» та «припинення шлюбу». Як зазначено в літературі, на думку багатьох учених, вказані поняття розрізняються тим, що при визнанні шлюбу недійсним наслідки шлюбу між чоловіком і дружиною припиняються з моменту укладення між ними шлюбу, а при припиненні шлюбу правові наслідки настають з дня припинення та/чи розірвання шлюбу[2].

Відповідно до положень сімейного законодавства, виділяють низку підстав для припинення шлюбних відносин, тобто розірвання (припинення) шлюбу: у разі смерті та оголошення померлим одного з подружжя (чоловіка чи жінки); у разі розірвання шлюбу за заявою одного чи обох з подружжя.

У разі смерті, загибелі одного з подружжя (чоловіка чи жінки) припиняється його дієздатність і правоздатність. Факт смерті реєструється в органах РАЦС на підставі відповідної довідки з медичної установи.

Військові дії призвели до загибелі багатьох громадян, включаючи військовослужбовців та цивільних. У таких випадках шлюб припиня-

[1] Сімейне право України: підручник. За заг. ред. Т. В. Боднар та О. В. Дзери. К.: Юрінком Інтер, 2016. 520 с.; Сімейний Кодекс України: наук.-практ. Коментар/Станом на 01.01.2025/за заг. ред. Харитонова Є. О., Сафончик О. І. 432 с.

[2] Сімейне право України: підручник. За ред. А. О. Дутко. Львів: Львівський державний університет внутрішніх справ, 2018. 480 с.

ється автоматично зі смертю одного з подружжя. Однак процес офіційного визнання смерті та отримання відповідних документів може бути ускладнений через бойові дії та відсутність доступу до певних територій.

Вимушена розлука подружжя через війну, міграцію або службу в армії могла призвести до зростання кількості розлучень. Відсутність можливості підтримувати сімейні стосунки, психологічний тиск та інші фактори сприяли цьому процесу.

Насамперед, варто зауважити, що правовий режим воєнного стану не є перешкодою для укладення чи розірвання шлюбу. Так, відділи державної реєстрації актів цивільного стану працюють у штатному режимі, окрім тих міст та районів, де ведуться активні бойові дії або які перебувають в окупації. Заяву про реєстрацію шлюбу можна подати через онлайн сервіси Міністерства юстиції, або безпосередньо звернутися до будь-якого відділу ДРАЦС незалежно від місця проживання.

Мешканці окупованих населених пунктів та територій, де тривають бойові дії, наразі не мають можливості подати такі заяви, адже місцеві відділи ДРАЦС не працюють. Якщо ж ваш ДРАЦС не працює, дізнайтеся, чи можете ви подати заяву онлайн або направити її поштою до іншого ДРАЦСу. Це варто уточнити на місці або за телефоном. Зокрема, відповідно до пункту 14 Правил державної реєстрації актів цивільного стану в Україні, затверджених наказом Міністерства юстиції України від 18 жовтня 2000 року № 52/5, та змінам до наказу від 26 лютого 2022 року № 606/5, можуть оформити розлучення у будь-якому працюючому органі ДРАЦС[1].

Шлюб може бути припинений шляхом його розірвання за життя подружжя внаслідок волевиявлення одного з них чи обох (у суді або в органах ДРАЦС). Зазначена підстава припинення шлюбу є найбільш поширеною[2]. Можливість припинення шлюбу на підставі волевиявлення одного чи обох з подружжя є проявом принципу

[1] Про затвердження Правил державної реєстрації актів цивільного стану в Україні: Наказ Міністерства юстиції України № 52/2 від 18.10.2000 р. URL: https://zakon.rada.gov.ua/laws/show/z0719-00#Text; Про внесення змін до деяких нормативно-правових актів у сфері державної реєстрації актів цивільного стану Наказ Міністерства юстиції України № 606/5 від 26.02.2022 р. URL: https://zakon.rada.gov.ua/laws/show/z0255-22#Text

[2] Сімейний кодекс України: наук.-практ. Коментар/Станом на 01.01.2025/за заг. ред. Харитонова Є. О., Сафончик О. І. 432с.

свободи шлюбу і рівності подружжя. Оскільки вступ у шлюб здійснюється вільно і добровільно, ніхто не може бути примушений до зберігання подружніх відносин, якщо їхні засади втрачені. Розірвати можна лише шлюб, укладений у законному порядку, з дотриманням усіх умов і підстав його укладення, тобто тільки дійсний шлюб. Фактичне припинення шлюбу з метою подальшого непоновлення шлюбних відносин з точки зору закону не є розлученням. Тому при фактичному припиненні шлюбних відносин шлюб продовжує породжувати сімейні правовідносини, крім випадків постанови судом рішення про встановлення для подружжя режиму окремого проживання.

Режим окремого проживання може бути встановлений судом за заявою одного з подружжя або їх обох у разі неможливості чи небажання дружини та/чи чоловіка проживати спільно (ст. 119 СК України). Встановлення режиму окремого проживання не припиняє прав і обов'язків подружжя, встановлених СК України, які дружина і чоловік мали до встановлення зазначеного режиму, а також прав і обов'язків, установлених шлюбним договором.

Припинення шлюбу в енциклопедичній літературі розцінюється як припинення особистих і майнових правовідносин подружжя[1]. У теорії сімейного права під припиненням шлюбу слід розуміти обумовлене настанням певних фактів припинення правовідносин, що виникли між подружжям з юридично оформленого шлюбу. До юридичних фактів, що припиняють шлюб, згідно із ст. 104 СК України, належать такі обставини: 1) шлюб припиняється внаслідок смерті одного з подружжя або оголошення його померлим; 2) шлюб припиняється внаслідок його розірвання.

У разі смерті чи оголошенні одного з подружжя померлим, будь-яке спеціальне оформлення припинення шлюбу не потрібно. У таких випадках шлюб уважається припиненим з моменту смерті подружжя або з моменту набрання чинності рішенням суду про оголошення одного з подружжя померлим. Єдиним документом, що підтверджує припинення шлюбу внаслідок смерті одного з подружжя, є свідоцтво про його смерть, що видає орган РАЦС. Порядок і умови оголошення громадянина померлим установлений у ЦК України.

[1] Цивільне процесуальне право України: навчальний посібник. За ред. В. О. Кучера, А. О. Дутко. Львів: Львівський державний університет внутрішніх справ, 2023. С.72

Сімейне законодавство України передбачає, що шлюб може бути припинено шляхом його розірвання, після чого шлюбні правовідносини між чоловіком і жінкою припиняються з відповідними правовими наслідками (поділ спільного майна, аліментні зобов'язання тощо). У літературі в теоретичному і практичному аспектах поняття «розірвання шлюбу» і «розлучення» розглядаються як синоніми (розділ 11 СК України). Так само ці поняття використовуються як синоніми під час вирішення спорів у суді, а також під час реєстрації в органах РАЦС.

Вивченням наукової літератури встановлено, що розірвання шлюбу слід розуміти як припинення шлюбу, тобто юридичний акт, підтверджуючий припинення шлюбних правовідносин між дружиною і чоловіком. Також висвітлюються суб'єктивні й об'єктивні підстави припинення шлюбних правовідносин шляхом розлучення. Об'єктивні підстави припинення шлюбних правовідносин шляхом розлучення закріплені в положеннях ст. 107 СК України. Відповідно до зазначеної статті, до підстав припинення шлюбних правовідносин шляхом розлучення належать: обставини, які залежать від вольових якостей осіб, а також від інтелектуальних якостей осіб, які розлучаються, та водночас і підстави, які не залежать від вищенаведених якостей осіб, котрі припиняють шлюбні правовідносини шляхом розірвання та/чи розлучення.

В юридичній літературі зазначається, що припинення правовідносин між подружжям, зумовлене певними юридичними фактами[1]. Визначаючи правову природу припинення шлюбу, правознавці підкреслюють, що: 1) припинення завжди обумовлено певними юридичними фактами[2]; 2) стосується правовідносин між подружжям, які виникли з дійсного шлюбу[3]; 3) припинення шлюбу пов'язується з втратою чинності шлюбу[4]. Проте з останньою точкою зору не можна

[1] Сімейне право України: підручник. За заг. ред. Т. В. Боднар, О. В. Дзери. Київ: Юрінком Інтер, 2016. С.112

[2] Дзера О. В., Боднар Т. В. Сімейне право України: підручник. Суми: Юрінком Інтер, 2020. С.52.

[3] Цивільне та сімейне право України: підручник /за ред. Є. О. Харитонова, Н. Ю. Голубєвої. Київ: Правова єдність: Всеукр. асоціація видавців, 2009. С.918; Сімейний Кодекс України: наук.-практ. Коментар/Станом на 01.01.2025/за заг. ред. Харитонова Є. О., Сафончик О. І. 432с.

[4] Болховітінова А. Б. Припинення шлюбу за законодавством України: дис. … канд. юрид. наук. Київ, 2009. С. 54.

погодитися, оскільки припинення шлюбу в разі його розірвання відбувається внаслідок вольового рішення певної особи (наприклад, подружжям, рішенням компетентного органу), а не автоматично, адже без стороннього втручання шлюб не може втратити юридичну силу. Зазначене обумовлено тим, що припинення шлюбу поставлено під контроль держави і може здійснюватися тільки відповідними державними органами: державним органом РАЦС або судом у випадках, прямо передбачених СК України[1].

Саме тому припинення шлюбу є юридичним фактом, з яким закон пов'язує певні правові наслідки, які мають важливе значення, адже в разі припинення шлюбу припиняються особисті немайнові та майнові правовідносини подружжя.

Що стосується підстав припинення шлюбу, то перш за все підстави – це те, на чому базується прийняття рішення компетентним органом (державним органом РАЦС, судом) щодо припинення шлюбу.

Стаття 104 СК України встановлює вичерпний перелік підстав для припинення шлюбу. Відповідно до вказаної статті шлюб припиняється за однією з двох підстав унаслідок: 1) смерті одного з подружжя або оголошення його померлим; 2) розірвання шлюбу.

Однак, у сучасності, з розвитком новітніх технологій та толерантного відношення до осіб з порушенням або зміною полової орієнтації, пропонується доповнити перелік підстав такою підставою, як зміна статі одним або обома з подружжя, закріпити на законодавчому рівні автоматичність припинення шлюбу та момент його припинення у разі видачі паспорту громадянина України, в якому визначено іншу стать. З урахуванням цього запропоновано доповнити ст. 104 СК України частиною п'ятою в такій редакції: «5. У разі зміни статі одним або обома з учасників шлюбних правовідносин шлюб припиняється автоматично з дати видачі паспорта громадянина України, в якому визначено іншу стать. Якщо рішення суду про розірвання шлюбу, яке ще не набрало чинності, прийняте до моменту видачі паспорта громадянина України, в якому визначено іншу стать, вважати шлюб припиненим з дати видачі паспорта громадянина України, в якому визначено іншу стать. Реєстрація припинення шлюбу в такому разі здійснюється державним органом реєстрації актів ци-

[1] Сафончик О. І. Правове регулювання припинення шлюбу в Україні: автореф. дис. … канд. юрид. наук. Одеса, 2004. С. 16.

вільного стану одночасно з видачею паспорта громадянина України, в якому визначено іншу стать».

Слід також ураховувати, що поняття «причини припинення шлюбу» і «підстави припинення шлюбу» не є тотожними. Підстави припинення шлюбу передбачає СК України: шлюб припиняється внаслідок смерті одного з подружжя (або оголошення його померлим) або внаслідок розірвання шлюбу. Причини – це ті обставини, завдяки яким подружжя припиняють шлюб. Крім того, у цьому разі правильніше говорити про причини саме розірвання шлюбу. В юридичній літературі виділяють об'єктивні й суб'єктивні причини розлучення. До об'єктивних причин можуть уважатися належними обставини, що не залежать від вольових та інтелектуальних якостей осіб, які розлучаються. До суб'єктивних причин розлучення належать різноманітні обставини, що характеризують, як правило, психологічний склад особистості подружжя. До цих причин належать і інші явища, пов'язані з подружньою зрадою, байдужістю ставлення до дітей, їх виховання, приниженням й образою гідності одного з подружжя та іншими випадками і пороками [1].

Крім того, слід також розмежовувати такі правові категорії, як «припинення шлюбу» і «розірвання шлюбу», адже перша правова категорія є більш широкою і включає в себе розірвання шлюбу, яке відбувається за життя подружжя.

За життя обох з подружжя шлюб може бути припинений шляхом його розірвання (розлучення). Терміни «розірвання шлюбу» і «розлучення» розглядаються в теорії сімейного права і застосовуються в практиці державних органів РАЦС і судів як синоніми. Ці терміни вживаються як синоніми й у законі (Розділ 11 СК України).

Порядок розірвання шлюбу встановлений Розділом 11 СК України. Розірвання шлюбу поставлено під контроль держави і може здійснюватися тільки відповідними державними органами: чи органом РАЦС, чи судом у випадках, прямо передбачених СК України.

Розірвання шлюбу можливо також і в судовому порядку. СК України передбачає, що розірвання шлюбу в судовому порядку можливо за взаємною згодою та за позовом одного з подружжя (ст.ст. 109, 112 СК України відповідно).

[1] Цивільне та сімейне право України: підручник. За ред. Є. О. Харитонова, Н. Ю. Голубєвої. Київ: Правова єдність: Всеукр. асоціація видавців, 2009. С.587

Якщо у справах, що належать до компетенції органів ДРАЦС, зацікавленому чоловікові/дружині з тих чи інших підстав було відмовлено в розлученні або у вирішенні спору по суті, він/вона може скористатися правом на судовий порядок розгляду його/її вимог[1].

Процедура розірвання шлюбу в судовому порядку регламентується цивільним процесуальним законодавством. Норми, що містяться в проекті Цивільного процесуального кодексу України, докладно роз'яснюють права й обов'язки учасників судового процесу, а також саме позовне провадження.

Зважаючи на проведене вище дослідження, враховуючи сьогодення, слід звернути особливу увагу та зупинитись на одній з підстав припинення шлюбу, зокрема внаслідок смерті або оголошення особи померлою, або визнання особи безвісно відсутньою. Таке акцентування уваги саме на цьому аспекті шлюбних відносин – припинення (розірвання) шлюбу внаслідок смерті (оголошення особи померлою, визнання безвісно відсутньою), обумовлено тим, що по всій території України введено в дію воєнний стан, у зв'язку із повномасштабним вторгненням 24 лютого 2022 року на територію України збройних формувань російської федерації, коли більшість громадян України вживають заходів із забезпечення національної безпеки і оборони, відсічі і стримування збройної агресії російської федерації[2].

Так, з наукової точки зору правоздатність і дієздатність людини припиняється з настанням смерті – певного юридичного факту, який підтверджується довідкою лікувального закладу або показаннями свідків. Особа може бути в судовому порядку оголошена померлою в разі, якщо в місці її постійного проживання немає відомостей про місце її перебування впродовж трьох років, а якщо вона пропала безвісти за обставин, що загрожували смертю або давали би підстави вважати її загиблою від нещасного випадку, – впродовж шести місяців. Тут слід виділити тезу про те, що у відповідності до діючого законодавства України – військовослужбовець або інший громадянин, який пропав безвісти у зв'язку з бойовими діями, може бути в судовому порядку оголошений померлим не раніше, як за два роки від дня за-

[1] Дзера О. В., Боднар Т. В. Сімейне право України: підручник. Суми: Юрінком Інтер, 2020. 520 с. С.217.

[2] Про затвердження Указу Президента України «Про введення воєнного стану в Україні: Закон України від 24 лютого 2022 року № 2102-IX. URL: https://zakon.rada.gov.ua/laws/show/2102-20#Text

кінчення бойових дій. Ураховуючи конкретні обставини справи, суд може оголосити фізичну особу померлою і до настання цього строку, але не раніше шести місяців (ст. 46 ЦК України).

Відповідні права й обов'язки в цьому разі виникають або припиняються внаслідок самого факту смерті або оголошення особи померлою, що проводиться відповідно до цивільного законодавства (ст. 46 ЦК України)[1]. Отримання свідоцтва про смерть і є достатнім підтвердженням припинення шлюбу. У разі оголошення особи померлою правовою підставою виникнення юридичних наслідків є відповідне рішення суду щодо оголошення фізичної особи померлою, яке набрало чинності.

У разі припинення шлюбу внаслідок смерті одного з подружжя або оголошення його померлим, припинення шлюбу не потребує спеціального оформлення.

Питання про оголошення особи померлою суд вирішує в порядку окремого провадження за місцем знаходження заявника (Розділ IV ЦПК України) на підставі заяви про визнання фізичної особи безвісти відсутньою або оголошення її померлою, яка подається до суду за місцем проживання заявника, або за останнім відомим місцем проживання (перебування) фізичної особи, місцеперебування якої невідомо, або за місцезнаходженням її майна (ст. 246 ЦПК України). Юридичні наслідки винесеного судом рішення дорівнюються до тих самих наслідків, що настають при смерті особи, тобто є підставою для реєстрації смерті в державних органах РАЦС та видачі свідоцтва про смерть.

Реєстрація припинення шлюбу провадиться відповідно до СК України, а також Правил реєстрації актів цивільного стану в Україні.

У разі появи фізичної особи, яка була оголошена померлою, або виявлення місця її перебування (зокрема враховуючи сьогодення – перебування у полоні країни агресора, або перебування у незаконному утриманні країною агресором, та/або незаконно переміщених громадян с території України на території країни агресора – російської федерації), суд відповідно до ст. 48 ЦК України скасовує рішення про оголошення зазначеної фізичної особи померлою. З моменту винесення судом рішення про оголошення фізичної особи померлою

[1] Цивільний кодекс України: Закон України від 16.01.2003 р. URL: https://zakon.rada.gov.ua/laws/show/435-15#Text

шлюб із нею вважається припиненим, тобто чоловік/дружина зазначеної особи має право на укладення повторного шлюбу, маючи на руках рішення про оголошення фізичної особи померлою.

Слід ураховувати, що той з подружжя, хто був оголошений померлим у разі, якщо насправді він є живим, не має права на укладення нового шлюбу незалежно від того, чи відомо йому про наявність рішення про оголошення його померлим або ні. Інакше такий шлюб може бути визнаний недійсним у порядку, визначеному Главою 5 (ст. ст. 38-47) СК України.

У разі появи фізичної особи, яка була оголошена померлою, постає питання про шлюб, який був припинений у порядку ст. 107 СК України. Стаття 118 СК України передбачає можливість поновлення шлюбу в разі з'явлення особи, яка була оголошена померлою або визнана безвісно відсутньою. Оголошення судом одного з подружжя померлим або визнання його безвісно відсутнім ґрунтується відповідно на презумпції (припущенні) смерті цієї особи чи на констатації факту неможливості вирішення питання про її життя або смерть, внаслідок чого не виключається можливість з'явлення зазначеної особи або виявлення місця її перебування.

У разі з'явлення особи, яка була оголошена померлою, і скасування відповідного рішення суду про визнання її такою, її шлюб з іншою особою поновлюється за умови, що ніхто з них не перебував у повторному шлюбі. Згідно із ст. 45 ЦК України, рішення про визнання особи безвісно відсутньою скасовується в разі її з'явлення або встановлення місця її перебування за заявою цієї особи або іншої заінтересованої особи за правилами ст. 250 ЦПК України.

Основними юридичними наслідками припинення шлюбу є припинення особистих та майнових правовідносин подружжя. Проте смерть одного з подружжя або оголошення його померлим означає абсолютне припинення всіх особистих та майнових правовідносин подружжя (зокрема, відкриття спадщини, визначення частки кожного з подружжя у спільному майні тощо), а при розірванні шлюбу можуть зберігатися де які взаємні права й обов'язки (зокрема, право на одержання аліментів від колишнього чоловіка чи дружини, право на спільне майно тощо).

У заяві про визнання фізичної особи безвісти відсутньою або оголошення її померлою має бути зазначені: мета такого визнання; об-

ставини, які підтверджують безвісну відсутність особи, або що загрози смертю особі, яка зникла безвісти, або припущення загибелі особи від нещасного випадку або в результаті бойових дій.

Відповідно до ст. 249 ЦПК України: «після набрання чинності рішенням про оголошення фізичної особи померлою суд надсилає рішення відповідному органу ДРАЦС для реєстрації смерті фізичної особи, а також до нотаріуса за місцем відкриття спадщини, а в населеному пункті, де немає нотаріуса, – до відповідного органу місцевого самоврядування для вжиття заходів щодо охорони спадкового майна»[1].

Також, відповідно до ЦПК України, «якщо надається заява про появу особи, яку було визнано безвісно відсутньою або оголошено померлою, чи надходить інформація про місцеперебування цієї особи, суд призначає справу до слухання за участю цієї особи, заявника та інших заінтересованих осіб і скасовує рішення про визнання фізичної особи безвісно відсутньою або оголошення її померлою»[2].

Є досить ускладненою ст. 250 ЦПК України, згідно з якою в разі одержання заяви про появу фізичної особи, яка була оголошена померлою, суд призначає справу до слухання за участю цієї особи, заявника та інших осіб і скасовує своє рішення про визнання фізично особи померлою. Немає також необхідності обов'язково бути присутнім у суді як особи, яка була оголошена померлою, так і заявника. Адже для скасування такого рішення необхідний певний час. Тому можлива ситуація, коли особа, з одного боку, має право реалізовувати свої суб'єктивні права й обов'язки, а з іншого – формально оголошена особою, яка померла. Таким чином, можливо вирішити проблему або шляхом зміни судового порядку на адміністративний (ДРАЦС), або в судовому – лише із зазначенням про негайність призначення справ до розгляду та винесення рішення.

Також слід зазначити, що шлюби, укладені або розірвані на окупованих територіях за нелегітимними нормами, не визнаються українською владою. Це створює додаткові правові колізії щодо статусу таких шлюбів та правового становища подружжя.

---

[1] Цивільний процесуальний кодекс України: Закон України від 18.03.2004 р. № 1618-IV. URL: https://zakon.rada.gov.ua/laws/show/1618-15#Text

[2] Цивільний процесуальний кодекс України: Закон України від 18.03.2004 р.№ 1618-IV. URL: https://zakon.rada.gov.ua/laws/show/1618-15#Text

До початку повномасштабної війни питання розірвання шлюбу, якщо один із подружжя перебував на окупованій території, вирішувалося так: один із подружжя приїздив до найближчого населеного пункту на підконтрольній Україні території, оформлював нотаріально засвідчену заяву про розірвання шлюбу для подання в РАЦС, передавав її іншому з подружжя та повертався додому.

Якщо ж розлучення можливе лише у судовому порядку, необхідно визначити відповідний суд для подання позову. Загалом позов подається до суду за зареєстрованим місцем проживання відповідача. Втім, у деяких випадках позов можна подати за власним місцем проживання позивача, зокрема якщо: 1) на утриманні перебувають неповнолітні діти; 2) виїзд до місця проживання відповідача неможливий через стан здоров'я або з інших поважних причин (це необхідно обґрунтувати в позові).

Якщо суд, до якого потрібно звернутися, не здійснює правосуддя через бойові дії або тимчасову окупацію, слід звернутися до переліку судів із зміненою територіальною підсудністю. Цю інформацію можна знайти, зокрема, на сайті Верховного Суду.

Окрему увагу слід приділити питанню адреси сторін. Якщо позивач або відповідач унаслідок війни змінили місце проживання, в позовній заяві необхідно зазначити актуальну адресу та надати підтверджуючі документи, наприклад, довідку про взяття на облік як внутрішньо переміщеної особи. Це важливо для визначення належного суду відповідно до територіальної підсудності справи.

Наразі держава докладає зусиль, щоб забезпечити безперервність життєво важливих процесів, незважаючи на воєнні умови. Реєстрація актів цивільного стану (шлюбу, народження дитини, розлучення, підтвердження факту смерті) повинна здійснюватися за місцем події. Якщо це неможливо через бойові дії або тимчасову окупацію, відповідний орган переноситься до найближчої доступної локації.

Особи, які раніше мали звертатися до ДРАЦСу або суду, що наразі не може виконувати свої функції, подають заяви до найближчого відділу, який тимчасово виконує їхні повноваження. Це дозволяє громадянам продовжувати реєстраційні дії без значних перешкод, навіть в умовах війни.

У разі, якщо один із подружжя знаходиться на тимчасово окупованій території, позивач повинен звернутися до ДРАЦСу або суду, що були перенесені до іншого населеного пункту.

За загальним правилом, позов про розірвання шлюбу подається до суду за місцем проживання відповідача. Однак існують винятки, коли справа може розглядатися за місцем проживання позивача. Це можливо, якщо позивач доведе, що: він не може в'їхати на тимчасово окуповану територію або перебувати там для здійснення юридичних дій; разом із ним проживають неповнолітні діти, і він не може залишити їх для поїздки до місця проживання відповідача.

У таких випадках суд враховує обставини та може розглянути справу за місцем перебування позивача.

Крім того, якщо позивач звернеться до адвоката, той може подати заяву дистанційно через Систему електронного суду. Це дає можливість розгляду справи в онлайн-режимі, без необхідності особистої присутності в суді.

Аналізуючи чинне законодавство України, а також синтезуючи різні підходи до визначення характерних рис припинення шлюбу, слід звернути увагу на необхідність виділення такого порядку припинення шлюбу: 1) залежно від процедурного аспекту – адміністративний, судовий, релігійний (лише для релігійних шлюбів); 2) залежно від волевиявлення – примусовий (судовий), добровільний (за взаємною згодою), випадковий (у разі смерті, в тому числі смерті в результаті бойових дій).

Встановлені характерні риси припинення шлюбу: 1) стосуються виключно дійсного шлюбу; 2) зумовлені певними юридичними фактами; 3) притаманні аспекти публічності; 4) діють на майбутнє; 5) як правило, припиняють існування прав та обов'язків чоловіка і дружини як у сімейних правовідносинах, так і в інших сферах; 6) породжують настання певних правових наслідків майнового і немайнового характеру, які настають як для колишнього подружжя, так і для інших осіб; 7) можливість настання в будь-який момент; 8) як правило, передбачає окреме проживання подружжя на майбутнє.

Історично сімейно-правове регулювання розірвання шлюбу всупереч різним протилежним тенденціям у цьому процесі – від повного вирішення питання розлучення на розсуд подружжя до складної процедури розірвання шлюбу в два етапи з втручанням суду в мотивацію розлучення – зупинилося сьогодні на розмежуванні розірвання шлюбу у спрощеному порядку (за взаємною згодою подружжя за певних обставин), а також зберіганні основного порядку – через суд.

Необхідно відзначити, що для цього стану суспільства це є оптимальним вирішенням проблеми: припущення розірвання шлюбу на свій розсуд при деякому контролі суду, а також визначення тих конкретних випадків, коли такий контроль не потрібний.[1]

Права дітей та ІТ в умовах гібридної війни

За аналізом українського сімейного законодавства, суб'єктами шлюбних правовідносин, так само як і сімейних правовідносин, є особи, що пов'язані відносинами шлюбу, спорідненості, усиновлення чи іншої форми прийняття дітей у сім'ю на виховання.

Коло суб'єктів сімейних правовідносин чітко окреслюється у ст. 2 СК України. Відповідно до зазначеної статті, сімейні правовідносини в залежності від кола суб'єктів неоднозначні й умовно поділяються на три певні категорії.

До першої категорії суб'єктів сімейних правовідносин як вітчизняні, так і зарубіжні науковці-правники вважають належними подружжя, батьків і дітей, усиновлених та всиновлювачів. Між зазначеними суб'єктами створюються майнові, немайнові та особисті відносини, які регулюються СК України.

До другої категорії суб'єктів сімейних правовідносин учені вважають належними діда і бабу, прадіда і прабабу, онуків, правнуків, рідних сестер і братів, а також вітчима і мачуху, пасинка, падчерку.

До третьої категорії суб'єктів сімейних правовідносин учені вважають належними осіб третього або другого ступеня споріднення і бічного споріднення. Водночас, якщо керуватись ч. 3 ст. 2 СК України, можна впевнено зазначити, що вітчизняна правова доктрина в сімейному праві передбачає участь у сімейних правовідносинах і інших членів сім'ї, якими, крім вищезазначеного, є суб'єкти відносин опіки і піклування, а також суб'єкти патронажу над дітьми.

Щодо цивільного партнерства, то в цьому разі доцільно запропонувати розглядати як суб'єктів цих відносин лише фізичних осіб однієї чи різної статі, які проживають разом однією сім'єю з метою набуття відносин, подібних до шлюбних (тобто ведення спільного

[1] Дзера О. В., Боднар Т. В. Сімейне право України: підручник. Суми: Юрінком Інтер, 2020. С.342.

господарства, піклування один про одного, фінансове забезпечення один одного, вступ у інтимні стосунки та навіть, за наявності, виховання дітей).

При цьому слід ураховувати, що існування шлюбних відносин, а також їх припинення може породжувати різні правові наслідки майнового та немайнового характеру як для суб'єктів шлюбних правовідносин, так і для інших осіб (наприклад, дітей, батьків тощо).

За загальним визначенням, об'єктом шлюбних правовідносин є: встановлення умов і порядку укладення шлюбу, припинення шлюбу, визнання шлюбу недійсним; регулювання особистих немайнових та майнових відносин між членами сім'ї, подружжям, батьками і дітьми, а також між іншими родичами та іншими особами (у випадках і в межах, установлених нормами сімейного права); визначення форми і порядку всиновлення та влаштування в сім'ю дітей, які залишилися без піклування батьків.

На сьогодні існує велика кількість класифікацій шлюбних відносин і правовідносин і кожна класифікація не має єдності та завжди розкриває велику кількість зазначених відносин, особливо в разі, коли правовідносини між чоловіком і жінкою, між батьками та дітьми і між іншими членами сім'ї перебувають на межі шлюбних та сімейних правовідносин.

Шлюб як союз чоловіка і жінки, що має соціальне значення, визначає правове становище дітей, народжених у цьому союзі, майнові відносини між подружжям та їхні спадкові права. Щодо цих прав шлюб є юридичним фактом, однак укладення такого союзу залежить від волі майбутнього подружжя і є юридичним правочином[1].

Однією з ключових цілей сімейного законодавства, визначеною статтею 3 Сімейного кодексу України, є забезпечення кожній дитині умов для виховання в сім'ї, а також створення передумов для її духовного та фізичного розвитку[2]. Держава, у свою чергу, гарантує пріоритетність саме сімейного виховання дітей, що закріплено у статті 5 СК України. Це зумовлено відсутністю у дітей достатнього соціального досвіду, що обумовлює необхідність саме сімейного середовища для всебічного фізичного, морального, інтелектуального та

[1] Шимон С. І. Майнові права як об'єкти цивільних правовідносин (теоретичні та практичні аспекти): автореф. дис.... д-ра юрид. наук. Київ, 2014. С. 25.

[2] Сімейний Кодекс України: наук.-практ. Коментар/Станом на 01.01.2025/за заг. ред. Харитонова Є. О., Сафончик О. І. 432с.

соціального розвитку особистості. Таке виховання сприяє інтеграції дитини в соціум і формує базу для набуття нею первинного соціального досвіду.

Процес виховання дитини в юридичній площині трактується як цілісна система заходів, спрямованих на формування гармонійно розвиненої особистості. У зв'язку з цим на батьків покладається не лише обов'язок щодо забезпечення життєвих потреб дитини, але й моральна підтримка, виховання впевненості в собі, соціалізація через участь у суспільному житті[1].

Попри відносну новизну активного правового захисту прав дитини в Україні, варто зазначити, що питання правового статусу дитини мають історичне підґрунтя, яке сягає глибокої давнини. Традиційно захист дітей сприймався як продовження роду, а батьківська турбота завжди визнавалася пріоритетною. Проте, незважаючи на стійкість цих уявлень, лише сучасне сімейне право надало цим відносинам необхідної юридичної форми.

Відповідно до положень чинного сімейного законодавства, батьки визнаються рівноправними суб'єктами правовідносин, що володіють як особистими немайновими правами, так і обов'язками щодо своїх дітей. До основних прав батьків належать: право на виховання дитини; право на підтримання спілкування з дитиною; право на захист дитини; право на визначення місця її проживання; право на витребування малолітньої дитини у сторонніх осіб.

Серед основних обов'язків батьків визначаються такі: обов'язок забрати дитину з пологового будинку або іншого медичного закладу; обов'язок зареєструвати народження дитини у відповідному органі державної реєстрації актів цивільного стану; обов'язок сприяти вихованню і розвитку дитини.

З іншого боку, у системі правовідносин між батьками і дітьми дитина також виступає як повноцінний суб'єкт сімейного права. Одним із ключових її прав є право на належне батьківське виховання. Це право вважається визначальним для майбутнього соціального та правового становища дитини в суспільстві.

Сімейне законодавство України, розширюючи предмет свого регулювання, забезпечує детальне правове врегулювання як особистих,

[1] Сімейне право України: підручн. За ред. Є. О. Харитонова. Н. Ю. Голубєвої. К.: Істина, 2010. С. 129.

так і майнових сімейних відносин. Воно охоплює не лише відносини між подружжям, батьками і дітьми, усиновлювачами та усиновленими, а й регулює зв'язки між іншими членами родини – дідами, бабусями, прадідами, прабабусями, братами і сестрами, а також мачухами, вітчимами та пасинками, падчерками тощо.

Законодавець також передбачає можливість урахування судом місцевих звичаїв і традицій національних меншин під час вирішення сімейних спорів, за умови їх відповідності чинному законодавству та моральним принципам суспільства.

Визначальним орієнтиром у регулюванні сімейних правовідносин є забезпечення найкращих інтересів дитини, що прямо передбачено положеннями Сімейного кодексу України[1].

У контексті забезпечення реалізації основоположних прав дитини, зокрема права на життя та здоров'я, законодавством України встановлено безумовну заборону на вчинення будь-яких актів насильства щодо дитини, а також на її експлуатацію. Зазначені дії кваліфікуються як правопорушення і тягнуть за собою відповідальність згідно з чинним законодавством. Крім того, на державу покладено обов'язок щодо утримання, виховання та соціального забезпечення дітей-сиріт і дітей, позбавлених батьківського піклування, що є проявом реалізації їх соціальних прав.

Українська держава також сприяє і підтримує діяльність благодійних організацій, спрямовану на надання допомоги дітям. Особливу увагу приділено освітнім правам дітей, що закріплено в Конституції України. Відповідно до статті 53 Основного Закону, повна загальна середня освіта є обов'язковою, а її доступність і безоплатність гарантується державою.

Організаційне забезпечення реалізації прав і свобод дитини здійснюється через систему державних органів, компетенція яких визначена Конституцією України. Зокрема, згідно зі статтею 102, Президент України виступає гарантом прав і свобод людини і громадянина, включаючи права дитини. Координаційні функції у цій сфері також покладено на Кабінет Міністрів України (пункт 2 статті 116), місцеві державні адміністрації (пункт 2 статті 119), органи прокуратури (стаття 121), Конституційний Суд України,

[1] Толкачова Г. В. Еволюція правового забезпечення гарантій захисту прав і свобод дитини. *Часопис Київського університету права.* 2014. № 1. С. 72-76.

суди загальної юрисдикції, органи місцевого самоврядування та інші інституції.

З метою створення умов для всебічного розвитку дитини, реалізації її потенціалу в безпечному середовищі сім'ї або в умовах опіки, а також для підготовки до самостійного життя в демократичному суспільстві, на державному рівні ухвалено низку нормативно-правових актів, які закріплюють систему гарантій прав дитини.[1]

Стрімке розширення цифрових технологій призвело до формування безпрецедентного спектра можливостей для дітей та молоді у сферах комунікації, соціальної інтеграції, освіти, обміну інформацією та доступу до знань. Цифрове середовище також відкриває нові канали для вираження особистих поглядів і позицій щодо суспільно значущих питань, що безпосередньо стосуються життя дітей та функціонування їхніх спільнот. Водночас така доступність цифрових послуг спричиняє нові, складні загрози, що порушують безпеку дитини як у віртуальному, так і в реальному середовищі.

Сучасне покоління дітей дедалі частіше стає об'єктом ризиків, серед яких порушення права на приватність, кібербулінг, доступ до жорстокого чи неприйнятного за віком контенту, кіберзлочинність, цифровий грумінг, сексуальна експлуатація та насильство. Масштаб загроз постійно зростає, а діяльність правопорушників ускладнюється через їх транснаціональний характер, а також через використання сучасних цифрових засобів, що ускладнюють ідентифікацію злочинців і притягнення їх до відповідальності.

Технологічний прогрес, зокрема створення інтерактивних платформ, стрімінгових сервісів, криптовалют, даркнету та програм сталого шифрування, активно використовується злочинцями. При цьому відсутність скоординованої та рішучої реакції з боку приватного сектора цифрової індустрії лише посилює масштаб і наслідки загроз для дитячої аудиторії.

У відповідь на зазначені виклики окремі технологічні рішення, зокрема впровадження бази даних Інтерполу щодо сексуальних зловживань над дітьми, що використовує штучний інтелект і алгоритми для аналізу та порівняння візуальних матеріалів, дозволяють швидко ідентифікувати зв'язки між постраждалими, правопорушниками та

[1] Толкачова Г. В. Еволюція правового забезпечення гарантій захисту прав і свобод дитини. *Часопис Київського університету права.* 2014. № 1. С. 72-76.

їхнім місцезнаходженням. Втім, самих лише технологічних інструментів недостатньо для ефективного подолання проблеми.

З огляду на необхідність одночасного забезпечення доступу до переваг цифрової революції та мінімізації пов'язаних з нею ризиків, актуальним постає формування комплексного, міжсекторального підходу до захисту дітей. Вирішення цього завдання вимагає тісної співпраці державних органів влади, інститутів громадянського суспільства, місцевих громад, міжнародних організацій та представників технологічної індустрії.

Ще у 2018 році, усвідомлюючи складність ситуації, держави-члени Міжнародного союзу електрозв'язку (МСЕ) ініціювали розробку оновлених Керівних настанов із захисту дитини в цифровому середовищі. Нові рекомендації було переглянуто й актуалізовано відповідно до суттєвих трансформацій цифрового ландшафту, в якому живе сучасне покоління. Особливої уваги в оновленому документі надано інклюзивному підходу, зокрема потребам дітей з інвалідністю, для яких цифрові інструменти відкривають нові можливості для повноцінної участі в соціальному, освітньому та культурному житті.

У сучасному світі окреслення межі між безпечним, доцільним і надмірним використанням цифрових технологій залишається складним завданням. Використання електронних пристроїв стало невід'ємною частиною повсякденного життя підлітків, однак дедалі частіше виникають занепокоєння щодо потенційної шкоди, яку може спричинити така «технологічна залученість», зокрема в контексті психічного здоров'я молоді. У цьому аспекті особливої актуальності набуває теза про ймовірність формування психологічної залежності та її наслідків.

Згідно з дослідженнями американських психологів, надмірне екранне навантаження може сприяти виникненню емоційної апатії, порушенням настрою, зростанню рівня тривожності та агресивності серед підлітків. Окрім того, воно асоціюється з труднощами у розвитку когнітивних здібностей – зниженням концентрації уваги, уповільненням темпів когнітивного дозрівання, обмеженням розвитку логічного мислення, уяви та креативності. Значною проблемою постає і зниження якості живого міжособистісного спілкування, що ускладнює процес соціалізації.

Попри це, повна відмова від цифрових технологій у сучасному світі є не лише недоцільною, а й нереалістичною. Вони можуть слугувати інструментом розвитку, однак потребують виваженого та контрольованого застосування. У зв'язку з цим зростає роль батьківського нагляду, а також своєчасного залучення фахівців у разі виявлення тривожних змін у поведінці дитини.

Додатковим чинником психоемоційного навантаження для українських дітей є воєнний контекст. Вторгнення в зону їхнього дитинства війни, до якої вони не були підготовлені, зумовлює зростання загального рівня тривожності, невизначеності та страху. Постійне перебування в напрузі, неможливість передбачити майбутнє, провокують появу емоційних зривів, істеричних реакцій, порушень поведінки (агресії, непослуху, конфліктів із однолітками). Обмеження соціалізації, зокрема внаслідок дистанційного навчання, лише поглиблює ці проблеми.

Окрему загрозу становить надмірне споживання медіа-контенту. Йдеться не лише про зміст інформації, а й про її обсяг. Особливу небезпеку становлять соціальні мережі, де не існує редакційного контролю, характерного для традиційних ЗМІ. Наявність у стрічках новин жорстоких зображень сприяє формуванню так званого «циклу страждання»: підвищена тривожність стимулює подальше занурення в потік новин, що, своєю чергою, лише посилює деструктивні емоції.

Уникнути повністю травматичного контенту в умовах війни практично неможливо, адже знання про безпекову ситуацію у регіоні є критично важливим для збереження життя та здоров'я. У цьому контексті важливим є пошук та застосування ресурсів психологічної підтримки. Експерти Всесвітньої організації охорони здоров'я рекомендують постраждалим від травматичних подій звертатися до системи соціальної підтримки – як до психологів, так і до членів релігійних або громадських спільнот. Адекватна терапевтична допомога дозволяє не лише пережити травму, а й сприяє відновленню психоемоційної рівноваги.

У контексті гібридної війни, яку веде Російська Федерація проти України, дедалі частіше фіксується використання сучасних інформаційних технологій як у межах інформаційно-психологічних операцій (ІПСО), так і з метою вербування цивільних осіб для здійснення протиправної діяльності. Особливу тривогу викликає залучення до

таких дій неповнолітніх осіб, які внаслідок вікових особливостей виявляються особливо вразливою цільовою аудиторією.

Так, в одному з останніх задокументованих випадків в Одесі правоохоронці виявили групу підлітків віком 13 та 16 років, які підпалили автомобілі, що належали військовослужбовцям Збройних сил України. Затримання відбулося під час спроби вчинення чергового підпалу[1]. Слідством установлено, що діти діяли на замовлення представників російських спецслужб, які пропонували грошову винагороду за виконання деструктивних дій.

Наймолодшого з підозрюваних передано під нагляд батьків, тоді як інші неповнолітні учасники отримали запобіжні заходи у вигляді тримання під вартою. Залежно від віку правопорушників і тяжкості правопорушення, законодавство України передбачає як адміністративну, так і кримінальну відповідальність. Згідно з чинним законодавством, адміністративна відповідальність настає з 16 років, а кримінальна – також з 16, але в окремих випадках (зокрема, за тяжкі злочини) – з 14 років.[2]

Вербування неповнолітніх, як правило, відбувається через соціальні мережі, де ворог використовує методи психологічного впливу та маніпуляції. Підлітки, які перебувають у процесі психоемоційної сепарації від дорослих, шукають самостійності, самореалізації та визнання, стають особливо сприйнятливими до пропозицій, що передбачають швидке досягнення цінностей – у тому числі матеріальних.

Ключову роль у формуванні стійкості до таких впливів відіграють критичне мислення, правова обізнаність, рівень інформаційної грамотності та підтримка в родинному середовищі. Саме тому важливим є впровадження комплексних освітньо-просвітницьких програм, спрямованих на розвиток цифрової компетентності дітей та їх здатності ідентифікувати фейкову інформацію, розпізнавати маніпулятивний контент і вчасно звертатися по допомогу.

Із метою виявлення деструктивних інтернет-ресурсів, що використовуються ворогом для впливу на громадян України, зокрема дітей, в Україні діє проєкт «Кібер брама»[3]. Його ресурси спрямовані на боротьбу з інформаційними загрозами та підвищення рівня цифрової

[1] Одеська районна військова адміністрація. Офіційний сайт. URL: https://odrda.od.gov.ua/

[2] Головне Управління поліції в Одеській області. Офіційний вебпортал. URL: https://od.npu.gov.ua/

[3] Про національний проєкт «Кібер Брама». URL: https://stopfraud.gov.ua/about-the-project

безпеки шляхом надання рекомендацій щодо розпізнавання фейкових новин, бот-мереж і шахрайських схем у мережі Інтернет.

Воєнний стан, зумовлений збройною агресією російської федерації проти України, справив винятково згубний вплив на реалізацію прав дітей, які є однією з найбільш вразливих соціальних груп. У зазначених умовах особливо загострюється проблема реалізації батьківських прав і обов'язків, яка проявляється полярно: з одного боку, спостерігається активна участь батьків у захисті фізичного та психоемоційного добробуту дитини, з іншого – мають місце численні випадки сімейної дезінтеграції, зумовленої деструктивним впливом війни.

Варто наголосити, що навіть у разі відсутності у дитини фізичних ушкоджень, експлуатації чи проявів жорстокого поводження, може мати місце порушення її основоположних прав, гарантованих Конституцією України та міжнародними актами. Стан психоемоційної нестабільності, втрата почуття безпеки, розрив із соціальним середовищем, відсутність належного доступу до освіти – усе це є маркерами системної кризи реалізації прав дітей у сучасних умовах.

Аналізуючи правову площину питання, слід визнати, що перші прояви агресії російської федерації проти України – анексія Криму та початок збройного конфлікту на Донбасі у 2014 році – застали державу без належної нормативної бази щодо захисту прав дітей у ситуації збройного конфлікту. Фахівці в галузі міжнародного та національного права справедливо звертали увагу на необхідність приведення внутрішнього законодавства України у відповідність до міжнародних стандартів, зокрема: ратифікації Римського статуту Міжнародного кримінального суду (із внесенням відповідних змін до ст. 124 Конституції України), законодавчого закріплення заборони на використання неповнолітніх у збройних формуваннях, адаптації Закону України «Про охорону дитинства» до вимог міжнародного права.

З часу початку повномасштабної агресії в лютому 2022 року, Україна досягла значного прогресу у вдосконаленні нормативно-правового забезпечення захисту прав дитини. Одним із ключових кроків у цьому напрямі стало ухвалення постанови Кабінету Міністрів України від 17 березня 2022 року № 302 «Про утворення Координаційного штабу з питань захисту прав дитини в умовах воєнного стану». Даний Штаб є тимчасовим консультативно-дорадчим органом

при уряді, покликаним забезпечити ефективну взаємодію органів державної влади всіх рівнів з питань захисту дітей.

Основними функціями Координаційного штабу є організація та супровід процесів евакуації дітей, у тому числі дітей з інвалідністю, сиріт та дітей, позбавлених батьківського піклування, з небезпечних територій; забезпечення їх безпечного розміщення, обліку та повернення після завершення бойових дій; розробка механізмів подолання проблем у сфері захисту прав дітей та інформування громадськості й міжнародної спільноти про ситуацію.

Ще одним інноваційним кроком стало запровадження загальнонаціональної програми «Дитина не сама», реалізованої Офісом Президента України спільно з UNICEF Ukraine та Міністерством соціальної політики. Програму втілено у форматі чат-бота, що виконує функцію консультаційно-інформаційного ресурсу з питань тимчасового прихистку, розшуку дітей, які залишилися без нагляду, та загального правового захисту неповнолітніх у воєнний час.

Чат-бот містить інформацію про правові основи захисту дітей, контакти відповідних служб, інструкції для родичів, опікунів, психологів та журналістів щодо роботи з дітьми, які зазнали травми. Крім того, надається можливість подати заявку на тимчасовий прихисток дитини, після чого відбувається перевірка умов та видача дозволу відповідно до встановленої процедури. За час дії програми вже подано понад 18 000 відповідних заявок, і їхня кількість продовжує зростати.[1]

Таким чином, попри складність обставин, Україна демонструє стійку динаміку розвитку у сфері забезпечення прав дитини, вдосконалення нормативної бази та запровадження дієвих механізмів реагування. Разом з тим, належний захист найменших громадян потребує подальшого комплексного підходу та залучення всіх гілок влади й громадянського суспільства, адже діти – це не лише найуразливіша, але й найцінніша частина національного надбання.

Ключові слова: цивільне право, цивільне законодавство, цивільні правовідносини, сімейне право, сімейне законодавство, сімейні правовідносини, ІТ-право, інформаційні технології, інформаційне суспільство, цифрова доба, гібридна війна, воєнний стан

[1] Захист прав дитини в умовах воєнного стану (опубліковано 02 вересня 2024 року). URL: https://rrda.rv.gov.ua/news/

Розділ 20

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЕЛЕКТРОННОГО СУДОЧИНСТВА В УМОВАХ ГІБРИДНОЇ ВІЙНИ В УКРАЇНІ

DOI

Крістіна Дрогозюк
кандидатка юридичних наук, доцентка

Вступ

Створення єдиного інформаційного простору, в межах якого відбувається накопичення, зберігання, дослідження та обмін даними, обумовило необхідність забезпечення інформаційної безпеки в усіх сферах суспільної та державної діяльності, зокрема, в сфері здійснення правосуддя.

В умовах сучасної трансформації суспільства, пов'язаної з масовим використанням інформаційних технологій, держава може розраховувати на лідерство у військовій, політичній, економічній та інших сферах, мати стратегічну і тактичну перевагу, гнучкіше регулювати економічні витрати на розвиток озброєнь і військової техніки, лише за умови наявності переваги в засобах забезпечення інформаційної боротьби[1].

Відповідно до ч.2 ст. 26 Закону України «Про правовий режим воєнного стану», в умовах воєнного стану скорочення або прискорення будь-якої форми судочинства заборонено. Попри відповідні положення законодавства, судова гілка влади все ж зазнала значного впливу війни та її наслідків, що внесло певні зміни у процес здійснення судочинства[2].

---

[1] Шульга В. І. Сучасні підходи до трактування поняття інформаційна безпека. Ефективна економіка. 2015. № 4. URL: http:// http://www.economy.nayka.com. ua/ ?op=1&z=5514.

[2] Притуляк В. М. Підсистема електронний суд: особливості її функціонування в умовах воєнного стану. *Цивільне судочинство та виконавче провадження в умовах воєнного стану*: матеріали всеукр. наук.-практ. конф. ім. Ю. С. Червоного (Одеса, 16 грудня 2022 р.). Одеса. Фенікс. 2022. С. 62

Зокрема, однією зі стратегій ведення гібридної війни з боку Росії є застосування кібератак, направлених на українські державні реєстри, сервіси та системи, зокрема, і на «Електронний суд», який є підсистемою Єдиної судової інформаційно-телекомунікаційної системи (далі – ЄСІТС). Зокрема, у 2022 році хакерами була заблокована робота Єдиного державного реєстру судових рішень, електронного суду, веб-порталу «Судова влада України» та інш. Певний проміжок часу після цієї кібератаки, спостерігалися проблеми з веб-програмою «Бронювання систем відеоконференцзв'язку» з іншими судами, що позбавляє можливості проведення судових засідань в режимі відеоконференції[1].

19 грудня 2024 року відбулася одна з найбільших зовнішніх кібератак на державні реєстри України. У зв'язку з цим Державне підприємство «Інформаційні судові системи» повідомило про введення певних обмежень в роботі Електронного кабінету підсистеми «Електронного суду». Зокрема, було обмежено можливість реєстрації нового кабінету юридичної особи, надання доступу новому керівнику юридичної особи до кабінету, подання електронного виконавчого документа на виконання до Автоматизованої системи виконавчих проваджень тощо[2].

Неможливість здійснення правосуддя підтверджується судовими рішеннями з посиланням на відповідні кібератаки. До прикладу, в ухвалі Господарського суду Кіровоградської області від 16.03.2023 у справі № 912/238/23 суд зазначив: «16.03.2023 близько 10:30 год із оголошення на офіційній сторінці ДП «ІСС» в соцмережі «Facebook» було з'ясовано про кібератаку на систему електронної пошти судової системи. У зв'язку із цією інформацією та з метою убезпечення АСДС від кібератаки, керівництвом суду було прийнято рішення про тимчасове відключення мережі суду від Інтернетзв'язку (Укртелеком)[3]. З огляду на вказане, в Господарському суді Кіровоградської області

[1] Ковальчук А., Чернявська Б. Забезпечення безпеки електронних даних у господарському судочинстві: правові та організаційні аспекти. *Право та державне управління.* 2023. вип. 2. С. 267

[2] Через атаку на державні реєстри у Електронному суді ввели низку обмежень. *Судово-юридична газета.* 20.12.2024. URL: https://sud.ua/uk/news/sud-info/318692-iz-za-ataki-na-gosudarstvennye-reestry-v-elektronnom-sude-vveli-ryad-ogranicheniy.

[3] Ковальчук А., Чернявська Б. Забезпечення безпеки електронних даних у господарському судочинстві: правові та організаційні аспекти. *Право та державне управління.* 2023. Вип. 2. С. 268.

станом на 16.03.2023 з 10:30 год відсутній зв'язок з мережею Інтернет, не працює офіційна електронна пошта суду, захищена система ВКЗ, підсистема «Електронний суд», що в свою чергу призвело до збоїв у роботі суду, зокрема проведення судових засідань в режимі відеоконференції, доступу до державних реєстрів, підписання електронним підписом електронних примірників судових рішень та направлення їх до ЄДРСР тощо»[1].

З урахуванням вищезазначеного, в умовах дії воєнного стану гостро постає питання забезпечення інформаційної безпеки під час здійснення правосуддя, що викликає нові завдання та покладає додаткову відповідальність на суддів під час розгляду та вирішення судових спорів, зокрема, через систему «Електронного суду». З отриманням беззаперечно прогресивних можливостей участі в судовому засіданні в режимі відеоконференції та дистанційного доступу до судових матеріалів виникає безліч викликів, серед яких, питання забезпечення конфіденційності, захисту персональних даних громадян тощо.

Відповідні загрози обумовлюють необхідність дослідження та розроблення пропозицій щодо удосконалення механізму забезпечення інформаційної безпеки під час здійснення судочинства, як під час повномасштабного вторгнення, так і у мирні часи. В контексті даного питання окремої уваги заслуговує робота підсистеми «Електронного суду», функціонування якої надає громадянам можливість отримати повноцінний доступ до захисту своїх прав та інтересів навіть у період дії воєнного стану[2].

Питанню правового забезпечення функціонування електронного судочинства присвячували свої наукові роботи такі вчені, як: А. Барікова, О. Бринцев, М. Гетманцев, Ю. Георгієвський, Н. Голубєва, С. Чванкін, Б. Чернявська, А. Ковальчук, С. Обрусна, І. Ізарова, Є. Петров та інші.

В Законі України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» від 09.01.2007 р. № 537-

[1] Ухвала Верховного Суду у справі No906/908/21. URL: https://reyestr.court.gov.ua/Review/109645641.

[2] Притуляк В. М. Підсистема електронний суд: особливості її функціонування в умовах воєнного стану. *Цивільне судочинство та виконавче провадження в умовах воєнного стану*: матеріали всеукр. наук.-практ. конф. ім. Ю. С. Червоного (Одеса, 16 грудня 2022 р.). Одеса: Фенікс, 2022. С. 62.

V було вперше було зроблено законодавче закріплення терміну «інформаційна безпека». А саме, відповідне поняття розкривається в законі як «стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; небажані наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації»[1].

Бакалінська О. зазначає, що інформаційна безпека передбачає захист інформації від випадкових чи навмисних несанкціонованих дій, направлених на порушення конфіденційності, цілісності чи доступності певних даних[2].

Як зазначалось вище, в умовах сьогодення інформаційна безпека посідає перше місце в системі національної безпеки кожної держави, що підтверджується ч.1 ст. 17 Конституції України, яка закріплює, що забезпечення інформаційної безпеки України є однією із важливіших функцій держави та справою всього Українського народу.

Правова основа інформаційної безпеки України складається з міжнародних зобов'язань та національного законодавства. На міжнародному рівні слід згадати Будапештську конвенцію та Директиву щодо мережевої й інформаційної безпеки (NIS) (з англ.: «*Network and Information Security Directive*»). На національному рівні основними документами, що регулюють сферу інформаційної безпеки є Закон України № 2163-VIII від 05.10.2017 р. «Про основні засади забезпечення кібербезпеки України» та Національна стратегія кібербезпеки України.

Будапештська конвенція, яка була ратифіковна Україною у 2005 році, являє собою єдиний юридично обов'язковий міжнародний документ з кібербезпеки, який встановлює спільну кримінальну політику щодо захисту від кіберзлочинності шляхом прийняття відповідного внутрішнього законодавства та сприяння міжнародному співробітництву.

У 2016 році Європейський парламент ухвалив «Директиву щодо мережевої й інформаційної безпеки» (NIS), яка встановлює єдині пра-

[1] Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки: Закон України від 9.01.2007 р. № 537-V. *ВВР України.* 2007. № 12. Ст. 102.

[2] Бакалінська О. Правове забезпечення кіберзахисту в Україні Координата. 2020. URL: https://coordynata.com.ua/pravove-zabezpecenna-kiberzahistu-v-ukraini

вила та вимоги для всіх країн ЄС у галузі кібербезпеки. Наразі Україна частково виконала відповідні вимоги і продовжує роботу в цьому напрямку.

Стаття 1 Закону України «Про основні засади забезпечення кібербезпеки України» визначає кібербезпеку, як захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України в кіберпросторі.

Вагомим кроком для удосконалення системи кібербезпеки України стало прийняття Постанови Кабінету Міністрів України № 518 від 19.06.2019 р. «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури», яким встановлено: визначення загальних вимог щодо кіберзахисту об'єктів критичної інфраструктури; визначення обов'язкових заходів забезпечення захисту від кібератак; запобігання порушенню конфіденційності, цілісності та доступності інформаційних ресурсів тощо.

Відповідно до Концепції побудови ЄСІТС, затвердженої Наказом ДСА України від 07.11.2019 р. № 1096, основним принципом побудови ЄСІТС є гібридна розподілена хмарна технологія, яка передбачає розмежування інформаційних середовищ ЄСІТС на відкрите, підключене до мережі Інтернет, і захищене, де обробляється інформація з обмеженим доступом. В Концепції ЄСІТС зазначається, що такі середовища є фізично розділеними, але побудовані за єдиними стандартами та технологіями, що забезпечують достатній рівень інформаційної безпеки.

Для забезпечення належного рівня інформаційної безпеки у складі ЄСІТС має бути передбачено створення захищеного інформаційного середовища та обмін інформацією з обмеженим доступом між судами, учасниками справи та іншими державними органами й установами системи правосуддя виключно через захищене середовище та захищену телекомунікаційну мережу.

Компоненти ЄСІТС мають функціонувати у складі захищеного та відкритого середовища. У захищеному середовищі, фізично відокремленому від мережі Інтернет та інших незахищених мереж, цир-

кулює інформація з обмеженим доступом (персональні дані, слідча таємниця, медична таємниця, сімейна таємниця, банківська таємниця, службова інформація тощо). Відкрите середовище ЄСІТС містить лише публічно доступні дані, в тому числі знеособлену інформацію. Доступ віддалених користувачів, у тому числі учасників судового процесу, здійснюється у відкрите середовище ЄСІТС. Подання та отримання даних, у тому числі документів судових справ у електронному вигляді, повідомлень про надходження/зміну документів тощо, здійснюється через захищений шлюз інформаційної взаємодії, який забезпечує фізичне розмежування захищеного та відкритого середовищ ЄСІТС і унеможливлює будь-які зовнішні втручання до компонентів ЄСІТС, що функціонують у захищеному середовищі ЄСІТС[1].

За своєю сутністю ЄСІТС, як комплексна уніфікована програма, надала можливість перенести більшість операцій пов'язаних зі здійсненням правосуддя, в електронну форму, автоматизувати деякі аналітичні, моніторингові, статистичні та інші операції[2].

З початку повномасштабної війни електронне судочинство деяких важливих змін, які стосуються як технічної, так і законодавної частини щодо його застосування. Так, наприклад, на думку Притуляка В. найбільш корисним нововведенням є інтеграція сервісу «Дія.Підпис» з підсистемою «Електронний суд», що дозволило значно швидше і легше підписувати і направляти документи одразу з підсистеми безпосередньо до суду, не використовуючи електронну пошту або інші додатки, які були раніше необхідні для підписання документів за допомогою КЕП[3].

Окрім того, підсистема «Електронного суду» отримала функціонал відеоконферецзв'язку. Отже, відтепер не потрібно використовувати інші програмні додатки, адже після авторизації в «Електронному суді» учасники справи можуть взяти участь у судовому засі-

[1] Про погодження Концепції побудови Єдиної судової інформаційно-телекомунікаційної системи: рішення Рада суддів України від 22.11.2019 No 97. URL: https://zakon.rada.gov.ua/rada/show/v0097414- 19#Text

[2] Берназюк О. Єдина судова інформаційно-телекомунікаційна система: поняття та структура. *Підприємництво, господарство і право.* 2019. № 6. С. 329. https://doi.org/10.32849/2663- 5313/2019.6.61

[3] Притуляк В. М. Підсистема електронний суд: особливості її функціонування в умовах воєнного стану. *Цивільне судочинство та виконавче провадження в умовах воєнного стану:* матеріали всеукр. наук.-практ. конф. ім. Ю. С. Червоного (Одеса, 16 грудня 2022 р.). Одеса. Фенікс. 2022. С. 63.

данні онлайн, що значного полегшує доступ до правосуддя, зокрема, громадянам, які знаходяться закордоном або не мають можливості брати участь без у судовому процесі безпосередньо в залі судового засідання з інших причин. Використання відеоконференції дозволяє забезпечити присутність сторін, свідків, перекладачів та інших учасників судового процесу, навіть якщо вони не можуть фізично перебувати в судовій залі або в умовах, коли їх участь є неможливою через потенційну загрозу їх життю, зокрема і під час воєнного стану.

Окрім зазначеного під час дії воєнного стану електронне судочинство дозволяє: отримувати повідомлення про надходження до кабінету нових документів та про зміну стану судової справи, у яких користувач є учасником; ознайомлюватись з матеріалами справи в електронному вигляді; переглядати та подавати заяви, клопотання та інші документи, які користувач створив в своєму кабінеті; формувати, переглядати та анульовувати електронні ордери та довіреності у підсистемі для швидкого доступу до матеріалів судової справи; мінімізувати час та кошти на роздруківку та відправку документів; отримувати судові рішення у електронному вигляді. Тобто, наразі наявні всі технічні можливості для забезпечення повноцінного дистанційного судового процесу: від моменту подання позову до моменту набрання рішенням законної сили[1].

Разом з тим, представниками суддівського апарату підкреслюється, що при розробці підсистеми «Електронний суд» та подальшому вдосконаленні дистанційного судочинста основний орієнтир був направлений на зручність та «доступность» цієї підсистеми для учасників справи та їх представників. Водночас, для суддів, їх помічників та секретарів судового засідання в питанні здійснення судочинства, по суті, нічого не змінилось, адже їх робота і далі передбачає особисту присутність в залі судового засідання, друк документів, формування паперових справ та спілкування з учасниками процесів традиційними засобами – поштою, телефоном або особисто[2].

---

[1] Притуляк В. М. Підсистема електронний суд: особливості її функціонування в умовах воєнного стану. *Цивільне судочинство та виконавче провадження в умовах воєнного стану*: матеріали всеукр. наук.-практ. конф. ім. Ю. С. Червоного (Одеса, 16 грудня 2022 р.). Одеса. Фенікс. 2022. С. 63.

[2] Арсірій Р. Електронне судочинство в період воєнного стану: очікування та реальність. *Судово-юридична газета*. 27.06.2024. URL: https://sud.ua/uk/news/blog/242253-elektronne-sudochinstvo-v-period-voyennogo-stanu-ochikuvannya-ta-realnist.

Окрім того, «левова частка» комунікації та документообіг між учасниками електронного судочинства відбувається за допомогою електронної пошти та хмарних сервісів для зберігання файлів, а також враховуючи значення відповідної інформації та небажані наслідки її розкриття, існує потреба в застосуванні дієвих заходів кібербезпеки. Витік інформації або небажане розголошення ходу чи результату судового процесу може спричинити суттєві наслідки, включаючи економічні втрати та репутаційну шкоду. Наприклад, публічне розкриття інформації щодо державних справ може негативно вплинути на державну політику.

Наразі одним з найбільш розповсюджених способів захисту даних є використання хмарних сервісів для їх зберігання, зважаючи доступність і достатню захищеність даних сервісів (наприклад, Google Drive від Google, Dropbox та OneDrive від Microsoft). Втім, на практиці використання хмарних сервісів є лише одним із можливих заходів покращення рівня інформаційної безпеки.

Як зазначалось вище, питання кібербезпеки в умовах воєнного стану є особливо важливим як для учасників процесу, так і для працівників судового апарату. Проте, попри численні кібератаки, які збільшились після початку повномасштабного вторгнення, вітчизняним законодавцем не було передбачено жодних нормативних змін в контексті покращення діловодства та підвищення інформаційної безпеки судочинства. Водночас, дистанційна форма здійснення судочинства залишається недостатньо унормованою в частині технічного забезпечення національних судів. Окрім того, до наявних проблем додались інші, зокрема, брак коштів на цифровий зв'язок чи забезпечення стабільного енергопостачання.

Водночас, ЄСІТС досі має різні вразливості, які можуть потенційно загрожувати інформаційній безпеці, зокрема, через хакерські атаки, фішинг, віруси, зловмисні програми тощо. Це може призвести до несанкціонованого доступу до судових даних, внищення інформації, порушення конфіденційності даних, а також перешкоджати нормальному функціонуванню системи правосуддя. Серед іншого, зловмисники можуть використовувати соціальну інженерію, щоб отримати несанкціонований доступ до судової інформації. Це може включати фальшиві електронні листи чи запити на інформацію тощо, з метою отримання доступу до системи. Такі ризики стають можли-

ві, а іноді навіть сприють атакам на систему, в умовах використання слабких паролів, кодів, недостатні навички працівників суду уникати шахрайство в Інтернеті тощо. Видається, що найбільш небезпечним є хакерські атаки, коли залучаються особи, що мають доступ до судової системи. Недостатня проінформованість персоналу про кіберзагрози може призвести до вразливостейсамої підсистеми «Електронний суд»[1].

З метою запобігання вищеперерахованим ризикам, видається доцільною розробка рекомендацій та протоколів роботи судів, які б могли зменшити загрозу стороннього втручання або маніпулювання в «ручному» режимі програмним забезпеченням підсистеми «Електронний суд». Зокрема, у жовтні 2024 року Національна школа суддів України проводила підготовку та підвищення рівня кваліфікації працівників апаратів судів, відповідальних за інформаційно-технічне забезпечення. Навчання полягало у підготовці працівників інформаційно-технічного забезпечення судів до ефективної та безпечної роботи в цифровому середовищі, забезпеченні надійності електронного документообігу та дотриманні стандартів кібербезпеки. Програма охоплювала як технічні аспекти обміну документами через підсистему "Електронний суд", так і правила інформаційної безпеки під час війни, включаючи інформаційно-психологічну гігієну[2].

При дослідженні вразливостей системи ЄСІТС неможливо оминути систему електронного архівування. А саме, ЄСІТС дозволяють створювати електронні архіви правових документів, судових рішень, законів та інших нормативних актів. В цьому контексті не варто забувати про можливість усвідомленого псування або некоректного внесення інформації працівниками судової системи, що мають доступ до ЄСІТС[3].

Відповідно до ст. 9 Закону України «Про захист інформації в інформаційно-комунікаційних системах», відповідальність за забезпе-

---

[1] Ковальчук А., Чернявська Б. Забезпечення безпеки електронних даних у господарському судочинстві: правові та організаційні аспекти. *Право та державне управління.* 2023. Вип. 2. С. 269.

[2] Інформаційна безпека судів під час війни. *Національна школа суддів України.* 31.10.2024. URL: https://nsj.gov.ua/ua/news/informatsiyna-bezpeka-sudiv-pid-chas-viyni/

[3] Ковальчук А., Чернявська Б. Забезпечення безпеки електронних даних у господарському судочинстві: правові та організаційні аспекти. *Право та державне управління.* 2023. Вип. 2. С. 269.

чення захисту інформації в системі покладається на власника системи. Розпорядником інформації, який відповідає за захист інформаційних систем судової системи є Державна судова адміністрація України. Разом з тим, до сфери управління ДСА належить Державне підприємство «Інформаційні судові системи»[1]. Вказане підприємство створено, серед іншого, з метою організації збереження та захисту даних, що містяться в автоматизованих системах державних реєстрів; надання послуг з інформаційно-технічного забезпечення судів; забезпечення діяльності органів судової влади, у тому числі в умовах особливого періоду[2]. Судячи з опису обов'язків підприємства, що були надані Державною судовою адміністрацією, саме до цієї юридичної особи слід звертатися з питаннями повного або часткового відключення суду від доступу до електронних сервісів.

У межах реалізації Стратегії кібербезпеки України для виконання постанови Кабміну від 04.04.2023 № 299, Адміністрацією Держспецзв'язку розроблено та затверджено Методичні рекомендації щодо реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі. Відповідний наказ від 03.07.2023 № 570 розміщений на сайті Служби. Серед методичних рекомендації можна виокремити: необхідний перелік заходів із кіберзахисту, яких можуть вживати суб'єкти забезпечення кібербезпеки послідовно за етапами реагування на кібератаки; механізм застосування критеріїв, за якими визначається категорія (рівень) критичності кібератаки; принципи пріоритезації кібератак; типовий перелік заходів із реагування на кібератаки для одночасного відстеження заходів до їх завершення тощо.

Реалізацію відповідних методичних рекомендацій покладено на начальника Відділу інформаційно-технічного забезпечення, захисту інформації та баз даних суду. Отже, начальник Відділу здійснює: забезпечення кібербезпеки та захисту інформації в суді, кіберзахи-

[1] Витяг із Статуту Державного підприємства «Інформаційні судові системи» (затвердженого наказом Державної судо- вої адміністрації України від 26 листопада 2019 року № 1142). URL: https://ics.gov.ua/ics/about/acts/

[2] Про затвердження Методичних рекомендацій щодо реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі. URL: https://cip. gov.ua/ua/news/nakaz-administraciyi- derzhspeczv-yazku-vid-03-07-2023-570- pro-zatverdzhennya-metodichnikh-rekomendacii-shodo-reaguvannya-sub- yektami-zabezpechennya-kiberbezpeki- na-rizni-vidi-podii-u-kiberprostori.

сту локального мережевого середовища суду та організація роботи по захисту інформації, проектування, розроблення, супроводження та модернізації комплексної системи захисту інформації в суді; забезпечення контролю за розробленням проектної та технічної документації комплексної системи захисту інформації, організації робіт, пов'язаної із забезпеченням захисту персональних даних у базах даних від незаконної обробки та несанкціонованого доступу. Також, на начальника Відділу покладається обов'язок з забезпечення формування довідкових матеріалів, презентацій по користуванню програмним забезпеченням та інформаційними системами, які впроваджені у суді. Тобто, вказана особа здійснює інформаційні роз'яснення для працівників суду, зокрема, щодо способів уникнення інтернет-шахрайства та інформаційної гігієни[1].

Висновки

Робота підсистеми «Електронного суду» заслуговує окремої уваги в період воєнного часу, адже саме відповідна підсистема дозволила адаптуватися до складних умов воєнного стану та забезпечити функціонування судової системи в дистанційному режимі, що надало можливість громадянам отримати доступ до правосуддя як законодом, так і в умовах ракетних обстрілів в межах України.

З урахуванням вищезазначеного, можна констатувати, що всі вищеперераховані виклики не зупиняюсь здійснення правосуддя, хоча можуть ускладнювати чи гальмувати роботу суддівського апарату. Одним із ризиків, який можна очікувати через кібератаки під час проведення судового процесу, є ризик погіршення репутації дистанційної форми судочинства, як надійного та прогресивного способу здійснення правосуддя.

Впровадження електронного судочинства в Україні має на меті підвищення ефективності, якості та прозорості правосуддя, зменшення бюрократичних процедур шляхом автоматизації процесів документообігу, розподілу справ, обміну документами між судами та

[1] Ковальчук А., Чернявська Б. Забезпечення безпеки електронних даних у господарському судочинстві: правові та організаційні аспекти. *Право та державне управління.* 2023. Вип. 2. С. 270.

учасниками судового процесу, фіксування судового процесу, участь учасників судового процесу в режимі відеоконференції, забезпечення фінансових, майнових, організаційних, інформаційно-телекомунікаційні та інші потреб органів судової влади.

Інформаційна безпека України забезпечується шляхом проведення державної політики відповідно до прийнятих в установленому порядку нормативно-правових актів, концепцій, стратегій і програм. Основними напрямами державної політики у сфері кібербезпеки України є: створення захищеного національного сегмента кіберпростору, що сприятиме підтриманню відкритого суспільства і забезпечуватиме безпечне використання цього простору суспільством; запобігання втручанню у внутрішні справи України і нейтралізація посягань на її інформаційні ресурси з боку інших держав; посилення обороноздатності держави у кіберпросторі; зниження рівня уразливості об'єктів кіберзахисту; забезпечення повноправної участі України в загальноєвропейській та регіональних системах забезпечення кібербезпеки тощо.

Для захисту системи ЄСІТС важливо приділяти увагу інформаційній безпеці, використовувати захисне програмне забезпечення, проводити регулярні тренінги серед працівників суду, аудити безпеки, а також дотримуватися міжнародних стандартів щодо обробки, збереження і передачі судових даних.

З урахуванням вищезазначеного, забезпечення безпечного функціонування ЄСІТС та підсистеми «Електронний суд» постає одним з пріоритетів подальшої державної політики в частині реформування судової системи України.

Ключові слова: електронне судочинство, інформаційна війна, гібридна війна, кіберзагроза, кібербезпека.

Розділ 21

КІБЕРСПОРТИВНА ДИПЛОМАТІЯ: ПЕРСПЕКТИВИ ДЛЯ УКРАЇНИ

DOI

Максим Ткалич
кандидат юридичних наук, доцент

Юлія Толмачевська
докторка філософії (081 право)

Сучасні реалії світової політики, зокрема повномасштабне вторгнення Російської Федерації в Україну у 2022 році, істотно трансформували підходи до міжнародної дипломатії. Традиційні інструменти, як-от класична дипломатія та міждержавні переговори, доповнюються новими формами м'якої сили – культурною, спортивною та, як демонструє практика останніх років, кіберспортивною дипломатією. У цьому контексті Україна опинилася в унікальному становищі: з одного боку, вона веде боротьбу за свою територіальну цілісність, а з іншого – активно просуває власний імідж на міжнародній арені через інноваційні гуманітарні інструменти.

У цьому контексті важливо дослідити, яким чином правове забезпечення може підтримати дипломатичний потенціал кіберспорту в Україні, зокрема через приклад гри S. T. A. L. K. E. R. 2, створеної українською студією GSC Game World.

S. T. A. L. K. E. R. 2: Heart of Chornobyl – це не лише чергова відеогра в жанрі survival horror, а важливий вияв українського культурного спротиву в умовах війни. Розроблена компанією GSC Game World, яка була змушена евакуюватися з Києва до Праги внаслідок вторгнення Російської Федерації, гра стала потужним міжнародним меседжем: український геймінг не лише вижив у часи війни, але й зберіг креативність, якість і здатність до глобального впливу. У березні 2022 року компанія офіційно припинила діяльність у Росії, тим самим підтвердивши проукраїнську позицію та солідарність зі світовою спільнотою.

Сама гра глибоко вкорінена в український наратив. Постапокаліптична тематика Чорнобиля тут виконує не лише роль антуражу, а й виступає як символ загроз, що стали реальністю – зокрема екологічних і геополітичних. Гасло "Made in Ukraine during the war", що супроводжує рекламні кампанії S. T. A. L. K. E. R. 2, перетворює гру на акт цифрового спротиву, який доносить до мільйонів гравців у всьому світі реалії української боротьби.

Варто зазначити, що серія S. T. A. L. K. E. R. уже має культовий статус у глобальному геймерському середовищі – перші частини стали бестселерами, сформували численні фан-спільноти та навіть надихнули на створення модифікацій, коміксів і документальних проєктів. У цьому контексті S. T. A. L. K. E. R. 2 розглядається не просто як комерційний продукт, а як платформа для стратегічної комунікації, яка поєднує ігрову індустрію, культурну ідентичність та елементи кібердипломатії.

Хоча гра формально не є дисципліною кіберспорту, її вплив відчувається на екосистему геймерського ком'юніті, до якого належать і професійні гравці, стримери, аналітики та креатори контенту. Рекламні ролики, фанатські проєкти, колаборації з іншими брендами й платформами трансформують S. T. A. L. K. E. R. 2 на інформаційний хаб української культури в цифровому середовищі.

З огляду на це, гра виконує функцію не лише культурної, а й кіберспортивної дипломатії, адже вона:

- просуває український бренд на глобальних ігрових платформах (Steam, Xbox, Epic Games);
- формує позитивний імідж країни, що здатна виробляти контент світового рівня навіть в умовах війни;
- слугує майданчиком для неформальної дипломатії – через співпрацю з блогерами, стримерами, геймерами;
- відкриває нові формати гуманітарної підтримки – через продаж ігрових бонусів, NFT, тематичних мерчів, кошти з яких спрямовуються на допомогу ЗСУ або гуманітарні ініціативи.

Гра набуває особливого значення з огляду на трагедію Володимира Єжова (псевдонім «Fresh») – дизайнера гри, який загинув 22 грудня 2022 року під Бахмутом, у складі добровольчого корпусу. Його подвиг став символом героїзму української культури та посилив дипломатичний імпульс проєкту.

Таким чином, S. T. A. L. K. E. R. 2: Heart of Chornobyl є прикладом того, як геймінг може стати каналом для формування політичного меседжу, мобілізації міжнародної підтримки та конструювання цифрової суб'єктності держави на тлі глобальних загроз.

Отже, кіберспорт, як динамічна сфера, що поєднує технології, молодіжну культуру та глобальні комунікації, стає важливим засобом репрезентації національних інтересів. Після початку війни багато українських кіберспортсменів стали не лише представниками своєї країни на змаганнях, а й символами стійкості, волі до перемоги та захисниками цифрового культурного фронту. У зв'язку з цим актуалізується потреба в правовому осмисленні кіберспортивної діяльності – як у межах національного правового поля, так і на міжнародному рівні.

Крім суто дипломатичних аспектів кіберспорту дослідження механізмів правового регулювання, договірних зобов'язань, міжнародного партнерства у сфері кіберспорту, а також аналіз потенціалу кіберспортивної дипломатії становлять наукову та практичну цінність в умовах нової геополітичної реальності. Особливої ваги це набуває для України, яка прагне інтегруватися до європейського правового простору та водночас протистоїть гібридним викликам з боку держави-агресора.

Варто нагадати, що кіберспорт (англ. esports) – це форма змагальної діяльності у відеоіграх, яка має ознаки спортивного змагання: чіткі правила, системи ліг, команди, тренерів і фанатів. Відповідно до рішення Міністерства молоді та спорту України від 2018 року, кіберспорт визнано офіційним видом спорту в Україні. Водночас українське законодавство досі не містить спеціального закону про кіберспорт.

У міжнародній площині регулювання здійснюється переважно приватноправовими актами розробників ігор (наприклад, EULA – End User License Agreement) та організаторів змагань. У Європейському Союзі відсутня уніфікована правова база щодо кіберспорту, однак низка держав (Франція, Німеччина, Іспанія) мають власні акти, які регулюють діяльність кіберспортсменів, контракти, оподаткування тощо.

Нормативно-правове регулювання кіберспорту в Україні базується на загальних положеннях Закону України «Про фізичну культуру

і спорт», а також на наказах Міністерства молоді та спорту. Водночас відсутність спеціального закону створює низку правових прогалин:

- не врегульовано статус кіберспортсмена;
- відсутній механізм ліцензування турнірів;
- невизначені вимоги до контрактів між гравцями й організаціями;
- слабке податкове регулювання діяльності кіберспортивних клубів.

У 2022 – 2023 роках у Верховній Раді лунали пропозиції щодо розробки спеціального закону про кіберспорт, однак наразі вони не реалізовані. Перспективним напрямом є гармонізація українського законодавства із практиками ЄС у межах Угоди про асоціацію.

Повертаючись до дипломатичних аспектів гри, слід зазначити, що за аналогією зі спортивною дипломатією (наприклад, Олімпійськими іграми, де держави просувають свою культурну ідентичність), поняття «кіберспортивної дипломатії» передбачає використання кіберспорту як платформи для посилення міжнародної суб'єктності держави, формування позитивного іміджу та культурного обміну. Механізмами є:

- участь національних команд у міжнародних турнірах;
- проведення великих івентів в Україні;
- підтримка власних розробників і гравців як культурних амбасадорів;
- створення державної програми підтримки кіберспорту на міжнародному рівні.

Прикметно, що Україна за останні роки стала одним із лідерів світової кіберспортивної сцени. Розвинена інфраструктура, висококваліфіковані гравці та міжнародні команди з українськими спортсменами сприяють формуванню позитивного іміджу країни в глобальному інформаційному просторі.

Однією з найвідоміших і найуспішніших команд у світі є український клан Natus Vincere (Na'Vi). Упродовж останніх трьох років Na'Vi продовжує утримувати високі позиції у дисциплінах Counter-Strike: Global Offensive (CS:GO), Dota 2 та Rainbow Six Siege, демонструючи стабільність, професіоналізм і спортивний дух.

PGL Major Antwerp 2022 (CS:GO): Na'Vi посіла друге місце, програвши у фіналі лише команді FaZe Clan, але підтвердила свій статус

однієї з найкращих у світі. Турнір транслювався мільйонами глядачів, що стало ефективним майданчиком для просування України на світовій арені.

The International 2021 (Dota 2): Хоча Na'Vi не змогла повторити тріумф 2011 року, команда увійшла до топ-8, демонструючи високий рівень гри та українську майстерність у світовому кіберспорті.

BLAST Premier Spring Finals 2023: Команда Na'Vi виборола титул чемпіонів, що стало яскравим сигналом про відродження їх домінування у CS:GO після кількох років поступового спадання.

На Європейському чемпіонаті з кіберспорту 2025 року (European Esports Championship 2025), який відбувся з 9 по 13 липня в Пріштіні, Косово, під егідою Європейської федерації кіберспорту (EEF) та Федерації кіберспорту Косова, українська змішана збірна дійшла до фіналу гри CS-2.

У контексті війни, в якій перебуває Україна, кожен міжнародний виступ українських кіберспортсменів набуває подвійного значення. Вони стають не лише змаганнями за трофеї, а й формою міжнародної дипломатії, що:

- поширює знання про Україну у світі, демонструючи її національну стійкість;
- формує образ України як сучасної, технологічно розвиненої країни, яка успішно конкурує у сфері цифрових технологій;
- сприяє консолідації української діаспори і прихильників у різних країнах;
- забезпечує додаткову увагу до гуманітарних проблем через прямі звернення гравців і команд до аудиторії.

Особливої ваги цьому надають участь українських команд у глобальних турнірах з великими трансляціями (наприклад, PGL Major, The International), де аудиторія сягає десятків мільйонів.

З точки зору правового аналізу, участь українських команд і гравців у міжнародних турнірах супроводжується низкою правовідносин:

- договірні зобов'язання між гравцями та клубами;
- ліцензійні угоди з власниками ігор;
- трудові відносини у частині контрактів, зарплат і соціальних гарантій;
- оподаткування призових і доходів;

- захист прав інтелектуальної власності, зокрема ніків, логотипів і трансляцій.

Європейська практика надає приклади нормативного регулювання: у Франції введено статус «професійного кіберспортсмена», а у Німеччині кіберспорт визнаний спортивною діяльністю, що дає змогу залучати іноземних гравців на пільгових умовах. Україні доцільно запозичити такі підходи, адаптуючи їх до національного контексту.

Щодо перспектив правового регулювання кіберспорту в Україні, то було б доцільно розробити спеціальний закон «Про кіберспорт», який включав би:

- визначення понять (кіберспортсмен, організатор турніру, кіберспортивний клуб);
- регулювання статусу учасників та їхньої правової відповідальності;
- процедуру реєстрації, ліцензування та контролю за кіберспортивними організаціями;
- захист прав учасників, зокрема неповнолітніх гравців;
- запобігання шахрайству, допінгу, маніпуляціям результатами.

Україна має всі передумови стати центром кіберспортивного розвитку в Східній Європі, а належне правове регулювання здатне стимулювати як внутрішній ринок, так і зміцнити міжнародну присутність.

Висновки

Упродовж останнього десятиліття кіберспорт поступово трансформувався з нішового хобі у глобальне явище, яке охоплює мільйони гравців, глядачів і спонсорів у всьому світі. Цей розвиток відкрив новий вимір публічної дипломатії – кіберспортивну дипломатію – яка дедалі частіше використовується як інструмент м'якої сили, зокрема в контексті гібридних загроз, культурної боротьби та просування національного іміджу. В умовах повномасштабної збройної агресії росії проти України кіберспорт набув не лише соціокультурного, але й геополітичного виміру, а українські гравці, розробники та команди почали відігравати роль цифрових амбасадорів своєї держави.

Глобальною тенденцією стало залучення кіберспорту до національних стратегій публічної дипломатії. Держави, як-от Південна Корея, Китай, США та Франція, активно фінансують розвиток кіберспортивної інфраструктури, підтримують участь у міжнародних турнірах, укладають стратегічні партнерства з провідними кіберспортивними організаціями. У деяких випадках (як у Франції чи ОАЕ) уряди виступають співорганізаторами кіберспортивних чемпіонатів світового рівня, які слугують майданчиком для просування іміджу країни, обміну технологіями та залучення іноземних інвестицій. Така стратегія відповідає сучасним вимогам цифрової дипломатії, де кіберпростір і віртуальні спільноти стають не менш впливовими за традиційні ЗМІ чи класичну культуру.

В Україні кіберспортивна дипломатія розвивається на тлі складної безпекової ситуації, але демонструє стійку позитивну динаміку. Гучні перемоги українських команд NAVI, Monte та гравців у дисциплінах CS:GO, Dota 2, Valorant стали важливими інформаційними приводами для зміцнення авторитету України на міжнародній арені. Завдяки участі в престижних світових турнірах, українські гравці не лише здобувають визнання, але й популяризують українську мову, символіку, патріотичну позицію. Це дозволяє формувати нові форми культурної присутності України у світовому медіапросторі, особливо серед молоді.

Ключову роль у формуванні іміджу України як цифрової нації відіграють також українські розробники, зокрема студія GSC Game World, яка створює гру S. T. A. L. K. E. R. 2: Heart of Chornobyl. Унікальність цього кейсу полягає в поєднанні культурної, технологічної та дипломатичної складових. Гра, створена в умовах війни, позиціонується як символ незламності та водночас – як витвір української ідентичності, спрямований на західного споживача. Вона виступає інструментом цифрової дипломатії, де гравець мимоволі занурюється в наративи, близькі українському досвіду спротиву, втрати й надії.

Перспективи подальшого розвитку кіберспортивної дипломатії в Україні залежать від кількох факторів:

Інституціоналізація. Потрібна державна стратегія підтримки кіберспорту як частини цифрової та культурної дипломатії. Зокрема, доцільно включити його до культурної політики, сприяти формуванню прозорої нормативної бази, підтримувати освітні програми та ініціативи на місцевому рівні;

Міжнародне партнерство. Важливо укладати меморандуми про співпрацю з провідними кіберспортивними організаціями світу, розвивати публічно-приватні партнерства, просувати участь українських гравців і команд у міжнародних лігах.

Символічний капітал. Україна повинна системно працювати над створенням нових ігрових продуктів на кшталт S. T. A. L. K. E. R., які просувають українську культурну спадщину, історичну пам'ять і сучасну реальність у привабливому форматі.

Отже, кіберспорт став не просто елементом розваг чи спортивного змагання, а справжнім інструментом дипломатичної взаємодії. Україна вже успішно використовує його у боротьбі за інформаційний простір, і має всі підстави для подальшого закріплення своїх позицій як цифрової культурної держави в сучасному світі.

Ключові слова: ІТ-право, інформаційне суспільство, кіберспорт, спортивна дипломатія, національна стратегія, збройна агресія, гібридна війна.

СПИСОК ОСНОВНИХ ПРАЦЬ ПРЕДСТАВНИКІВ ШКОЛИ

2011 р.

1. Харитонова О. І., Харитонов Є. О. Об'єкт інформаційних цивільних правовідносин та цивільних правовідносин право інтелектуальної власності: до проблеми співвідношення. *Інформаційні правовідносини та право інтелектуальної власності як інститути приватного права*: четверті цивілістичні читання, присвячені пам'яті професора О. А. Підопригори: 25 березня 2010 року: зб. наук. доп. та ст. К.: Видавничо-поліграфічний центр «Київський університет», 2011. С. 62-68.

2015 р.

2. Харитонов Є. О. Спроба класифікації порушення авторських прав у мережі Інтернет. *Захист права інтелектуальної власності у мережі Інтернет*: теоретичні та практичні аспекти: матеріали Інтернет-конференції (Одеса, 22 травня 2015 р.). За заг.ред. О. І. Харитонової. Одеса: Юридична література, 2015. С. 75-78.
3. Харитонова О. І., Позова Д. До проблеми визначення правової природи мережі Інтернет. *Вісник Південного регіонального центру Національної академії правових наук України*. 2015. № 4. С.79-88.
4. Харитонова О. І. Об'єкти авторського права і електронні бібліотеки. *Роль принципів DCFR в імплементації угод про асоціацію ЄС – Україна:* матеріали круглого столу (Одеса, 12 груд. 2015 р.). Одеса : Фенікс, 2015. С. 41-44.
5. Харитонова О. І. Піратство у всесвітній мережі Інтернет. *Правові та інституційні механізми забезпечення сталого розвитку України* : матеріали Міжнародної науково-практичної конференції (15-16 травня 2015 р., Одеса): у 2 т. Т.2. Одеса: Юридична література, 2015. С. 507-509.
6. Харитонова О. І. Розвиток законодавства щодо регулювання відносин у мережі Інтернет: досвід ЄС. *Цивілістичні читання, присвячені пам'яті І. В. Шерешевського «Проблеми адаптації законодавства України до законодавства ЄС:* матер.інтернет-конф. (Одеса, 11 грудня 2015 р.). Одеса: Фенікс, 2015. С. 9-14.
7. Харитонова О. І. Специфіка регулювання відносин у всесвітній мережі Інтернет: проблемні питання. *Римське право і сучасність*: матер. Міжнар. наук. конф. (Одеса, 29 травня 2015 р.). За заг. ред. Є. О. Харитонова. Одеса.: Фенікс, 2015. С. 90-91.
8. Харитонова О. І., Ульянова Г. О. та ін. Проблемні питання визначення правової природи і структури правовідносин інтелектуальної власності, що вини-

кають у мережі Інтернет. *Наукові праці Національного університету «Одеська юридична академія»*. Т. XVII. Одеса: Юридична література, 2015. С. 159-200.

9. Харитонова О. І., Харитонов Є. О. «Інтернет-відносини» – віртуальна нереальність. *Захист права інтелектуальної власності у мережі Інтернет*: теоретичні та практичні аспекти: матеріали Інтернет-конференції (Одеса, 22 травня 2015 р.). За заг.ред. О. І. Харитонової. Одеса: Юридична література, 2015. С. 72-75.
10. Харитонова О. І., Харитонов Є. О. «Інтернет-відносини» – віртуальна нереальність. *Від засад римського права до принципів приватного права ЄС* : матер. круглого столу (Одеса, 29 травня 2015 р.). Одеса : Фенікс, 2015. 27-30.

2016 р.

11. Бааджи Н. П. Деякі правопорушення у мережі Інтернет. *Правові та інституційні механізми забезпечення розвитку держави та права в умовах євроінтеграції:* матеріали Міжнародної науково-практичної конференції (20 травня 2016 р., м. Одеса): у 2т. Т.2. Одеса: Юридична література, 2016. С. 559-561.
12. Харитонов Є. О. ІТ-право з погляду цивілізаційного та концептного підходів. *Часопис цивілістики.* 2016. Вип. 22. С.122-127.
13. Харитонов Є. О. Сутність ІТ-права (ІТ-право як концепт). *ІТ-право: проблеми і перспективи розвитку в Україні:* збірник матеріалів науково-практичної конференції. Львів: НУ «Львівська політехніка», 2016. С.274-280.
14. Харитонов Є. О., Харитонова О. І. Інтернет-право, інформаційне право та ІТ-право: проблема співвідношення. *Правова адаптації законодавства України до умов внутрішнього ринку ЄС* : матеріали Міжнародної інтернет-конференції, присвяченої пам'яті І. В. Шерешевського (2 грудня 2016 р., Одеса). Одеса : Фенікс, 2016. С. 3-7.
15. Харитонов Є. О., Харитонова О. І. Інтернет-право, інформаційне право та ІТ-право: проблема співвідношення. *Правова адаптації законодавства України до умов внутрішнього ринку ЄС* : матеріали Міжнародної інтернет-конференції, присвяченої пам'яті І. В. Шерешевського (2 грудня 2016 р., м. Одеса). Одеса : Фенікс, 2016. С.3-7.
16. Харитонова О., Ульянова Г. Неправомірне використання об'єктів права інтелектуальної власності в мережі Інтернет. *Юридичний вісник.* 2016. № 4. С.55-64.
17. Харитонова О. І Мережа Інтернет як інформаційне підґрунтя інтеграційних процесів в галузі права. *Право та інтеграція: глобальний, регіональний, національний виміри*: Робочі матеріали Всеукраїнської наукової веб-конференції 21 квітня 2016 року. м. Одеса. Електронне наукове видання. С. 5-7.
18. Харитонова О. І. Електронні твори як об'єкти авторського права в епоху комп'ютерних технологій. *Правові та інституційні механізми забезпечення розвитку держави та права в умовах євроінтеграції:* матеріали Міжна-

родної науково-практичної конференції (20 травня 2016 р., Одеса) : у 2 т. Т.2. Одеса: Юридична література, 2016. С.535-537.

19. Харитонова О. І. Інтерактивне громадянське суспільство: до проблеми формування. *Римське право як підґрунтя сучасного права Європи* : матеріали між нар.наук.-практ.конф. (м. Одеса, 27 травня 2016 р.). За заг.ред. Є. О. Харитонова. Одеса: Фенікс, 2016. С. 103-105.
20. Харитонова О. І. Інтернет і поява нових категорій цивільного права: до постановки проблеми. *Правові та інституційні механізми забезпечення розвитку держави та права в умовах євроінтеграції*: матеріали Міжнародної науково-практичної конференції (20 травня 2016 р., м. Одеса) : у 2 т. Т.2. Одеса: Юридична література, 2016. С.556-559.
21. Харитонова О. І. Перший посібник з ІТ-права. *Право України.* 2016. № 11. С. 274-275.
22. Харитонова О. І. Питання боротьби з порушенням авторських прав у Всесвітній мережі Інтернет. Досвід правових реформ України та Республіки Молдова на шляху до євроінтеграції : матеріали інтернет-конф. (Одеса, 29 березня 2016 р.). За заг. ред. Харитонова Є. О. Одеса: Фенікс, 2016. С. 58-61.
23. Харитонова О. І. Проблемні питання визначення системи (структури) ІТ-права. *ІТ-право: проблеми і перспективи розвитку в Україні:* збірник матеріалів науково-практичної конференції. Львів: НУ «Львівська політехніка», 2016. С.280-285.
24. Харитонова О. І. Рецензія на посібник Т. В. Бачинського як привід для роздумів про систему ІТ-права. *Часопис цивілістики.* 2016. Вип. 22. С. 145-148.
25. Харитонова О. І., Харитонов Є. О. Деякі проблеми захисту прав користувачів у мережі Інтернет. *Актуальні проблеми приватного права* : матеріали наук-практ. конф., присвяченої 94-й річниці з дня народж.д-ра юрид.наук, проф., чл.-кор. АН УРСР В. П. Маслова (Харків, 19 лют. 2016 р.). Х.: Право, 2016. С.51-54.
26. Харитонова О. І., Харитонов Є. О. Деякі проблеми захисту прав користувачів у мережі Інтернет. *Актуальні проблеми приватного права* : матеріали наук-практ. конф., присвяченої 94-й річниці з дня народж.д-ра юрид.наук, проф., чл.-кор. АН УРСР В. П. Маслова (Харків, 19 лют. 2016 р.). Х.: Право, 2016. С.51-54.
27. Харитонова О. І. Відносини, що виникають у мережі інтернет: специфіка і проблеми визначення правової природи. *Вісник Південного регіонального центру Національної академії правових наук України.* 2016. № 6. С. 63-68.
28. Kharitonova O. I., Pozova D. D. Some aspects of the legal nature of the internet network. *Часопис цивілістики.* 2016. Вип. 20. С.188-192.

2017 р.

29. Авторське право та авторознавча лінгвістична експертиза у цифрову добу: монографія: О. І. Харитонова, Н. І. Клименко, Є. О. Харитонов, Г. О. Улья-

нова, Г. І. Григорянц; за ред. О. І. Харитонової, Н. І. Клименко.Одеса: Фенікс, 2017. 270 с.
30. Бааджи Н. П. Зміст правовідносин у мережі Інтернет : проблеми та шляхи вирішення. *Науковий вісник Херсонського державного університету.* 2017. Т.1. С. 166-171.
31. Давидова І. В. ЕЦП та інші ідентифікатори особи, як чинники гармонізації українського законодавства із законодавством Європейського Союзу. *Молодий вчений.* 2017. № 12 (52). С. 287-291.
32. Давидова І. В. Правочини у ІТ-сфері та інформаційна безпека. *ІТ-право та інформаційна безпека:* моногр. За ред. О. І. Харитонової, Є. О. Харитонова. Одеса : Фенікс, 2017. С. 74-86.
33. Давидова І. В. Правочини як підстави виникнення цивільних правовідносин в інформаційному суспільстві. *Часопис цивілістики.* 2017. Вип. 27. С. 38-41.
34. ІТ- право та інформаційна безпека: монографія. За ред. О. І. Харитонової, Є. О. Харитонова.Одеса:Фенікс, 2017.176 с.
35. ІТ-право – це просто: посібник. За ред. Є. О. Харитонова. Одеса : Фенікс, 2017. 106 с.
36. ІТ-право та інформаційна безпека: навч.-метод. посібник. За ред. Є. О. Харитонова. Одеса: Фенікс, 2017. 136 с.
37. ІТ-право: теорія та практика: навч. посіб. За ред.. Є. О. Харитонова, О. І. Харитонової. Одеса: Фенікс, 2017. 472 с.
38. Information security and IT law in conditions of integration processes: Collective monograph. Edited by O. Kharytonova, E. Kharytonov. Riga: Izdevnieciba Baltija Publishing, 2017. 213 p.
39. Некіт К. Г. Право власності та право інтелектуальної власності у сфері ІТ-відносин: проблема співвідношення. *ІТ-право : поняття та сутність : монографія.* За ред. О. І. Харитонової, Є. О. Харитонова. Одеса : Фенікс, 2017. С. 185-207.
40. Некіт К. Г. Веб-сайт як комплексний об'єкт цивільних прав. *Часопис цивілістики.* 2017. № 26 (Спецвипуск ІТ-право). С. 50-55.
41. Некіт К. Г. Доменне ім'я як об'єкт цивільних прав. *Часопис цивілістики.* 2017. № 23. С. 40-45.
42. Некіт К. Г. ІТ-активи. Доменне ім'я як об'єкт майнових прав у ІТ-сфері. Вебсайт як майновий комплекс. Інтернет речей. *ІТ-право: теорія і практика:* навч. посібник. За ред.. Є. О. Харитонова, О. І. Харитонової. Одеса: Фенікс, 2017. С. 182-185; 185-192; 192-197; 197-201.
43. Некіт К. Г. Проблеми забезпечення інформаційної безпеки та відшкодування шкоди, заподіяної пристроями, підключеними до Інтернету речей. *Часопис цивілістики.* 2017. № 27. С. 107-112.
44. Некіт К. Г. Суб'єкти та об'єкти правовідносин у ІТ-сфері. Інтерне. *ІТ-право це просто*: посібник. За ред. Є. О. Харитонова. Одеса: Фенікс, 2017. С. 12-19; С. 26-29.
45. Сафончик О. І. ІТ та укладання шлюбу. Спільна власність подружжя на ІТ-об'єкти. Права та обов'язки батьків і дітей та ІТ. Порядок видачі докумен-

тів про державну реєстрацію актів цивільного стану в сфері ІТ. *ІТ-право: теорія та практика.* За заг. ред. Є. О. Харитонова, О. І. Харитонової. Одеса: Фенікс, 2017. С. 343-363.
46. Сафончик О. І. Шлюбний договір і ІТ: проблемні питання застосування. *Часопис цивілістики.* 2017. Вип. 26. С. 83-87.
47. Kharytonov Y. O., Kharytonova O. I. The integrative processes and the IT-law. *Законодавство України, Польщі та Литви у галузі приватного права*: матер. міжнародн. кругл. столу (16 травня 2017 р., Одеса) / за ред. д.ю.н., проф. Є. О. Харитонова. Одеса : Фенікс, 2017. С. 3-5.
48. Kharytonova O., Kharytonov E., Davydova I. It transactions and information security. *Information security and IT law in conditions of integration processes.* Edited by Riga : Izdevnieciba Baltija Publishing, 2017. P. 87-97.
49. Харитонов Є. О., Харитонова О. І. Проблема асекурації інформаційної безпеки неповнолітніх у ІТ – сфері в контексті немайнових правовідносин батьків та дітей. *Сучасний стан і перспективи розвитку сімейного права України в умовах адаптації до європейського права*: матер. всеукр. кругл. столу (Одеса, 26 травня 2017). За заг. ред. Є. О. Харитонова. Одеса: Фенікс, 2017. С. 4-9.
50. Харитонов Є. О. Інформаційна безпека з погляду цивілістики. *Цивільне право та інформаційна безпека в умовах інтеграційних процесів* : мат. кругл. столу (3 червня 2017 р., м. Одеса). Збірник матеріалів Міжнародного Конгресу «Правові проблеми державно-правового партнерства в умовах євроінтеграції», присвяченого 20-річчю Національного університету «Одеська юридична академія», м. Одеса, 2-4 червня 2017 р. Відп.ред.: Є. О. Харитонов, О. І. Харитонова, Т. Є. Харитонова. Одеса: Юридична література, 2017. С. 64-68.
51. Харитонов Є. О. Інформаційне суспільство та ІТ-сфера: шляхи впорядкування. *Часопис цивілістики.* 2017. № 26. С.6-10.
52. Харитонов Є. О. Проблема асекурація інформаційної безпеки неповнолітніх у ІТ-сфері в контексті немайнових правовідносин батьків та дітей. *Сучасний стан і перспективи розвитку сімейного права України в умовах адаптації до Європейського права* : мат. всеукр. кругл. столу (26 травня 2017 р., м. Одеса). За ред. Є. О. Харитонова, Калітенко О. М. Одеса: Фенікс, 2017. С. 4-9.
53. Харитонов Є. О., Давидова І. В. Особливості підстав виникнення цивільних правовідносин у ІТ-сфері. *ІТ-право: поняття та сутність: моногр.* Одеса: Фенікс, 2017. С. 161-184.
54. Харитонов Є. О., Некіт К. Г. Цивілістична школа національного університету «Одеська юридична академія» за 20 років – від рецепції римського права до концепції ІТ-права (ІТ-law). *Часопис цивілістики.* 2017. № 27. С. 8-15.
55. Харитонов Є. О., Харитонова О. І. Інформаційні технології та авторське право. *Вісник Південного регіонального центру Національної академії правових наук України.* 2017. № 10. С. 119-127.
56. Харитонов Є. О., Харитонова О. І. Проблема ІТ-права : матер. всеукр. наук.-практ.конф., яка проводиться в рамках тижня цивільного процесу

(Одеса, 18 квітня 2017 р.). За заг.ред. Голубєвої Н. Ю. Одеса: Фенікс, 2017. 112-115 с.
57. Харитонов Є. О., Харитонова О. І. Проблеми правового регулювання в ІТ-сфері в умовах інформаційної війни. *Проблеми відновлення конституційного ладу в Україні:* Матеріали міжнародної науково-практичної конференції. м. Київ. 19-20 травня 2017 р. Київ: Таврійський національний університет ім..В. І. Вернадського. 2017 С.159-163.
58. Харитонов Є. О., Харитонова О. І, Спасова К. І Формування одеської школи ІТ-права. *Часопис цивілістики.* 2017. № 27. С. 96-101.
59. Харитонов Є. О., Харитонова О. І. «Інтернет-відносини» та «Інтернет-правовідносини»: до визначення поняття і сутності. *Університетські наукові записки.* 2017.№ 3 (63). С. 27-38.
60. Харитонов Є. О., Харитонова О. І. «ІТ-право» як феномен правового регулювання. *Право як регулятор суспільних відносин: історія, теорія, практика*: збірник матеріалів Третьої міжнародної науково-практичної конференції (Київ, 20-21 квітня 2017 р.). Відп. ред. С. Г. Стеценко, Л. О. Васечко. К.: ВГО «Майбутнє країни», журнал «Публічне право», 2017. С.91-94.
61. Харитонов Є. О., Харитонова О. І. «ІТ-правовідносини» і загальна категорія правовідносин: до проблеми співвідношення. *Часопис цивілістики.* 2017. № 24. С. 87-93.
62. Харитонов Є. О., Харитонова О. І. Деякі проблеми характеристики категорії «Інтернет-правовідносини». *Наукові праці Національного університету «Одеська юридична академія».* Т.19. 2017. С. 382-389.
63. Харитонов Є. О., Харитонова О. І. Інформаційна безпека. *ІТ-право – це просто:* посібник. За ред. Є. О. Харитонова. Одеса: Фенікс, 2017. С. 36-42.
64. Харитонов Є. О., Харитонова О. І. Інформаційне суспільство, ІТ-сфера, ІТ-право. *ІТ-право – це просто :* посібник. За ред. Є. О. Харитонова. Одеса : Фенікс, 2017. С. 6-12.
65. Харитонов Є. О., Харитонова О. І. ІТ-право: альтернатива парадигми. *Наукові праці Національного університету «Одеська юридична академія».* 2017. Т.18. С. 191-200.
66. Харитонов Є. О., Харитонова О. І. Категорія «право власності» перед викликами цифрового світу. *Цивільне судочинство у світлі судової реформи в Україні:* всеукр.наук.-практ.конф.до 90-річчя від дня народження Ю. С. Червоного (м. Одеса, 6 листоп. 2017 р.). За заг.ред. Н. Ю. Голубєвої. Одеса: Фенікс, 2017. С. 21-25.
67. Харитонов Є. О., Харитонова О. І. Методологічні проблеми впорядкування відносин у сфері Інтернет речей. *Інтернет речей: проблеми правового регулювання та впровадження*: матеріали науково-практичної конференції (24 жовтня 2017 р., Київ). Київ: національний технічний університет України «Київський політехнічний інститут ім. Ігоря Сікорського» вид-во «Політехніка». 2017 С.121-128.

68. Харитонов Є. О., Харитонова О. І. Правове регулювання та саморегулювання у сфері застосування інформаційних технологій. *Право як регулятор суспільних відносин: історія, теорія, практика:* збірник матеріалів Четвертої міжнародної науково-практичної конференції (м.Київ, 7-8 листопада 2017 р.). Відп.ред. С. Г. Стеценко, Д. О. Васечко. К.: ВГО «Майбутнє країни», журнал «Публічне право». 2017. С.64-67.
69. Харитонов Є. О., Харитонова О. І. Юридична сутність ІТ-права. *ІТ-право: проблеми і перспективи розвитку в Україні*: збірник матеріалів ІІ-ї Міжнародної науково-практичної конференції (Львів, 17 листопада 2017 р.). Львів: НУ «Львівська політехніка», 2017. С.199-205.
70. Харитонова О. І. Інформаційні технології та авторські права: сучасні виклики. *Часопис цивілістики.* 2017. № 26. С.11-16.
71. Харитонова О. І. Інформаційно-комунікаційні технології і деякі проблеми авторського права. *Правове регулювання ІТ-відносин*: матер.всеукр. кругл. столу (м. Одеса, 18 травня 2017 р.). За заг. ред. О. І. Харитонової. Одеса : Фенікс, 2017. С. 4-6.
72. Харитонова О. І., Кулініч О. О., Мазуренко С. В., Менсо І. В. Правове регулювання використання зображень у електронних бібліотеках за законодавством України: монографія. Одеса: Юридична література, 2017. 72 с.
73. Харитонова О. І., Харитонов Є. О. Віртуальна власність та право інтелектуальної власності. *Спогади про Людину, Вченого, Цивіліста-епоху* (до 85-річчя від Дня народження академіка Ярославни Миколаївни Шевченко). За заг. ред. Р. О. Стефанчука. К.: АртЕк, 2017. С.335-347.
74. Харитонова О. І., Харитонов Є. О. Інтернет речей: об'єкт чи суб'єкт правовідносин. ІТ-право та цифрове суспільство: матеріали Всеукр.конференції (м. Одеса, 24 листопада 2017 р.). За заг.ред. Є. О. Харитонова. Одеса: Юридична література, 2017. С. 5-8.
75. Харитонова О. І., Харитонов Є. О. Деякі проблеми правосуб'єктності корпорацій у цифрову добу. *Корпоративне право України та європейських країн: питання теорії та практики*: збірник наукових праць за матеріалами ХУ Міжнародної науково-практичної конференції (6-7 жовтня 2017 р., Івано-Франківськ). За ред. В. В. Луця. Івано-Франківськ, 2017. С.242-246.

2018 р.

76. Актуальні проблеми цивілістики у цифрову добу: онлайнові соціальні мережі : монографія. За ред. Є. О. Харитонова, О. І. Харитонової. Одеса : Юридична література, 2018. 176 с.
77. Давидова І. В. Блокчейн та категорія правочину. *Актуальні проблеми цивілістики у цифрову добу: онлайнові соціальні мережі.* моногр. За ред. Є. О. Харитонова, О. І. Харитонової. Одеса : Юридична література, 2018. С. 59-92.
78. Давидова І. В. Правочини в інформаційному суспільстві: перспективи розвитку. *Visegrad Journal on Human Rights.* 2018. Вип. 2. Частина 2. С. 47-51.

79. Давидова І. В. Правочини в соціальній мережі. *Актуальні проблеми цивілістики у цифрову добу: онлайнові соціальні мережі:* моногр. За ред. Є. О. Харитонова, О. І. Харитонової. Одеса: Юридична література, 2018. С. 65-76.
80. Давидова І. В. Правочини та їх недійсність в інформаційному суспільстві: теорія і практика: моногр. Одеса: Юридична література, 2018. 368 с.
81. Давидова І. В. Трансформації розуміння категорії «правочин» в інформаційному суспільстві. *Visegrad Journal on Human Rights.* 2018. Вип. 3. Частина 2. С. 59-63.
82. Некіт К. Г. Акаунт у соціальній мережі як об'єкт цивільних правовідносин. *Актуальні проблеми цивілістики у цифрову добу : онлайнові соціальні мережі* : моногр. За ред. Є. О. Харитонова, О. І. Харитонової. Одеса : Юридична література, 2018. С. 77-92.
83. Некіт К. Г. Деякі правові проблеми інтернету речей і напрями їх вирішення. *Часопис цивілістики.* 2018. № 31. С. 54-58.
84. Некіт К. Г. Деякі проблеми акаунтів у соціальних мережах як об'єктів цивільного обігу. *Вісник Південного регіонального центру Національної академії правових наук України.* 2018. № 16. С. 91-97.
85. Некіт К. Г. Поняття та правова природа акаунту в соціальній мережі. *Часопис цивілістики.* 2018. № 30. С. 60-66.
86. Некіт К. Г. Правовий статус криптовалют в Україні та у світі. *Юридичний науковий електронний журнал.* 2018. № 1. http://lsej.org.ua/1_2018/12.pdf
87. Некіт К. Г. Світові підходи до визначення правового статусу криптовалют. *Часопис цивілістики.* 2018. № 29. С. 100-106.
88. Некіт К. Г. Суб'єкти права приватної власності в інформаційному суспільстві. *Lex Portus.* 2018. № 2. С. 128-141.
89. Харитонов Є. О. Деякі цивілістичні проблеми «Інтернету речей». *Правові та інституційні механізми забезпечення розвитку України в умовах Європейської інтеграції:* Матеріали Міжнародної науково-практичної конференції. Одеса, 18 травня 2018 р.). Одеса, Гельветика, 2018. С. 530-534.
90. Харитонов Є. О., Давидова І. В. Категорії правочину: від римського negotium до «ІТ-правочину». *Часопис цивілістики.* 2018. Вип. 29. С. 89-94.
91. Харитонов Є. О., Харитонова О. І. Інформаційне суспільство, громадянське суспільство та приватне право: питання співвідношення. *Часопис цивілістики.* 2018. № 28. С. 8-13.

2019 р.

92. Бааджи Н. П. Можливості штучного інтелекту у боротьбі з плагіатом. *Рекодифікація цивільного законодавства і системи права України у контексті євроінтеграційних процесів:* матер.всеукр. науково-практичн. конф.(Одеса, 8-9 листопада 2019 р.). За заг. ред. Є. О. Харитонова. Одеса: Фенікс, 2019. С. 86-92.

93. Давидова І. В. Використання інформаційних технологій як гарантія інформаційної безпеки при створенні юридичних осіб. *Часопис цивілістики.* 2019. Вип. 35. С. 55-59.
94. Davydova I., Buletsa S., Kharytonov E. Prospects of Blockchain Technology and Smart Contracts in the Medical Sphere. Education Excellence and Innovation Management: A 2025 Vision to Sustain Economic Development during Global Challenges. (nov. 13-14, 2019). P. 11980-11989.
95. Davydova I., Orzikh Y., Samoylenko G., Andronov I., Pysarenko M. Legal Consequences of the Invalidity of a Transaction made by Using Information Technology: Problems of Theory and Practice. *Revista Amazonia Investiga.* Vol. 8 Núm. 19 /Marzo – abril 2019. URL: https://www.amazoniainvestiga.info/index.php/amazonia/article/view/276/253
96. Davydova I., Bernaz-Lukavetska O., Fedenko Y. Separate aspects of image rights using in holograms: world experience and problems of ukrainian legal regulation. *Revista Amazonia Investiga.* Vol. 8 Núm. 23 /Noviembre – diciembre 2019. P. 269-277. URL: https://amazoniainvestiga.info/index.php/amazonia/article/view/869/812
97. Інформаційна безпека: проблеми приватного права : навчальний посібник. За ред.. Є. О. Харитонова. Одеса: Юридична література, 2019. 194 с.
98. ІТ-право: теорія та практика: *навч. посібн.* За заг. ред. Є. О. Харитонова, О. І. Харитонової. 2-ге видан., виправлене та доповнене. Одеса: Фенікс. 2019. 472 с.
99. Некіт К. Г. Віртуальна власність: поняття та сутність. *Право і суспільство.* 2019. № 2. С. 37-42.
100. Некіт К. Г. Довірча власність як спосіб забезпечення виконання зобов'язань за цивільним законодавством України: оцінка ризиків *Часопис цивілістики.* 2019. № 35. С. 28-35.
101. Некіт К. Г. Деякі правові проблеми інтернету речей і напрями їх вирішення. *Часопис цивілістики.* 2019. № 31. С. 54-58.
102. Некіт К. Г. Особливості змісту та здійснення права віртуальної власності. Часопис цивілістики . 2019. № 32. С. 86-92.
103. Некіт К. Г. Віртуальна власність крізь призму теорій права власності. *Часопис цивілістики* . 2019. № 33. С. 78-82.
104. Харитонов Є. О. «Інтернет правовідносини» та інформаційна безпека. *Інформаційна безпека: проблеми приватного прав*а: навчальний посібник. За ред.. Є. О. Харитонова. Одеса: Юридична література, 2019. С. 101-111.
105. Харитонов Є. О. Види піратства в Інтернеті. *Інформаційна безпека: проблеми приватного права*: навчальний посібник. За ред. Є. О. Харитонова. Одеса: Юридична література, 2019. С. 54-56.
106. Харитонов Є. О. Забезпечення інформаційної безпеки як основний напрямок державної інформаційної політики. *Інформаційна безпека: проблеми приватного права*: навчальний посібник. За ред.. Є. О. Харитонова. Одеса: Юридична література, 2019. С.63-67.

107. Харитонов Є. О. Загрози інформаційній безпеці. *Інформаційна безпека: проблеми приватного права*: навчальний посібник. За ред. Є. О. Харитонова. Одеса: Юридична література, 2019. С. 47-50.
108. Харитонов Є. О. Інформаційна безпека та ІТ – сфера. *ІТ – право: теорія та практика*: навч. посібн. За ред. Є. О. Харитонова, О. І. Харитонової. 2-ге видан., виправлене та доповнене. Одеса: Фенікс, 2019. 52-82.
109. Харитонов Є. О. Інформаційне суспільство, соціальне управління та ІТ. *ІТ – право: теорія та практика*: навч. посіб. За ред. Є. О. Харитонова, О. І. Харитонової. 2-ге видан., виправлене та доповнене. Одеса: Фенікс, 2019. С. 10-31.
110. Харитонов Є. О. Інформаційні технології та право. *ІТ – право: теорія та практика*: навч. посіб. За ред. Є. О. Харитонова, О. І. Харитонової. 2-ге видан., виправлене та доповнене. Одеса: Фенікс, 2019. С. 32-51.
111. Харитонов Є. О. Інформаційні технології як виклик приватному праву. *Цивілістика в інформаційному суспільстві*: матер. Всеукр. круглого столу (Одеса, 17 травня 2019 року). За заг. ред. Є. О. Харитонова. Одеса: Фенікс, 2019. С. 5-8.
112. Харитонов Є. О. Інформація, безпека та приватне право. *Інформаційна безпека: проблеми приватного права:* навчальний посібник. За ред. Є. О. Харитонова. Одеса: Юридична література, 2019. С.7-15.
113. Харитонов Є. О. Концепт самодостатності ІТ – сфери та його чинники. *ІТ – право: теорія та практика:* навч. посіб. За ред. Є. О. Харитонова, О. І. Харитонової. 2-ге видан., виправлене та доповнене. Одеса: Фенікс, 2019. С. 83-88.
114. Харитонов Є. О. Поняття піратства в Інтернеті та його основні ознаки. *Інформаційна безпека: проблеми приватного права*: навчальний посібник. За ред. Є. О. Харитонова. Одеса: Юридична література, 2019. С. 50-54.
115. Харитонов Є. О. Правосуб'єктність учасників ІТ – відносин. *ІТ – право: теорія та практика:* навч. посіб. За ред. Є. О. Харитонова, О. І. Харитонової. 2-ге видан., виправлене та доповнене. Одеса: Фенікс, 2019. С. 143-150.
116. Харитонов Є. О. Технічні засоби кіберзахисту. *Інформаційна безпека: проблеми приватного права:* навчальний посібник. За ред. Є. О. Харитонова. Одеса: Юридична література, 2019. С. 128-132.
117. Kharytonov E. Human rights as the basic value of the concept of private law in modern Europe. Amazonia Investiga, 8(20). P.477-485. (in co-authorship with Kharytonova O., Kharytonova T., Kolodin D., Tolmachevska Y.)
118. Kharytonov E. Kharytonova, O. Human rights, civil society, private law: correlation problems. Ius Humani. LawJournal.2019. Vol. 8. P.225-244.
119. Kirilyuk A. V., Baadzhy N. P. Civil Law Ways to Protect Rights on the Internet. *Amazonia Investiga*. 2019. 8(22).
120. Kyryliuk A., Baadzhy N., Honhalo R., Kapustina N., Galupova L. Protection of copyright on the Internet. *Amazonia Investiga*. ESCI Web of Science. 2019. 8(24). Nekit K. Ulianova G. Kolodin D. Website as an object of legal protection by Ukrainian legislation. *Amazonia investiga*. 2019. Vol.8. № 21. P. 222-230.

121. Харитонов Є. О., Толмачевська Ю. О. Кіберспорт як сфера цивільно-правового регулювання. *Часопис цивілістики.* 2019. № 32. С. 72-75.
122. Харитонов Є. О., Харитонова О. І. Віртуальна власність. *IT – право: теорія та практика:* навч. посіб. За ред. Є. О. Харитонова, О. І. Харитонової. 2-ге видан., виправлене та доповнене. Одеса: Фенікс, 2019. 212-222.
123. Харитонов Є. О., Харитонова О. І. Приватне право як концепт. Том ІІІ. Концепт приватного права і рекодифікації цивільного законодавства в Україні: рефлексії фронтиру : монографія. Одеса : Фенікс, 2019. 752 с.
124. Харитонов Є. О., Харитонова О. І. Проблеми відшкодування майнової шкоди у сфері використання інформаційних технологій. *Спогади про Людину, Вченого, Цивіліста* (до 90-річчя від Дня народження професора Діни Василівни Боброової); за заг. ред. Р. О. Стефанчука. К.: АртЕк, 2019. С.275-287.
125. Харитонов Є. О., Харитонова О. І. Цивілістичні категорії доби інформаційного суспільства у національній доктрині приватного права: правовідносини. *Право України.* 2019. № 1. С. 136-153.
126. Харитонова О. І. Інтелектуальна власність та інформаційна безпека. *Інформаційна безпека: проблеми приватного права*: навчальний посібник. За ред. Є. О. Харитонова. Одеса: Юридична література, 2019. С. 180-195.
127. Харитонова О. І. Цивільно-правовий захист та охорона авторських і суміжних прав від піратства в Інтернеті. *Інформаційна безпека: проблеми приватного права*: навчальний посібник. За ред. Є. О. Харитонова. Одеса: Юридична література, 2019. С. 94-99.
128. Харитонова О. І., Харитонов Є. О. Дещо про симулякри, нову реальність і політичні процеси в Україні. *Актуальні проблеми інтелектуального, інформаційного та IT права:* матеріали третьої всеукраїнської науково-практичної конференції (Львів, 17-18 травня 2019 р.). Львів: Юрид. ф–т Львів. нац. ун–ту ім. І. Франка, 2019. С. 176–191.

2020 р.

129. Давидова І. В. Визначальна роль електронного підпису як цивільної ідентифікації особи в умовах карантину. *Часопис цивілістики.* 2020. Вип. 38. С. 69-74.
130. Давидова І. В. Правосвідомість та вчинення правочинів: особливості взаємозв'язку в умовах розвитку інформаційного суспільства. *Часопис цивілістики.* 2020. Вип. 37. С. 88-92.
131. Davydova I., Bernaz-Lukavetska O., Reznichenko S. Certain aspects of personal data protection in the social network: european experience and legislative regulation in Ukraine. *Revista Amnazonia Investiga.* Vol. 9 Núm. 27 /March 2020. P. 383-390.
132. Кирилюк А. В. Відповідальність штучного інтелекту. *Правове життя сучасної України* : у 3 т.: матеріали Міжнар. наук.-практ. конф. (м. Одеса, 15 трав. 2020 р.). Одеса: Гельветика, 2020. Т. 3. С. 511-514.

133. Кирилюк А. В. Досвід США у сфері захисту авторських прав в мережі Інтернет. *Права людини – пріоритет сучасної держави* : Всеукраїнська науково-практична Інтернет конференція, 10 грудня 2020 року, м. Одеса: збірник матеріалів конференції. Одеса: Гельветика, 2020. С. 221-226.
134. Некіт К. Г. Користувацька угода (Terms of Service) як підстава виникнення права власності на віртуальне майно. *Право та інновації.* 2020. № 4. С. 62-68.
135. Некіт К. Г. Переваги та недоліки смарт-контрактів як підстав виникнення права власності. *Вісник Національного технічного університету України «Київський політехнічний інститут».* 2020. №. 3(47). С. 101-105.
136. Некіт К. Г. Персональні дані та індустріальні дані як об'єкти права власності: оцінка можливостей. *Часопис цивілістики.* 2020. № 36. С. 57-65.
137. Nekit K. Fiduciary management of a social media account. *Trusts & Trustees.* 2020. Volume 26. Issue 4. P. 295–302, https://doi.org/10.1093/tandt/ttaa016
138. Nekit K. Legal aspects of the use of social media accounts: current state and perspectives. *The Lawyer Quarterly.* 2020. Vol. 10. № 3. P. 305-323
139. Nekit K. Social media account as an object of virtual property. *Masaryk University Journal of Law and Technology.* 2020 № 14(2). P. 201-226. https://doi.org/10.5817/MUJLT2020-2-3
140. Nekit K. The theoretical foundations for the recognition of virtual property as a type of ownership. *Current issues of recodification of Ukrainian civil legislation: collective monograph.* Lviv-Torun: Liha-Pres, 2020. P. 76-91.
141. Nekit K., Kolodin D., Fedorov V. Personal data protection and liability for damage in the field of the Internet of Things. *Juridical Tribune.* 2020. Vol. 10, Issue 1. P. 80-93.
142. Nekit K., Tokareva V., Zubar V. Artificial intelligence as a potential subject of property and intellectual property relations. *Ius Humani. Law Journal.* 2020. 9 (1), 231-250. https://doi.org/https://doi.org/10.31207/ih.v9i1.227
143. Розумейко Д. О. Цивільно-правові відносини та цивільне законодавство у сфері стартапів. *Теоретичні та практичні аспекти розвитку науки та освіти* : матеріали ІІ Міжнародної науково-практичної конференції, (Львів, 15-16 верес. 2020). Львів : Львівський науковий форум, 2020. С. 83-84.
144. Харитонов Є. О. Право інформаційних технологій. *Енциклопедія соціогуманітарної інформології.* Коорд. проекту та заг. ред. проф. К. І. Бєляков. Київ: Гельветика, 2020. Т. 1. С. 190-194.
145. Kharytonov E., Kharytonova O., Bignyak O. Property rights in the information age. 2020. Espacois, 41(10), 7.
146. Kharytonov E., Kharytonova O., Davydova I. La formación de un componente práctico y teórico-práctico del proceso educativo en el contexto de la reforma de la educación jurídica en Ucrania. Revista Dilemas contemporáneos: *Educación, Política y Valores.* 2020. № 2 (49). URL: https://www.dilemascontemporaneoseducacionpoliticayvalores.com/index.php/dilemas/article/view/2005
147. Kharytonov E., Kharytonova O., Kostruba A., Tkalych M., Tolmachevska Y. Las peculiaridades de la regulación legal y no legal de las relaciones sociales en el

ámbito del deporte (To the Peculiarities of Legal and Non-Legal Regulation of Social Relations in the Field of Sport). *Retos.* 2020. 41. 131-137.

148. Kyryliuk A., Lysenko V., Podolieva A. Bloggers, Copyrights and Some Other Legal Issues. Ius Humani. *Law Journal.* 2020. 9(2). 421-446. https://doi.org/https://doi.org/10.31207/ih.v9i2.262

2021 р.

149. Берназ-Лукавецька О. До питання про підтримку малого та середнього бізнесу у боротьбі з пандемією COVID 19: світовій досвід. *Юридичний вісник.* 2021. № 4. С. 143-149.
150. Давидова І. В., Берназ-Лукавецька О. М. Блокчейн як засіб безпечного укладення правочинів в умовах COVID-19: *Приватні та публічні інтереси в умовах пандемії COVID-19: колізії та правові шляхи вирішення:* монографія; За ред. Є. О. Харитонова, О. І. Харитонової, С. Б. Булеци. Одеса: Гельветика, 2021. С. 167-181.
151. Davydova I., Tokareva V., Bernaz-Lukavetska O., Andriienko I., Tserkovna O. Freedom of contract in the digital age and its implementation in modern technologies: theory and practice. *International Journal of Computer Science and Network Security*, VOL.21 No.12, December 2021. P. 544-548. URL: http://paper.ijcsns.org/07_book/202112/20211275.pdf
152. Кирилюк А. В. Форми та види захисту авторських прав у мережі Інтернет. *Наука та суспільне життя України в епоху глобальних викликів людства у цифрову еру* (з нагоди 30-річчя проголошення незалежності України та 25-річчя прийняття Конституції України): у 2 т.: матеріали Міжнар. Наук.-практ. конф. (м. Одеса, 21 травня, 2021 р.). Одеса: Гельветика, 2021. Т. 2. С. 493-497.
153. Kolomoiets T., Tkalych M., Melnyk P., Panchenko B., Tolmachevska, Y. Combating Corruption in Sport: Legal Aspect. *Retos.* 2021. 41. 746-755.
154. Некіт К. Г. Право приватної власності в інформаційному суспільстві: теорія і практика: монографія. Одеса: Гельветика, 2021. 554 с.
155. Некіт К. Г. Цифрові дані та інформація як об'єкти права власності. *Часопис цивілістики.* 2021. № 42. С. 38-44.
156. Розумейко Д. О. Криптовалюта – Нова ера. *Шерешевські читання : Проблеми цивілістики в умовах пандемії та ІТ :* матеріали Всеукраїнської наукової конференції (Одеса, 10 груд. 2021).За ред. Є. Харитонов. Одеса : Фенікс, 2021. С. 192–194.
157. Ткалич М. О., Толмачевська Ю. О. Санкції у спорті: міжнародно-правовий досвід. *Lex Sportiva.* 2021. № 1. С. 34–37.
158. Толмачевська Ю. О. правове регулювання сфери кіберспорту: загальні положення. *Lex Sportiva.* 2021. № 2. С. 27-31.
159. Kharytonov E., Kharytonova O., Tkalych M., Bolokan I., Samilo H., Tolmachevska, Y.: Intellectual Property Law in the Field of Sports: Specifics

of Manifestations and Features of Legal Regulation. *Cuestiones Políticas.* 20210. 39(69), 530-546.
160. Харитонов Є. О. COVID-19 та проблеми інформаційної безпеки. *Цивілістичні проблеми інформаційної безпеки в умовах COVID-19* : матеріали Всеукр. круглого столу, Одеса, 21 червня 2021 р. За заг. ред. Є. О. Харитонова, д.ю.н., проф. І. В. Давидової. Одеса : Фенікс, 2021. С. 5-9.
161. Харитонов Є. О., Харитонова, О. І., Толмачевська Ю. О. Використання штучного інтелекту у спорті: проблеми і перспективи. *Lex Sportiva.* 2021. № 1. С. 38-45.

2022 р.

162. Берназ-Лукавецька О. М. Проблемні питання виконання окремих видів договорів в умовах воєнного стану. *Юридичний науковий електронний журнал.* 2022. № 7. С. 527-529.
163. Галупова Л. І. Захист прав інтелектуальної власності в умовах воєнного стану. *Європейський вибір України, розвиток науки та національна безпека в реаліях масштабної військової агресії та глобальних викликів XXI століття* (до 25-річчя Національного університету «Одеська юридична академія» та 175-річчя Одеської школи права) : у 2 т. : матеріали Міжнар.наук.-практ. конф. (м. Одеса, 17 червня 2022 р.). Одеса: Гельветика, 2022. Т. 2. С. 745-749.
164. Галупова Л. І. Авторські права на твори, створені за допомогою штучного інтелекту. *Міжнародна транспортна інфраструктура, індустріальні центри та корпоративна логістика*: вісімнадцята науково- практична конференція (2-3 червня 2022 р. Харків.) С.220-222.
165. Галупова Л. І. Врегулювання транскордонний конфліктів щодо прав інтелектуальної власності за допомогою приватних процедур. *Приватне право в умовах війни* : матеріали всеукр. наук. конф. (Одеса, 15 листоп. 2022 р.). За заг. ред.: Є. Харитонова, І. Давидової. Одеса, 2022. С. 84-88.
166. Давидова І. В. Місце смарт-контрактів серед цивільно-правових договорів. *Часопис цивілістики.* 2022. Вип. 46. С. 46-51.
167. Давидова І. В., Берназ-Лукавецька О. М. Е-ідентифікація особи в умовах імплементації законодавства Європейського Союзу. *Південноукраїнський правничий часопис.* 2022. № 4. Т. 1. С. 213-219.
168. Davydova I., Harhan S. Compensation for damages caused in violation of information security. *Дніпровський науковий часопис публічного управління, психології, права.* 2022. Вип. 1. С. 93-97.
169. Davydova I., Nahnybida V., Adamova O., Zhurylo S. Tokareva V. Blockchain and Civil Proceedings: Points of Convergence. *Dixi*, 2022. Vol. 25, Num. 1. P. 1-20.
170. Davydova I., Zhurylo S., Tserkovna O., Herasymchuk L., Tokareva V. Virtual Assets as the Newest Object of Property Rights. International Journal of Computer Science and Network Security. 2022. VOL.22 № 5, May. P. 115-120.

171. Кирилюк А. В. Міфи щодо безкарності порушення авторських прав у мережі Інтернет. *Римське право і сучасність: цивільне право в умовах війни:* мат. всеукраїнської наукової конференції (м. Одеса, 24 травня, 2022 року). За заг. ред. О. І. Харитонової, К. Г. Некіт. Одеса: Фенікс, 2022. С.84-88.
172. Кирилюк А. В. Теоретичні положення захисту авторських прав в мережі Інтернет. *Європейский вибір України, розвиток науки та національна безпека в реаліях масштабної військової агресії та глобальних викликів XXI століття* (до 25-річчя Національного університету «Одеська юридична академія» та 175-річчя Одеської школи права) : у 2 т.: матеріали Міжнар. Наук.-практ. конф. (м. Одеса, 21 травня, 2022 р.). За ред.. С. В. Ківалова. Одеса: Гельветика, 2022. С.731-735.
173. Некіт К. Г. Віртуальні активи як різновид цифрових речей. *Часопис цивілістики.* 2022. № 45. С. 53-58.
174. Некіт К. Г. Напрями змін у правовому регулюванні обігу криптоактивів: аналіз зарубіжного досвіду. *Економіка і право.* 2022. № 1(64). С. 33-44.
175. Некіт К. Г. Проблеми захисту персональних даних в умовах вакцинації від COVID-19. *Вакцинація від COVID-19: соціальні та правові проблеми* : монографія. За ред. Є. О. Харитонова, О. І. Харитонової, К. Г. Некіт. Одеса: Гельветика, 2022. С. 258-282.
176. Некіт К. Г. Розвиток правового регулювання обігу віртуальних активів (криптовалют) в Україні. *Часопис цивілістики.* 2022. № 44. С. 45-51.
177. Nekit K. Legal approaches to solving security issues in the field of the Internet of Things in the light of European integration of Ukraine. *Південноукраїнський часопис.* 2022. № 4. С. 230-235.
178. Розумейко Д. О. Сучасні реалії віртуальних активів. *Римське право і сучасність: цивільне право в умовах війни :* матер. Всеукр. наук. конф., (Одеса, 24 трав. 2022). За ред. Є. О. Харитонов. Одеса : Фенікс, 2022. С. 120–123.
179. Токарева В. О. Щодо визначення персональних даних в умовах Євроінтеграційних процесів. *Південноукраїнський правничий часопис.* 2022. № 4. Том 3. С. 169-174.
180. Токарева В. О. Щодо питання цифрової ідентичності у мережі Інтернет. *Публічне та приватне право.* 2022. № 4. С. 35-40.
181. Фєдосов Д. В., Толмачевська Ю. О. Особливості оподаткування кіберспортивної діяльності в Україні. *Lex Sportiva.* 2022. № 1. С. 25–29.
182. Харитонов Є. О., Харитонова О. І. Віртуальний світ, віртуальна особистість і симулякри. *Цифрова трансформація та цифрова економіка в умовах воєнного стану: аспекти інтелектуальної власності.* Збірник матеріалів V Всеукр. наук.-практ. конф. з проблем економіки інтелектуальної власності (27 травня 2022 р., Київ). К.: Науково-дослідний інститут інтелектуальної власності НАПрН України, 2022.С. 225-229
183. Харитонов Є. О., Харитонова О. І., Толмачевська Ю. О. Використання штучного інтелекту у спорті: проблеми і перспективи. *Lex Sportiva.* 2022. (1), 38–45.

184. Харитонова О. І. Крипто-арт, NFT та інтелектуальна власність. *Європейський вибір України, розвиток науки та національна безпека в реаліях масштабної військової агресії та глобальних викликів XXI століття* (до 25-річчя Національного університету «Одеська юридична академія» та 175-річчя Одеської школи права): у 2 т. : матеріали Міжнар.наук.-практ. конф. (м. Одеса, 17 червня 2022 р.). Одеса : Гельветика, 2022. Т. 2. С. 717-719.
185. Kharytonov E., Kharytonova O., Kolodin D., Tkalych M., Larkin M., Tolmachevska Y., Rojas-Bahamon M. J., Arbelaez-Campillo D. F., Panchenko O. I. Distance learning in the conditions of Covid-19: problems and prospects of their solutions. *AMAZONIA INVESTIGA*. Volume 10. Issue 48. P. 157-169. 2022.
186. Kharytonov E., Kostruba A., Davydova I. Sistema monetario digital y relaciones sociales: realidades jurídicas y perspectivas del mecanismo de implementación. Revista De La Universidad Del Zulia. 2022. 13(38), 3-7.

2023 р.

187. Берназ-Лукавецька О. М. Кірсанов О. В. Проблемні аспекти кредитних договорів в Україні та міжнародному просторі. *Морська безпека та оборона.* 2023. № 2. С. 7-12.
188. Берназ-Лукавецька О. М. Цивільно-правове регулювання страхових відносин. *Правова позиція.* 2023. № 3 (40). С. 103-106.
189. Галупова Л. І. Захист авторських прав на контент, розміщений в соціальних мережах. *Європейські орієнтири розвитку України в умовах війни та глобальних викликів XXI століття: синергія наукових, освітніх та технологічних рішень:* у 2 т.: матеріали Міжнар. Наук.-практ. конф. (19 травня 2023, м. Одеса). За заг. ред. С. В. Ківалова. Одеса: Юридика, 2023. Т. 2. С. 584-588.
190. Галупова Л. І. Проблеми захисту авторських прав у цифровому середовищі. *Шерешевські читання: представництво в умовах надзвичайних ситуацій :* матер. Круглого столу (Одеса, 15 груд. 2023 р.) За заг. ред.: Є. Харитонова, І. Давидової. Одеса : Фенікс, 2023. С. 33-36.
191. Давидова І. В. Правочини в умовах воєнного стану (розділ 5). *Проблеми здійснення та захисту цивільних прав в умовах воєнного стану*: моногр. За ред. Харитонова Є. О., Харитонвої О. І., Некіт К. Г. 2023. С. 113-122.
192. Davydova I., Zhurylo S., Havrik R., Yakymchuk S., Samilo H. Implementing artificial intelligence in civil procedure and legal education: challenges and perspectives. *Revista Educacion*, 2023. Vol. 17 Núm. 4. P. 154-164.
193. Калітенко О. М. Самоврегулювання в сфері цифрового спадкування: окремі аспекти. *Юридичний вісник.* 2023. № 4. С. 38-44.
194. Кирилюк А. В. Світовий досвід вирішення спорів з інтелектуальної власності. *Європейські орієнтири розвитку України в умовах війни та глобальних викликів XXI століття: синергія наукових, освітніх та технологічних рішень*: у 2 т.: матеріали Міжнар. наук.-практ. конф. (19 травня 2023, м. Одеса). За заг. ред. С. В. Ківалова. Одеса: Юридика, 2023. Т. 2. С. 592-596.

195. Кирилюк А. В., Галупова Л. І. Судова юрисдикція у сфері захисту прав інтелектуальної власності: міжнародний аспект. *Правові новели.* 2023. № 21. С. 238-244.
196. Nekit K. Legal nature and types of digital assets in the activities of technology-oriented startups. *Juridical Tribune.* 2023. Vol. 13. Issue 2. P. 304-326.
197. Nekit K. Legal nature of a smart-contract and issues of its application in the field of digital assets. *Економіка та право.* 2023. № 1. С. 53-61.
198. Сафончик О. І. Актуальні питання цивільно-правового захисту та охорони персональних даних в мережі інтернет за законодавством України. *Юридичний вісник.* № 5. 2023. С. 93-99.
199. Токарева В. О. До питання прийняття рішень із застосування алгоритмів. *Публічне та приватне право.* 2023. № 1. С. 30-35.
200. Токарева В. О. Правове регулювання використання алгоритмів для прийняття юридично значущих рішень. *Часопис цивілістики.* 2023. № 49. С. 32-37.
201. Толмачевська Ю. О. Цивільно-правові договори в сфері кіберспорту : дис… доктора філос. 081 «Право». Одеса, 2023. 240 с.
202. Толмачевська Ю. О. Цивільно-правові договори у кіберспорті: правовий аналіз. *Lex Sportiva.* 2023. № 1. С. 28-34.
203. Ульянова Г. О., Галупова Л. І., Кирилюк А. В. Виконання умови угоди за результатами медіації у сферіінтелектуальної власності в умовах надзвичайного стану. *Юридичний науковий електронний журнал.* 2023. № 2. С. 723-726.
204. Харитонова О., Харитонов Є. Категорії нової реальності: цифрова людина, цифрова особа, цифрова особистість та цифрова ідентичність: до проблеми співвідношення. *Правове регулювання цифрової економіки та штучного інтелекту: національний та міжнародний виміри:* матеріали міжнародної науково-практичної конференції 16 листопада 2023 р.; Науково-дослідний інститут інтелектуальної власності НАПрН України. К. : Інтерсервіс, 2023. 308 с.
205. Харитонова О. І., Харитонов Є. О. Цифрова людина, цифрова особа та цифрова особистість: до проблеми співвідношення. *Часопис цивілістики.* 2023. № 49. С. 5-13.

2024 р.

206. Бааджи Н. П. Використання торговельної марки в мережі Інтернет. *Юридичний науковий електронний журнал.* 2024. № 1. С. 750-755.
207. Берназ-Лукавецька О. М. Кірсанов О. В. Comparative analysis of the credit agreement and factoring agreement. *Морська безпека та оборона.* 2024. № 1. С. 3-8.
208. Берназ-Лукавецька О. М., Наумов А. С. До питання загальних засад договору підряду за законодавством України. *Юридичний науковий електронний журнал.* 2024. № 9. С. 60-63.

209. Берназ-Лукавецька О. М. Щодо виконання окремих видів договорів про надання послуг укладених за допомогою ІТ. *Часопис цивілістики.* 2024. № 55. С. 37-41.
210. Давидова І. В. Банківські договори: особливості в умовах дії воєнного стану. *Часопис цивілістики.* 2024. Вип. 54. С. 37-42.
211. Давидова І. В. Від правочину до гіг-контракту. *Часопис цивілістики.* 2024. Вип. 52. С. 56-59.
212. Давидова І. В., Токарева В. О. Цифрова нерівність та право на доступ до Інтернету. *Юридичний вісник.* 2024. № 6. С. 68-75.
213. Didenko L., Izbash O., Kyryliuk A., Halupova L., Denysiak N. Intellectual property rights issues in the digital era: Cuestiones de derechos de propiedad intelectual en la era digital. Cuestiones Políticas. 2024. 42(80), 136-158.
214. Калітенко О. М. До питання про перспективи розвитку договору онлайн кредитування у цифровому світі. *Юридичний науковий електронний журнал.* 2024. № 2. С. 103-105.
215. Кирилюк А. В. Основні концепції об'єків інтернет-правовідносин. *Європейські орієнтири розвитку України: науково-практичний вимір в умовах воєнних викликів*: матеріали Міжнар. наук.-практ. конф. (Одеса, 26 квітня 2024 р.). За заг. ред. С. В. Ківалова. Одеса: Фенікс, 2024. С. 667-670.
216. Nekit K. Digital ownership as a reflection of the Rule of Law. Rule of Law in a transitional spectrum. Ed. by Rigmor Argren. Uppsala: *Iustus.* 2024. 470 p. P. 405-439.
217. Nekit K. Terms of Service as a new type of contract: approaches to legal regulation and issues to be solved. *Часопис цивілістики.* 2024. № 52. С. 60-66.
218. Nekit K. The (im)possibility of personal and industrial (machine-generated) data to be subject to property rights. International Journal of Law and Information Technology. Volume 32, Issue 1, 2024, P. 1-16.
219. Розумейко Д. О. Еволюція стартапів: історичний розвиток та ключові етапи становлення. *Інтеграція світових наукових процесів як основа суспільного прогресу* : матеріали VIII Міжнародної науково-практичної конференції (Київ, 29-30 листоп. 2024). Київ–Запоріжжя: АА Тандем, 2024. С. 60-63.
220. Розумейко Д. О. Стартап як суб'єкт права: правові аспекти організації. *Роль інновацій в трансформації образу сучасної науки* : матеріали VIII Міжнародної науково-практичної конференції, Київ, Україна, 27–28 груд. 2024. Київ–Запоріжжя: АА Тандем, 2024. С. 81-84.
221. Сафончик О. І. Загальна характеристика цивільних правовідносин в сфері інформаційних технологій. *Юридичний вісник.* № 2. 2024. С.45-51.
222. Сафончик О. І. Окремі аспекти договору як підстави виникнення зобов'язань у цифрову добу. *Юридичний вісник.* № 5. 2024. С.92-97.
223. Харитонова О. Актуальні проблеми штучного інтелекту в праві інтелектуальної власності. *Юридичний вісник.* 2024. № 5. С. 121-129.
224. Харитонова О., Харитонов Є. Інформаційна безпека як один з чинників національної безпеки України: загрози під час війни. *Незалежність України:*

права людини та національна безпека : збірник матеріалів Четвертої міжнародної науково-практичної конференції (Львів, 12 квітня 2024 року). Київ : КНТ, 2024. С. 53-56.
225. Харитонова О., Харитонов Є. Віртуальний світ, віртуальна ідентичність, симулякри та гібридна війна. *Цифрова трансформація в Україні: ШІ, метавсесвіт і суспільство 5.0. Наукова апробація.* Монографія . Відредаговано: Олексій Костенко, канд. в праві Юрій Єхануров, канд. в економіці SciFormat Publishing Inc. Канада, 2024 рік . С. 14-20.
226. Харитонова О. І., Кирилюк А. В., Галупова Л. І. Правові аспекти використання творів, створених штучним інтелектом. *The 23rd International scientific and practical conference "World ways and methods of improving outdated theories and trends"* (June 11 – 14, 2024) Zagreb, Croatia. International Science Group. 2024. С. 143-146
227. Харитонова О. І., Харитонов Є. О. Телемедицина в Україні: правові проблеми та перспективи. Цивільно-правове регулювання медичних відносин в умовах війни : матер. Всеукр. кругл.столу (Одеса, 15 листоп. 2024 р.). За ред.: Є. Харитонова, Ю. Кривенко. Одеса : Фенікс, 2024. 74 с.

2025 р.

228. Давидова І. В. До питання про використання технології блокчейн в медичній сфері. *Юридичний вісник.* 2025. № 1. С. 38-43.
229. Давидова І. В., Токарева В. О. Ідентифікація та автентифікація особи: вітчизняний та зарубіжний досвід. *Часопис цивілістики.* 2025. Вип. 56. С. 58-63.
230. ІТ-право: практ. посіб. За ред. Харитонова Є. О.; Спасової К. І. Київ. Норма права. 2025. 264 с.
231. Калітенко О. М. Інформаційне середовище, як стратегічний ресурс у гібридних конфліктах. *ІТ-право та кібербезпека в умовах гібридної війни* : матеріали Всеукр. круглого столу (м. Одеса, 12 квіт. 2025 р.). За заг. ред.: Є. Харитонова, Ю. Кривенко. Одеса: Фенікс, 2025. С. 52-55.
232. Кирилюк А. В., Галупова Л. І. Людиноцентристський підхід у сфері захисту прав інтелектуальної власності. *The 6th International scientific and practical conference "Motivation of professional activity of pedagogical workers"* (February 11 – 14, 2025) Tallinn, Estonia. International Science Group. 2025. 283 p. С. 110-114.
233. Некіт К. До питання про (не)ефективність сучасного підходу до врегулювання відносин щодо цифрових активів для захисту прав їх володільців. *Цивілістична платформа.* 2025. № 1(4). С. 60-71.
234. Некіт К. Г. Система правових проблем у сфері Інтернету речей. «Розумні речі» як об'єкти права власності: проблеми правового регулювання. Правовий статус криптовалюти у світі. Проблеми правового регулювання криптовалюти як об'єкту права власності в Україні. *Актуальні проблеми цивілістики в інформаційному суспільстві*: монографія. За ред. Є. О. Харитонова, О. І. Харитонової. С. 108-129; С. 139-160.

235. Розумейко Д. О. Юридичні інструменти стартапів: основні види договорів та їх ролі. *Модернізація та інноваційні наукові дослідження* : матеріали Міжнародних науково-практичних конференцій (Київ, 27-28 лют. 2025). Київ–Запоріжжя : АА Тандем, 2025. С. 18–21.
236. Розумейко Д. О. Стартап. ІТ-Право : практичний посібник. Київ : Норма права, 2025. С. 186–200.
237. Сафончик О. І. Окремі аспекти правового регулювання укладання шлюбу онлайн за допомогою застосунку дія в Україні. *Одеські грудневі цивілістичні читання: приватне право, як концепт в умовах війни: людський вимір*: матеріали Всеукр. наук. конф. (Одеса, 12 груд. 2024 р.). За заг. ред.: Є. Харитонова, І. Давидової. Одеса. Фенікс. 2025. С.24-27.
238. Харитонов Є.. Інформаційне суспільство, ІТ-сфера, ІТ-право. *ІТ-право: практ.посіб.* Київ: Норма права, 2025. С. 12-33.
239. Харитонов Є., Харитонова О., Толмачевська Ю. Штучний інтелект та/або кіберзагрози в гібридній війні. *Цифровізація, метавсесвіт, штучний інтелект у контексті захисту прав людини та індивідуальних прав в Україні та світі.* https://sciformat.ca/books/index.php/sf/catalog/book/6.
240. Харитонов Є. О. Інформаційна безпека, Кібербезпека. ІТ-право: практ.посіб. Київ: Норма права, 2025. С. 33-68.
241. Харитонов Є. О., Харитонова О. І. Концепція «комп'ютерної симуляції» як методологічна основа виникнення «віртуальної власності»: практ.посіб. Київ: Норма права, 2025. С. 69-74.
242. Харитонов Є. О., Харитонова О. І. Проблеми застосування штучного інтелекту у контексті захисту прав людини. *Права людини та публічне врядування*: матеріали VIII Міжнародного правничого форуму, м. Чернівці, 30 травня 2025 р. Львів – Торунь : Liha-Pres, 2025. – 456 с. С. 126-129.
243. Харитонова О., Харитонов Є., Харитонова Т., Григорьєва Х. Штучний інтелект як правова категорія. В Костенко Олексій, Харитонова Олена та Харитонов Євген (Ред.), Цифровізація, метавсесвіт, штучний інтелект у контексті захисту прав людини та особи в Україні та світі. 2025. С. 68-89. URL: https://doi.org/10.69635/978-1-0690482-4-0-ch4
244. Харитонова О. І. Віртуальна власність». *ІТ-право:* практ.посіб. Київ: Норма права, 2025. С. 69-94.
245. Харитонова О. І., Харитонов Є. О. Віртуальна (цифрова) власність у світлі рекодифікації речового права. *Рекодифікація речового права* : збірник матеріалів XIV Міжнародного цивілістичного форуму (м. Київ, 16 травня 2025 р.). Одеса : Юридика, 2025. С. 162-167.
246. Харитонова О. І., Харитонов Є. О. Проблеми визначення правового статусу особи у цифровому середовищі. *Проблеми правового регулювання забезпечення особистих немайнових прав особи та прав на віртуальні активи в умовах цифровізації: матеріали Міжнародної науково-практичної конференції (10 травня 2025 р., Ужгород-Піза*). За заг. ред. С. Б. Булеци, М. В. Менджул. Ужгород, 2025. С. 178-181.

247. Харитонова О. І., Харитонов Є. О. Цифрові права: до проблеми питання. *Незалежність України: права людини та національна безпека: збірник матеріалів П'ятої міжнародної науково-практичної конференції (*Львів, 4 квітня 2025 року). За ред. проф. В. Б. Ковальчука, проф. Л. В. Ярмол; Навчально-науковий інститут права, психології та інноваційної освіти Національного університету «Львівська політехніка». Львів-Острог: вид-во ТОВ «4Фемілі», 2025. С. 55-58.

Наукове видання

ІТ-ПРАВО ПІД ЧАС ГІБРИДНОЇ ВІЙНИ: ВІД ПОШУКУ ПАРАДИГМИ ДО ПРАГМАТИЧНИХ РІШЕНЬ

Колективна монографія

За редакцією
Є. Харитонова, О. Харитонової, І. Давидової

В авторській редакції

Підписано до друку 25.07.2025.
Формат 60х84/16. Ум-друк. арк. 34,18.
Наклад 100 прим. Зам. № 2507-05.

Видавець ПП «Фенікс»
(Свідоцтво суб'єкта видавничої справи ДК № 1044 від 17.09.02).
Україна, м. Одеса, 65009, вул. Зоопаркова, 25.
e-mail: fenix-izd@ukr.net