НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
«ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»

Кафедра цивільного права

ІТ-ПРАВО ТА КІБЕРБЕЗПЕКА В УМОВАХ ГІБРИДНОЇ ВІЙНИ

МАТЕРІАЛИ
Всеукраїнського круглого столу

Одеса,
12 квітня 2025 року

Одеса
Фенікс
2025

УДК 342.95 : 343.32 (477): 351.863
І-52

За загальною редакцією
доктора юридичних наук, професора **Є. Харитонова**,
кандидатки юридичних наук, доцентки **Ю. Кривенко**.

Упорядники-укладачі:
Кривенко Юлія – к.ю.н., доцентка кафедри цивільного права Національного університету «Одеська юридична академія», доцентка;
Лешкова Єлизавета – лаборантка кафедри цивільного права Національного університету «Одеська юридична академія».

ІТ-право та кібербезпека в умовах гібридної війни : матеріали Всеукр. круглого столу (м. Одеса, 12 квіт. 2025 р.) / за заг. ред.: Є. О. Харитонова, Ю. Кривенко ; кафедра цив. права НУ «Одес. юрид. академія». – Одеса : Фенікс, 2025. – 138 с. – Режим доступу: ….

І-52

ISBN 978-617-8430-57-3

Збірник містить матеріали доповідей з теоретичних, історичних і методологічних проблем ІТ-права та кібербезпеки, які були оприлюднені на Всеукраїнському круглому столі «ІТ-право та кібербезпека в умовах гібридної війни» 12 квітня 2025 у Національному університеті «Одеська юридична академія».

Збірник спрямований на ознайомлення громадськості з дослідженнями науковців у сфері ІТ-права та кібербезпеки і може бути корисний як у навчальному процесі, так і в практичній діяльності.

УДК 342.95 : 343.32 (477): 351.863

ISBN 978-617-8430-57-3

Харитонов Євген Олегович,
доктор юридичних наук, професор, член-кореспондент НАПрН України,
зав. кафедри цивільного права Національного університету
«Одеська юридична академія»

ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ У РОСІЙСЬКО-УКРАЇНСЬКІЙ ВІЙНІ: ПРАВОВІ ПРОБЛЕМИ

Сутність російсько-українського конфлікту як «гібридної» війни охарактеризована у позиції Міністерства закордонних справ України наступним чином: «Збройна агресія є лише одним з елементів гібридної війни Росії проти України. Іншими елементами стали: 1) пропаганда, що базується на брехні та підміні понять; 2) торговельно-економічний тиск; 3) енергетична блокада; 4) терор і залякування громадян України; 5) кібератаки; 6) категоричне заперечення самого факту війни попри наявність безлічі неспростовних доказів; 7) використання у своїх інтересах проросійських сил та держав-сателітів; 8) звинувачення іншої сторони у власних злочинах» [1].

Слід нагадати, що Мирослав Попович ще у 2010 році у передмові до книги Володимира Горбуліна «Без права на покаяння» наголошував на тому, що: «майбутні конфлікти потребують насамперед високоточної зброї й розвиненої системи інформаційних технологій» [2, с. 5].

Інформаційні технології відіграють величезну роль у сучасних збройних конфліктах. При цьому Сенгер зазнач, шо 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… США були одними з перших – створили так звані «Сили кібероперацій» … 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, с. 19].

«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 діятиме настільки швидко, що люди не встигнуть ні усвідомити загрози, ні запобігти їй – тож атаки відбудуться і призведуть до ескалації конфлікту» [3, с. 21].

Отже зафіксуємо цю обставину, що 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 адекватної /гібридної відповіді, зокрема, за допомогою юридичних заходів.

Ці юридичні заходи мають забезпечити «кібербезпеку» – стан захищеності кіберпростору від кібератак, за якого забезпечується його сталий розвиток, а також своєчасне виявлення, запобігання і нейтралізація реальних та потенційних функціонуванню його елементів» [4, с. 189]. «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 [5].

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.

Істотну кіберзагрозу становлять кібератаки – 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 [5].

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 [6].

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 [7].

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.

Отже, 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 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 безпеки України, 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 [8], 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.

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.

ЛІТЕРАТУРА:

1. 10 фактів про збройну агресію Росії проти України. Опубліковано 09 грудня 2019 року о 14:10. URL: https://mfa.gov.ua/10-faktiv-pro-zbrojnu-agresiyu-rosiyi-proti-ukrayini

2. Горбулін В. П. Без права на покаяння. Харків: Фоліо, 2010. 383 с.

3. 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. 496 с.

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

5. 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

6. Вимоги до захисту інформації в інформаційних системах у воєнний час: роз'яснення Держспецзв'язку | Кабінет Міністрів України (kmu.gov.ua)

7. 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)

8. Доктрина інформаційної безпеки України – це лише декларація – експерти. URL: https://www.radiosvoboda.org/a/28336852.html

Булеца Сібілла Богданівна,

докторка юридичних наук, професорка, зав. кафедри цивільного права та процесу ДВНЗ «Ужгородський національний університет»

ЦИФРОВІ АВАТАРИ: ОБ'ЄКТИ ЧИ СУБ'ЄКТИ ПРИВАТНОГО ПРАВА

Аватар у цифровому контексті – це віртуальне втілення особи у віртуальному середовищі, тобто її цифрова проекція. При цьому аватар може бути схожим на користувача або ж відрізнятися від нього. [1, с.18] Спочатку слово аватар мало переважно релігійне або духовне підґрунтя та зміст і означало сходження божества на землю, згідно з індуїзмом [2, с.72–73]. Свого сучасного значен-

Зміст