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

ЗМІСТ

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 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 Боброової*; 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/