DOI: 10.33498/louu-2022-08-076

III. Правове забезпечення інформаційної безпеки під час дії в Україні правового режиму воєнного стану

Тарас Ткачук

доктор юридичних наук, доцент,
заступник директора інституту (з навчальної та наукової роботи)
Навчально-наукового гуманітарного інституту
Національної академії Служби безпеки України
ORCID ID: https://orcid.org/0000-0002-4620-3300
tarast25@gmail.com

Наталія Ткачук

кандидатка юридичних наук,
провідна наукова співробітниця наукової лабораторії
дослідження проблем забезпечення інформаційної безпеки
та інформаційно-аналітичної діяльності
Науково-організаційного центру
Національної академії Служби безпеки України
ORCID ID: https://orcid.org/0000-0003-4311-0712
natalie-tkachuk@ukr.net

УДК 342.746.1(477)

СТРАТЕГІЯ АНТИКРИХКОСТІ У ЗАБЕЗПЕЧЕННІ КІБЕРБЕЗПЕКИ УКРАЇНИ: ПРАВОВИЙ АСПЕКТ

Анотація. Кібербезпека держави безпосередньо впливає на стабільність усіх критично важливих сфер: військової, економіки, зовнішньої політики, медицини, освіти тощо. Держава, в особі уповноважених органів, може впровадити ефективні кіберполітики та використовувати дорогі ІТ-системи, проте якщо у державі діють більш низькі стандарти кібербезпеки, аніж у наших міжнародних партнерів, операційні процеси на тактичному рівні можуть опинитися під загрозою. Власне, у цьому контексті роль правового чинника є першоосновою. Впровадження апробованих стандартів та їх імплементація у національне законодавство має відбуватися досить оперативно, а також синхронно щодо основних гравців на міжнародному просторі.

В умовах війни, підсиленої тотальною диджиталізацією, питання правового врегулювання збереження даних, управління ІТ-системами, швидкого й ефективного відновлення у разі кібератак стають ключовим ресурсом для успіху у кібервійні та протидії кіберзагрозам.

Все це зумовлює необхідність пошуку нових, більш ефективних стратегій у сфері кібербезпеки. Національна система кібербезпеки повинна не лише протистояти викликам і загрозам зовнішнього середовища, адаптуватися до нових умов, а й зміцнювати власні спроможності в умовах непередбачуваності. На нашу думку, однією з таких актуальних стратегій може бути стратегія антикрихкості.

Метою статті є екстраполяція основних загроз кібербезпеці держави, а також можливостей їхній протидії на стратегію антикрихкості Н. Талеба. Вироблення на цій основі конкретних пропозицій до удосконалення національного інформаційного законодавства у частині забезпечення кібербезпеки держави.

У статті окреслено характерні загрозливі маркери сучасної кіберепохи:

1. Пропаганда набула нових форм як у контексті воєнної агресії, так і в захисті й обороні, активне поширення державою-агресоркою дезінформації, викривлення відомостей, а також виправдування або заперечення збройної агресії Російської Федерації проти України.
2. Вразливість до кіберзагроз об'єктів критичної інфраструктури, систем зв'язку, космічної галузі тощо.
3. Виникнення нових типів загроз, пов'язаних із маніпуляцією.
4. Реальні загрози глобальному інформаційному суспільству та кожній людині несуть: мілітаризація кіберпростору, розв'язування широкомасштабних інформаційних війн, поширення екстремістських і маніпулятивних матеріалів, деструктивні інформаційно-психологічні впливи на індивідуальну, групову й суспільну свідомість, використання штучного інтелекту у військовій сфері тощо.

У статті здійснено аналіз міжнародного та національного інформаційного законодавства. На цій основі доведено, що правовий чинник є базовим елементом системи кібербезпеки. У цьому контексті Україна потребує низки принципово важливих напрямів удосконалення інформаційного законодавства у сфері забезпечення кібербезпеки.

Зроблено висновок, що чорнолебедині ризики і загрози вимагають від кіберпростору антикрихкості, здатності оновлюватися й отримувати користь від несподіваних ударів. Сьогодні ми маємо шукати можливості діяти на випередження. Для цього нам доведеться використовувати комплексний підхід, що включає в себе правові, кадрові та організаційні заходи, спрямовані на: аналіз і оцінку не лише добре відомих ризиків і загроз, з якими система кібербезпеки стикалася раніше, а й тих, що належать до Чорних лебедів, подій малопередбачуваних і непрогнозованих; розроблення різних прогнозних сценаріїв, які видаються найсуттєвішими і значущими для безпеки держав; вибудовування програм оперативного відновлення у випадку кіберзагроз; створення механізмів активної оборони у кіберпросторі.

Система зазначених основоположних заходів і буде нашою стратегією антикрихкості в умовах як війни, так і ризиків, що постійно змінюються у нашому динамічному суспільстві.

Доведено, що розвиток цифрового середовища, наскрізних цифрових платформ, технологій тощо став фундаментом для зародження та розвитку нових суспільних відносин, потребує чіткого правового врегулювання.

Водночас новий етап кіберзагроз, продемонстрований під час російсько-української війни, вимагає подальшого удосконалення стратегії протидії ним. Національна система кібербезпеки має не лише ефективно стримувати деструктивні дії в кіберпросторі, досягати кіберстійкості на всіх рівнях і взаємодії всіх суб'єктів забезпечення кібербезпеки, а й посилювати власні спроможності в умовах непередбачуваності і невизначеності, в умовах збройної агресії проти України. Вона має ґрунтуватися на єдиних міжнародних правових засадах, обміну про такі загрози в режимі реального часу, подальшого розвитку партнерської взаємодії на всіх рівнях: міжнародному, державному та, особливо, державно-партнерському. Пріоритет нових підходів має відбуватися на основі правових підходів до впровадження новіт-

ніх інформаційно-комунікаційних технологій, правових меж застосування штучного інтелекту, інтернету-речей, зокрема у військовій сфері, посилення юридичної відповідальності за використання кіберпростору проти миру, життя та гідності людей, негативних інформаційних впливів, розв'язування конфліктів тощо.

Процеси технологічного розвитку кіберсфери у найближчі роки матимуть тенденцію до динамічного розвитку в усіх сферах соціуму, а особливо військовій, світ вже немислимий без цілеспрямованої глобальної інформатизації. Тому інформаційне право має посісти своє чільне місце як регулятор цих процесів, а також потужний механізм підвищення рівня захисту соціальних об'єктів від агресивного кібервпливу.

Ключові слова: антикрихкість; кібербезпека; кіберзагрози; інформаційне право; інформаційне законодавство.

Кібербезпека держави безпосередньо впливає на стабільність усіх критично важливих сфер: військової, економіки, зовнішньої політики, медицини, освіти тощо. Держава, в особі уповноважених органів, може впровадити ефективні кіберполітики та використовувати дорогі ІТ-системи, проте якщо у державі діють більш низькі стандарти кібербезпеки, аніж у наших міжнародних партнерів, операційні процесі на тактичному рівні можуть опинитися під загрозою. Власне, у цьому контексті роль правового чинника є першоосновою. Впровадження апробованих стандартів та їх імплементація у національне інформаційне законодавство має відбуватися досить оперативно, а також синхронно щодо основних гравців на міжнародному просторі.

В умовах війни, підсиленої тотальною диджиталізацією, питання правового врегулювання збереження даних, управління ІТ-системами, швидкого й ефективного відновлення у разі кібератак стають ключовим ресурсом для успіху у кібервійні та протидії кіберзагрозам. При цьому прагнення миру і безпеки постійно призводили до зміни поглядів на саму суть інформації, виникнення нових суспільних відносин і, відповідно, нових норм права. У контексті цього констатуємо розвиток правового забезпечення кібербезпеки як підгалузі права, яка входить до комплексної галузі права – інформаційне право[1]. Таким чином, предмет правового забезпечення кібербезпеки становить сукупність суспільних відносин, пов'язаних з інформацією, інформаційною інфраструктурою і правовим статусом суб'єктів інформаційної сфери, що належать до об'єктів національних інтересів, а також із проявом загроз безпеки цих об'єктів.

Все це зумовлює необхідність пошуку нових, більш ефективних стратегій у сфері кібербезпеки. Національна система кібербезпеки повинна не лише протистояти викликам і загрозам зовнішнього середовища, адаптуватися до нових умови, а й зміцнювати власні спроможності

[1] О Довгань, Т Ткачук, 'Правове забезпечення інформаційної безпеки держави як підгалузь інформаційного права: теоретичний дискурс' [2018] 2 (25) Інформація і право 84.

в умовах непередбачуваності. На нашу думку, однією з таких актуальних стратегій може бути стратегія антикрихкості.

Питання антикрихкості є новим і малодослідженим у науковій літературі. Термін "антикрихкість" з'явився у науковому обігу завдяки сучасному лівансько-американському науковцю та біржовому аналітику Насіму Ніколасу Талебу. У жодному словнику немає визначення терміна "антикрихкість", а сам Н. Талеб вважає, що його корені варто шукати у філософії стоїків – Фалеса та Сенеки[2]. Тема антикрихкості основним чином розкривається у працях Н. Талеба. Проте низка вітчизняних учених також приділяють їй значну увагу. Л. Мельник О. Маценко, О. Дериколенко, М. Кириленко, І. Стародуб досліджують антикрихкість в економіці підприємств, територій та макроекономічних систем в умовах цифрових трансформацій. Дослідження питань кібербезпеки держави крізь призму стратегії антикрихкості є досить новим для української правничої науки, що значно розширює сферу наукового пошуку та меж інформаційного права.

Метою дослідження є екстраполяція основних загроз кібербезпеці держави, а також можливостей їхній протидії на стратегію антикрихкості Н. Талеба. Вироблення на цій основі конкретних пропозицій до удосконалення національного інформаційного законодавства у частині забезпечення кібербезпеки держави.

Н. Талеб виводить поняття антикрихкості з розширеного визначення крихкості. "Крихкість" не має формального визначення і описується як те, що не любить мінливості. З мінливістю пов'язаний кластер невпорядкованих, хаотичних, випадкових феноменів. Це: 1) невизначеність; 2) варіативність; 3) недосконале, неповне знання; 4) імовірність; 5) хаос; 6) волатильність; 7) безлад; 8) ентропія; 9) час; 10) невідомість; 11) випадковість; 12) сум'яття; 13) стресор; 14) помилка; 15) дисперсія результатів; 16) незнання[3].

> Деяким речам шок іде на користь; вони розквітають і розвиваються, стикнувшись із коливаннями, випадковістю, безладом, стресом, любовними пригодами, ризиками, невизначеністю. Це поширене явище, але в нашій мові немає антоніма до слова "крихкий". Назвімо цю властивість "антикрихкістю"[4].

У вітчизняних наукових колах "антикрихкість" визначають як властивість систем ставати стійкішими і досконалішими під впливом несприятливих факторів. До принципів забезпечення антикрихкості

[2] Євген Пенцак, 'Книга: дослідження "антикрихкості"' (*LB.ua,* 21.05.2014) <https://lb.ua/economics/2014/05/21/266991_doslidzhennya_antikrihkosti.html> (дата звернення: 20.08.2022).
[3] Н Талеб, *Антикрихкість. Про (не)вразливе у реальному житті* (пер з англ, Наш формат 2020) 17.
[4] Там само 9.

економічних систем відносять: застосування інновацій, толерантність до змін, усунення крихких складових, самоуправління колективу, мінімізацію надмірного ризику, формування запасу ресурсів, орієнтацію на стратегічні цілі, активізацію нелінійного мислення. Робляться висновки, що антикрихкість є універсальним інструментом, який підходить різним організаціям, незалежно від їх параметрів[5]. О. Дерев'янко досліджує управлінські аспекти забезпечення антикрихкості репутації підприємства, науково обґрунтовує необхідність формувати й оцінювати репутацію підприємства за критерієм антикрихкості. Антикрихкість репутації – це стан сформованого репутаційного менеджменту підприємства. Забезпечення антикрихкості репутації підприємства вимагає прямого обмеження управлінського впливу з боку менеджменту підприємства на процес його формування. Автор проєктує концепцію Н. Талеба на управління репутацією підприємства і доходить цікавого висновку. Досягнення антикрихкості є можливим тільки на основі органічного, а не механічного підходу (організація як природна система, організм, а не штучна – механізм). Доцільний концептуальний підхід – гормезис (загартовування шкодою – наприклад, ініційованими володарем репутації та/або менеджерами його репутації скандалами). Помилковий шлях – ятрогенія (зайве втручання у природні процеси, що призводить до крихкості системи – штучні події, зайво інтенсивна медіаактивність, пристрасть до проплачених публікацій)[6]. Г. Филюк , Т. Сірик розглядають антикрихкість та її основні характеристики як актуальну конкурентну стратегію в умовах непередбачуваності. Її сутність полягає у тому, що антикрихкі суб'єкти не тільки не піддаються впливу негативних факторів, а й отримують від них власну вигоду, пристосовуються до мінливих умов зовнішнього середовища та забезпечують стійкі темпи зростання[7]. О. Радутний протиставляє антикрихкість саморозвитку особистості штучному інтелекту та високотехнологічним напрямам, зокрема біоінженерії, що перетворюють *Homo sapience* на цифрову людину[8].

Атикрихкість виникла як засіб проти Чорних лебедів (інший феномен, описаний Н. Талебом). Це непередбачувані рідкісні події великого масштабу, які спричиняють серйозні наслідки і водночас, на його думку, творять історію, технологію, науку, все на світі. Головний аспект

[5] Л Мельник, О Маценко, О Дериколенко, М Кириленко, І Стародуб, 'Економіка підприємств, територій та макроекономічних систем в умовах цифрових трансформацій: від стабільності й лінійного мислення до антикрихкості та нелінійного, інноваційного мислення' (2021) 3 Механізм регулювання економіки 76.

[6] О Дерев'янко, 'Управлінські аспекти забезпечення антикрихкості репутації підприємства' (2014) 16 Вчені записки: зб. наук. праць 78.

[7] Г Филюк, Т Сірик, 'Антикрихкість як нова стратегія досягнення конкурентних переваг підприємства' [2021] 2 (25) Приазовський економічний вісник 54.

[8] О Радутний, 'Антикрихкість саморозвитку особистості проти чорного лебедя штучного інтелекту та цифрової людини' в *Проблеми саморозвитку особистості в сучасному суспільстві: матеріали Міжнар. наук. -практ. конф., 15 листоп. 2019 р.* (Право 2019) 133.

проблеми Чорного лебедя полягає в тому, що вирахувати ймовірність незвичайних подій неможливо. Також неможливо обчислити ризики рідкісних подій і передбачити, коли вони настануть. Прикладом цього є аналітичні дослідження щодо нинішньої російсько-української війни, більшість із яких виявилися неточними, а то й зовсім протилежними сучасним реаліям. Отже, слід погодитися з Н. Талебом, що передбачити майбутнє принципово неможливо. Проте зрозуміти, як не постраждати від удару значно легше, ніж спрогнозувати сам удар[9].

Як зазначає Н. Талеб, рідкісні кейси потребують окремого аналізу, а велика війна – це рідкісна подія[10]. Російсько-українська війна, що триває, попри інші системні зміни світової архітектури безпеки, окреслила характерні загрозливі маркери сучасної кіберепохи:

1. Пропаганда набула нових форм як у контексті воєнної агресії, так і в захисті й обороні, активне поширення державою-агресоркою дезінформації, викривлення відомостей, а також виправдовування або заперечення збройної агресії Російської Федерації проти України. З метою донесення правди про війну, забезпечення єдиної інформаційної політики в період дії в Україні правового режиму воєнного стану, запровадженого Указом Президента України "Про введення воєнного стану в Україні"[11], затвердженого Законом України "Про затвердження Указу Президента України 'Про введення воєнного стану в Україні'"[12], рішенням Ради національної безпеки і оборони України від 18 березня 2022 р. встановлено, що

> в умовах воєнного стану реалізація єдиної інформаційної політики є пріоритетним питанням національної безпеки, забезпечення якої реалізується шляхом об'єднання усіх загальнонаціональних телеканалів, програмне наповнення яких складається переважно з інформаційних та/або інформаційно-аналітичних передач на єдиній інформаційній платформі стратегічної комунікації – цілодобовому інформаційному марафоні "Єдині новини #UAразом"[13].

Слід окремо наголосити, що функціональні демократичні інституції в Україні протягом тривалого часу їх розвитку завжди вирізняли нашу

[9] Н Талеб, *Чорний лебідь. Про (не)ймовірне у реальному житті* (пер з англ, Наш формат 2019) 10.

[10] 'Нассім Талеб про крихкість, антикрихкість та падіння великих імперій. Лекція' *(Forbes Україна,* 09.03.2022) <https://forbes.ua/inside/nasim-taleb-pro-krikhkist-antikrikhkist-ta-padinnya-velikikh-imperiy-lektsiya-09032022-4418> (дата звернення: 20.08.2022).

[11] Про введення воєнного стану в Україні: Указ Президента України від 24 лютого 2022 р. № 64/2022 <https://zakon.rada.gov.ua/laws/show/64/2022#Text> (дата звернення: 20.08.2022).

[12] Про затвердження Указу Президента України "Про введення воєнного стану в Україні" від 24 лютого 2022 р. № 2102-IX <https://zakon.rada.gov.ua/laws/show/2102-20#Text> (дата звернення: 20.08.2022).

[13] Щодо реалізації єдиної інформаційної політики в умовах воєнного стану: рішення Ради національної безпеки і оборони України від 18 березня 2022 року, введено в дію Указом Президента України від 19 березня 2022 р. № 152/2022 <https://zakon.rada.gov.ua/laws/show/n0004525-22#n2> (дата звернення: 20.08.2022).

країну від Росії, що й є потужною конкурентною перевагою в інформаційній війні. Найбільша перевага полягає в тому, що відсутність демократії, жорстка цензура, тотальний державний контроль медіаранку стали причиною того, що російське вище політичне й військове керівництво отримало спотворену інформацію про боєготовність української армії, про настрої українського суспільства й розпочало програшну військову кампанію.

2. Вразливість до кіберзагроз об'єктів критичної інфраструктури, систем зв'язку, космічної галузі тощо. Власне російсько-українська кібервійна розпочалася задовго до 24 лютого 2022 р. Майбутній директор американського Агентства національної безпеки М. Роджерс із цього приводу зазначав, що разом із військовою операцією із захоплення Криму, Росія розпочала проти України кібервійну[14]. За два місяці російсько-української війни нейтралізовано понад 250 потужних кібератак ворога. Тут слід додати, що нинішня війна з Росією розпочалася з кібернападу на супутники. З цього приводу Європейський Союз (далі – ЄС) і його держави-члени разом із міжнародними партнерами засудили зловмисну кібератівність Росії проти України, спрямовану на супутникову мережу *KA-SAT*, що належить *Viasat*. Кібератака сталася за годину до неспровокованого та невиправданого вторгнення Росії в Україну 24 лютого 2022 р., що сприяло військовій агресії. Ця кібератака мала значний вплив, спричинивши не вибіркові перебої у зв'язку та збоїв у роботі кількох державних органів, підприємств та користувачів в Україні, а також вплинула на декілька держав – членів ЄС[15].

3. Виникнення нових типів загроз, пов'язаних із маніпуляцією. Транскордонність кіберпростору, попри наявність значних переваг, має і низку проблем, особливу чутливість яких ми зрозуміли під час нинішньої російсько-української війни. Зокрема, це нівелювання можливостей національних інформаційного законодавств, державного контролю й економічного впливу. У такій ситуації концентруються потужні деструктивні ризики, які здатні завдати значної шкоди реалізації законних інтересів людини в глобальному інформаційному просторі. Про це свідчить низка проблем, таких як: ідентифікація; спотворення результатів електронного голосування; технологічні негаразди під час створення систем електронного урядування й електронної демократії; недостовірності баз даних; незахищеності конфіденційної інформації та персональних даних у процесі надання державних адміністративних послуг;

[14] Jarno Limnéll, 'The Exploitation of Cyber Domain as Part of Warfare: Russo-Ukrainian War' [2015] 4 (4) International Journal of Cyber-Security and Digital Forensics 521–32.

[15] Russian cyber operations against Ukraine: Declaration by the High Representative on behalf of the European Union (*Council of the EU Press release,* 10.05.2022) <https://www.consilium.europa.eu/en/press/press-releases/2022/05/10/russian-cyber-operations-against-ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union/?fbclid=IwAR35cBJAxxoPB5Ot_Aw-zSTUpGo9UsQlGihQQ9Avtkw45bAAECtEPhrR0rw> (accessed: 20.08.2022).

зловмисного використання вказаних даних під час здійснення електронного судочинства; поширення шкідливого, незаконного контенту, який становить загрозу для життя і здоров'я людини й дезорієнтує її; оприлюднення електронними засобами масової інформації відомостей, які паплюжать честь і гідність людини; викрадення інформації, що використовується у фінансово-банківських установах (інтернет-банкінг); втрата інформації через зловмисні кібератаки під час користування інтернет-мережею тощо.

4. Реальні загрози глобальному інформаційному суспільству та кожній людині несуть: мілітаризація кіберпростору, розв'язування широкомасштабних інформаційних війн, поширення екстремістських і маніпулятивних матеріалів, деструктивні інформаційно-психологічні впливи на індивідуальну, групову й суспільну свідомість, використання штучного інтелекту у військовій сфері тощо.

В умовах військової агресії чинна Стратегія кібербезпеки України зазнала нових викликів. Відповідно до Стратегії розбудова національної системи кібербезпеки відбувається на засадах стримування, кіберстійкості та взаємодії. Кіберстійкість – це набуття здатності швидко адаптуватися до внутрішніх і зовнішніх загроз у кіберпросторі, підтримувати та відновлювати стале функціонування національної інформаційної інфраструктури, насамперед об'єктів критичної інформаційної інфраструктури[16].

Проте, якщо порівняти кіберстійкість та антикрихкість, то ми побачимо, що кіберстійкість, як будь-що стійке, гнучке та міцне, загалом витримує удар і залишається таким самим. Стійкість у контексті національної безпеки стосується здатності суспільств справлятися із загрозами та ризиками, адаптуватися до них та відновлюватися у разі нападу чи іншої події, не втрачаючи здатність забезпечувати виконання основних функцій і надання основних послуг членам цього суспільства[17]. Антикрихкому удар іде на користь, воно стає кращим. Антикрихке (і крихке) майже завжди можна розпізнати за допомогою простого тесту на асиметрію: все, чому рідкісні події (або який-небудь стрес) пішли на користь, – антикрихке; і все, що від них, навпаки, постраждало, – крихке. Антикрихкому подобається нестабільність. Воно любить перевірку часом. Міцно і в корисний спосіб пов'язане з нелінійністю: все нелінійне або крихке, або некрихке стосовно того чи іншого джерела випадковості[18]. Варто також, на нашу думку, акцентувати увагу, що існуючі форми та способи комуніка-

[16] Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України": Указ Президента України від 26 серпня 2021 р. № 447/2021 <https://zakon.rada.gov.ua/laws/show/392/2020#n12> (дата звернення: 20.08.2022).

[17] Oliver Tamminga, 'Zum Umgang mit hybriden Bedrohungen. Auf dem Weg zu einer nationalen Resilienzstrategie' (2015) 92 SWP-Aktuell 3.

[18] Талеб (н 3) 9–10.

цій, характерні для суспільства знань, розвиток якого ми спостерігаємо у світі, здійснюються задля задоволення потреб, реалізації інтересів і цінностей особи й суспільства, а не заради інформаційної взаємодії як такої. Саме це, як вважає низка дослідників, і є ціннісним самопізнанням під час аналізу інформаційної картини світу. Саме в цьому полягає сутність аксіологічного підходу до вивчення інформаційної сфери – процесів, взаємодії, обміну, продукції, послуг[19].

Події російсько-української війни підтвердили одну з найяскравіших думок Н. Талеба: 'Антикрихкість дає нам змогу функціонувати в умовах невизначеності, коли ми не до пуття відаємо, що робимо, – і все одно досягаємо успіху. Скажу просто: робити ми вміємо краще, ніж думати, – саме завдяки антикрихкості'[20].

Можна стверджувати, що антикрихкість вже стала характерною рисою національної системи кібербезпеки. Виникла вона в абсолютно природний спосіб як реакція на російську агресію. Національна система кібербезпеки не лише адаптувалася до внутрішніх і зовнішніх загроз та відновила функціонування національної інформаційної інфраструктури. Вона змогла ще й посилити власні спроможності в умовах високої невизначеності.

Ми стали більш волатильними та згуртованими. Так, наприкінці лютого 2022 р., з метою протидії російським кібератакам і створення відповідних загроз для ворога, була організована спільнота українських ІТ-спеціалістів, яка на початок червня 2022 р. налічувала близько пів мільйона учасників. Досить ефективним у процесі створення та реалізації кіберзагроз для ворога стало міжнародне угрупування *Anonymous.* У відповідь на вторгнення Росії до України 2022 р., *Anonymous* оголосило кібервійну російському уряду. Повідомлення про це було опубліковане у твітері у ніч на п'ятницю, 25 лютого. Угруповання вперше у своїй історії оголосило війну цілій країні[21]. Міжнародна спільнота відзначила зусилля України із протидії кіберзагрозам – наша країна вперше здобула одразу дві важливі нагороди у сфері кібербезпеки *CYBERSEC Award.* Україну нагородили за героїчний спротив російській агресії та захист цифрових кордонів демократичного світу[22].

Кібергігієна, медіаграмотність набули особливої значущості під час отримання цінної інформації, її обробки та аналізу. У контексті анти-

[19] T Tkachuk, L Chystokletov, O Khytra, V Shyshko, L Ostapenko, 'Philosophical reflections on the information society in the context of a security-creating paradigm' [2021] 13 (1) IJESDF 105–113.

[20] Талеб (н 3) 10.

[21] Євген Жуков, Анастасія Шепелева, 'Хакери Anonymous оголосили кібервійну Росії' (*DW*, 25.02.2022) <https://www.dw.com/uk/khakery-anonymous-oholosyly-kiberviinu-rosii-cherez-yii-napad-na-ukrainu/a-60917117> (дата звернення: 20.08.2022).

[22] 'Україна здобула одразу дві міжнародні нагороди за ефективний кіберзахист' (*Державна служба спеціального зв'язку та захисту інформації України,* 17.05.2022) <https://cip.gov.ua/ua/news/ukrayina-zdobula-odrazu-dvi-mizhnarodni-nagorodi-za-efektivnii-kiberzakhist> (дата звернення: 20.08.2022).

крихкості в Україні запрацювали досить ефективні та дієві проєкти, серед яких можемо виокремити проєкт із медіаграмотності Міністерства культури та інформаційної політики України "ФІЛЬТР"[23]. Крім того, Україні вдалося згуртувати весь цивілізований світ у протидії кіберзагрозам, кібератакам, кібертероризму, налагодити обмін розвідувальними даними в режимі реального часу з іноземними партерами[24].

Відбулося формування нового планетарного кіберпростору, де інформаційні й телекомунікаційні технології забезпечують ефективну міжособистісну взаємодію. Основними властивостями таких процесів є безмежність, доступність, гіперзв'язаність, прозорість територіальних кордонів, рух у масштабі часу, розвиток інтернету речей, штучного інтелекту тощо. Сьогодні свою допомогу Україні у кіберзахисті запропонували всі уряди демократичних країн, зокрема США, Канада, Велика Британія, більшість країн ЄС та низка інших країн. Україну також підтримують і провідні міжнародні компанії: *Microsoft, Google, Amazon, Cisco, Oracle* та ін. Крім того, Україна приєднається до Об'єднаного центру передових технологій з кібероборони НАТО *(CCDCOE)* як країна, яка бере участь у роботі *(contributing participant),* попри блокування такого вступу Угорщиною. 30 травня 2022 р. українська делегація вперше взяла участь у засіданні Керівного комітету Об'єднаного центру передових технологій з кібероборони НАТО *(CCDCOE).*

Новий формат кіберзагроз у зв'язку із військовою агресією Російської Федерації, глобалізація кіберпростору, розширення суб'єктів протидії цим загрозам спровокувало появу нових суспільних відносин, які потребують свого правового врегулювання нормами інформаційного права. Як результат, 13 травня 2022 р. Європейський Парламент ухвалив Директиву про заходи для високого загального рівня кібербезпеки у ЄС (далі – Директива *NIS 2*), яка адаптує попередню Директиву *NIS* до сучасних викликів, загроз і поточних потреб[25].

Директива *NIS 2* реагує на посилення впливу кіберзагроз на Європу через підвищення стійкості та спроможності реагувати на інциденти державного й приватного секторів і ЄС загалом. Нові правила охоплюють ширшу сферу дії порівняно з попередньою Директивою та розширюють коло організацій, які зобов'язані вживати заходів щодо управління ризиками кібербезпеки.

[23] Національний проєкт з медіаграмотності <https://filter.mkip.gov.ua/pro-nas> (дата звернення: 20.08.2022).

[24] Заява МЗС України щодо формування міжнародної коаліції для протидії злочинній діяльності Росії в кіберпросторі від 11 травня 2022 року *(Урядовий портал)* <https://www.kmu.gov.ua/news/zayava-mzs-ukrayini-shchodo-formuvannya-mizhnarodnoyi-koaliciyi-dlya-protidiyi-zlochinnij-diyalnosti-rosiyi-v-kiberprostori> (дата звернення: 20.08.2022).

[25] Commission welcomes political agreement on new rules on cybersecurity of network and information systems (13 may 2022) <https://ec.europa.eu/commission/presscorner/detail/en/IP_22_2985> (accessed: 20.08.2022).

Зокрема, Директива *NIS 2* посилить вимоги до кібербезпеки, запровадить суворіші наглядові заходи для національних органів влади, узгодить режими санкцій у країнах-членах, а також покращить обмін інформацією та співпрацю з управління кіберкризами в Європі. Вона вимагатиме від компаній у секторах енергетики, транспорту, фінансових ринків, охорони здоров'я та цифрової інфраструктури дотримання заходів щодо управління ризиками кібербезпеки та зобов'язань щодо звітності. Організації повинні будуть повідомляти органи влади про кіберінциденти протягом 24 годин, виправляти вразливість програмного забезпечення та готувати заходи захисту мереж. Невиконання вимог тягне за собою накладання штрафів.

Верховна Рада України ухвалила Закон України "Про внесення змін до Кримінального процесуального кодексу України щодо підвищення ефективності досудового розслідування за "гарячими слідами" та протидії кібератакам"[26], яким, зокрема, передбачено такі зміни:

– щодо кіберзлочинів та інших кримінальних правопорушень, пов'язаних із комп'ютерними даними, запроваджено новий вид заходів забезпечення кримінального провадження – термінове збереження інформації, що здійснюється на підставі постанови слідчого, прокурора на строк до 90 діб із можливістю продовження;

– змінено обсяг інформації, яка є у постачальників електронних комунікаційних послуг і відноситься до охоронюваної законом таємниці;

– запроваджено нові слідчі (розшукові) дії – отримання інформації щодо електронних комунікацій, зняття показань технічних приладів і технічних засобів, що мають функції фото-, кінозйомки, відеозапису, чи засобів фото-, кінозйомки, відеозапису;

– введено термін "віртуальні активи" у перелік майна, на яке може бути накладено арешт.

Також Верховною Радою України, з метою посилення спроможностей та оптимізації національної системи кібербезпеки для протидії кіберзагрозам, впровадженню дієвих кримінально-правових механізмів протидії кіберзлочинності та забезпечення надійності й безпеки використання цифрових послуг, було ухвалено Закон України "Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану"[27].

Щодо функціонування неофіційного громадського руху "КіберАрмія" як протидії кіберзагрозам і створення відповідних загроз против-

[26] Про внесення змін до Кримінального процесуального кодексу України та Закону України "Про електронні комунікації" щодо підвищення ефективності досудового розслідування "за гарячими слідами" та протидії кібератакам: Закон України від 15 березня 2022 р. № 2137 <https://zakon.rada.gov.ua/laws/show/2137-%D0%86%D0%A5#Text> (дата звернення: 20.08.2022).

[27] Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану: Закон України від 24 березня 2022 р. № 2149 <https://ips.ligazakon.net/document/view/T222149?an=16> (дата звернення: 20.08.2022).

нику потребує удосконалення національне кримінальне законодавство в частині уточнення статей 361, 361[1] Кримінального кодексу України (далі – КК України)[28] ("Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж" і "Створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут"). Формально такі дії можуть підпадати під ознаки складів злочинів, що передбачені зазначеними статтями КК України. Зрозуміло, що дії цих людей відповідають інтересам України та українського народу й не є суспільно небезпечними. Та попри це формалізація звільнення від кримінальної відповідальності на рівні приміток чи окремих частин відповідних спеціальних статей КК України буде доцільною та такою, що цілком відповідає потребам сьогодення і спрямована на протидію російській агресії.

Досить новаторським, з огляду на міжнародну практику, стало підписання Президентом України Закону "Про хмарні послуги"[29], який набув чинності 16 вересня 2022 р. Аналогічні технології вже дали позитивні результати у практиці органів влади США, Німеччині, Канади, Швеції, Норвегії, Данії, Сінгапуру, Республіці Корея, Австралії, Саудівській Аравії. Подібна практика дала змогу Англії зменшити витрати на цифрові трансформації та інформаційні технології більш ніж на 3 млрд фунтів стерлінгів. Законом встановлено, що

> надання хмарних послуг та/або послуг центру обробки даних публічним користувачам хмарних послуг здійснюється з дотриманням вимог законодавства про захист персональних даних, про захист інформації та про кібербезпеку.
>
> Забороняється обробка інформації, що становить державну таємницю, службової інформації, державних та єдиних реєстрів, створення та забезпечення функціонування яких встановлено законом, за допомогою хмарних ресурсів та/або центрів обробки даних, що розміщені за кордоном або на тимчасово окупованій території України, або належать державі, визнаній Верховною Радою України державою-агресором чи державою окупантом, або належать суб'єктам, діяльність яких підпадає під дію Закону України "Про санкції" та щодо яких прийнято рішення про застосування санкцій в Україні[30].

[28] Кримінальний кодекс України: Закон України від 5 квітня 2001 р. № 2341-III <https://zakon.rada.gov.ua/laws/show/2341-14#Text> (дата звернення: 20.08.2022).
[29] Про хмарні послуги: Закон України від 17 лютого 2022 р. № 2075 <https://zakon.rada.gov.ua/laws/show/2075-20#Text> (дата звернення: 20.08.2022).
[30] Там само.

Ці та низка інших особливостей визначили засади формування нової дійсності – віртуальної реальності, що характеризується нелінійним розвитком суспільства, що значно ускладнює всі аналітичні прогнози. Яскравим прикладом є аналітичні дослідження щодо нинішньої російсько-української війни, більшість з яких виявилися неточними, а то й зовсім протилежними сучасним реаліям. Формування нової реальності зумовило виникнення нових суспільних цінностей – інформаційних, які на цьому етапі еволюції світової спільноти стали визначальними.

Загалом у сучасних умовах розбудови інформаційного суспільства та цифрової трансформації успішне розв'язання глобальних соціально-економічних, політичних, безпекових та інших проблем можливе лише в разі об'єднаних плідних зусиль держав світу та усієї міжнародної спільноти, розроблення чітких правил поведінки у кіберпросторі, що ґрунтуються на міжнародному законодавстві.

Вважаємо, що правовий чинник є базовим елементом системи кібербезпеки. У цьому контексті Україна потребує низки принципово важливих напрямів удосконалення інформаційного законодавства у сфері забезпечення кібербезпеки.

Зупинимося на найсуттєвіших. Подальший розвиток інституту захисту персональних даних. Ми спостерігаємо досить динамічний розвиток цієї сфери впродовж останніх років. Проте ті виклики, які пов'язані з війною, потребують значного прискорення імплементації окремих норм у життя чи прийняття нових. Зокрема, це пов'язано з інформацією про осіб, які безпосередньо задіяні в захисті нашої країни та можливістю використання такої інформації проти них. Це стосується насамперед військовослужбовців, волонтерів, працівників підприємств критичної інфраструктури та ін. У цьому напрямі Верховною Радою України 15 березня взято за основу та в цілому Закон "Про внесення змін до деяких законів України щодо забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів"[31]. Законом вносяться зміни до законів України "Про захист інформації в інформаційно-комунікаційних системах"[32] та "Про публічні електронні реєстри"[33] та передбачається:

[31] Про внесення змін до деяких законів України щодо забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів: Закон України від 15 березня 2022 р. № 2130-IX <https://ips.ligazakon.net/document/view/ji07094a?ed=2022_03_13> (дата звернення: 20.08.2022).

[32] Про захист інформації в інформаційно-комунікаційних системах: Закон України від 5 липня 1994 р. № 80/94-ВР <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text> (дата звернення: 20.08.2022).

[33] Про публічні електронні реєстри: Закон України від 18 листопада 2021 р. № 1907-IX <https://zakon.rada.gov.ua/laws/show/1907-20#Text> (дата звернення: 20.08.2022).

– створення резервних копій державних інформаційних ресурсів із дотриманням встановлених для таких ресурсів вимог щодо їх захисту, цілісності, конфіденційності та їх розміщення за межами України;
– можливість розміщення інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів за межами України.
Основна мета Закону – дозвіл на створення резервних копій держа них інформаційних ресурсів та їх розміщення за межами України із дотриманням встановлених для таких ресурсів вимог щодо їх захисту, цілісності та конфіденційності, а також можливість розміщення інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів за межами України[34].

Потребує прискорення ухвалення Закону України "Про державну реєстрацію геномної інформації людини"[35] з урахуванням вимог чинного національного законодавства, а також міжнародної практики, так як у проєкті міститься низка термінологічних неузгодженостей, не відповідність практиці Європейського суду з прав людини та вимогам кіберзахисту даних.

Також вважаємо за доцільне продовження роботи з удосконалення національного законодавства про захист персональних даних, особливо приведення його у відповідність до Загального регламенту захисту даних *(General Data Protection Regulation, GDPR)*[36]. Цей Регламент забороняє здійснювати будь-які операції з даними резидентів ЄС у країнах, де рівень захищеності персональних даних нижчий, ніж у ЄС. Виходячи з тих міркувань, що український "аналог" *GDPR* був ухвалений понад 10 років тому, хоча й із певними змінами, залишається той факт, що рівень захисту персональних даних в Україні значно нижчий порівняно з вимогами, які ставляться Загальним регламентом.

Інший напрям, що потребує оперативного правового реагування, – це розроблення підзаконних нормативних актів, що визначатимуть підстави для вилучення ненадійних компаній із переліку складальників мобільних мереж *5G*, особливо для критичних систем функціонування держави в секторах оборони, економіки, транспорту, енергетики тощо. Низка таких комплектуючих виготовляють у Китаї і гіпотетично їх мо-

[34] Прийнято Закон щодо збереження державних інформаційних ресурсів. Верховна Рада України (16 березня 2022) <https://www.rada.gov.ua/print/220553.html> (дата звернення: 20.08.2022).
[35] Про прийняття за основу проекту Закону України про державну реєстрацію геномної інформації людини: постанова Верховної ради України від 14 квітня 2022 р. № 2202 <https://zakon.rada.gov.ua/laws/show/2202-20#Text> (дата звернення: 20.08.2022).
Прим ред.: на момент опублікування статті Закон України "Про державну реєстрацію геномної інформації людини" прийнято та направлено на підпис Президенту.
[36] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) <https://eur-lex.europa.eu/eli/reg/2016/679/oj> (accessed: 20.08.2022).

жуть використати для збирання інформації, зокрема й персональних даних. Нині вже таке занепокоєння висловили Чехія[37], Канада[38] та Англія[39].

Отже, чорнолебедині ризики і загрози вимагають від кіберпростору антикрихкості, здатності оновлюватися й отримувати користь від несподіваних ударів. Сьогодні ми маємо шукати можливості діяти на випередження. Для цього нам доведеться використовувати комплексний підхід, що включає в себе правові, кадрові та організаційні заходи, спрямовані на:

– аналіз та оцінювання не лише добре відомих ризиків і загроз, з якими система кібербезпеки стикалася раніше, а й тих, що належать до Чорних лебедів, подій малопередбачуваних і непрогнозованих;

– розроблення різних прогнозних сценаріїв, які видаються найсуттєвішими і значущими для безпеки держав;

– вибудовування програм оперативного відновлення у випадку кіберзагроз;

– створення механізмів активної оборони у кіберпросторі.

Система зазначених основоположних заходів і буде нашою стратегією антикрихкості в умовах як війни, так і ризиків, що постійно змінюються у нашому динамічному суспільстві.

Висновки. Розвиток цифрового середовища, наскрізних цифрових платформ, технологій тощо став фундаментом для зародження та розвитку нових суспільних відносин, що, зі свого боку, потребує чіткого правового врегулювання. Часті проблеми, пов'язані з використанням неефективних правових методів забезпечення цих відносин і безпосередньо пов'язані з питаннями кібербезпеки, породжують, їх правове забезпечення без належного розуміння технологічних процесів, що відбуваються. Відповідно, є необхідність проведення теоретичних правових досліджень, спрямованих на розроблення концепції та методології реалізації державою своїх охоронних і регулятивних функцій з урахуванням рівня розвитку інформаційних технологій, визначення закономірностей трансформації державного цифрового управління, а також забезпечення кібернетичної безпеки в усіх її проявах як функціонування держави, так і життєдіяльності людини.

Водночас новий етап кіберзагроз, продемонстрований під час російсько-української війни, вимагає подальшого удосконалення стратегії

[37] Lukáš Valášek, 'Stát chystá zákon proti hrozbám z Ruska a Číny. Poslanec ANO svolal jen jeho odpůrce' (*Aktualne.cz,* 20.04.2022) <https://zpravy.aktualne.cz/domaci/stat-pripravuje-zakony-na-hrozby-z-ruska-a-ciny/r~2e536588bfb511ecb5bd0cc47ab5f122> (accessed: 20.08.2022).

[38] 'Канада заборонила Huawei будувати 5G інфраструктуру' (*Укрінформ,* 20.05.2022) <https://www.ukrinform.ua/rubric-technology/3487472-kanada-zaboronila-huawei-buduvati-5g-infrastrukturu.html> (дата звернення: 20.08.2022).

[39] Valeria R, 'Великобританія відмовиться від послуг Huawei в 5G' (*ITsider*, 07.07.2020) <https://itsider.com.ua/velykobrytaniya-vidmovytsya-vid-poslug-huawei-v-5g> (дата звернення: 20.08.2022).

протидії ним. Національна система кібербезпеки має не лише ефективно стримувати деструктивні дії в кіберпросторі, досягати кіберстійкості на всіх рівнях і взаємодії всіх суб'єктів забезпечення кібербезпеки, а й посилювати власні спроможності в умовах непередбачуваності й невизначеності в умовах збройної агресії проти України. Вона має ґрунтуватися на єдиних міжнародних правових засадах обміну про такі загрози в режимі реального часу, подальшого розвитку партнерської взаємодії на всіх рівнях: міжнародному, державному та, особливо, державно-партнерському. Пріоритет нових підходів має відбуватися на основі правових підходів до впровадження новітніх інформаційно-комунікаційних технологій, правових меж застосування штучного інтелекту, інтернету-речей, зокрема у військовій сфері, посилення юридичної відповідальності за використання кіберпростору проти миру, життя та гідності людей, негативних інформаційних впливів, розв'язування конфліктів тощо.

Процеси технологічного розвитку кіберсфери у найближчі роки матимуть тенденцію до динамічного розвитку в усіх сферах соціуму, а особливо військовій, світ вже немислимий без цілеспрямованої глобальної інформатизації. Тому інформаційне право має зайняти своє чільне місце як регулятора цих процесів, а також потужного механізму підвищення рівня захисту соціальних об'єктів від агресивного кібервпливу.

REFERENCES

Bibliography

Translated books

1. Taleb N, *Antykrykhkist. Pro (ne)vrazlyve u realnomu zhytti* (per z anhl, Nash format 2020) (in Ukrainian).
2. Taleb N, *Chornyi lebid. Pro (ne)imovirne u realnomu zhytti* (per z anhl, Nash format 2019) (in Ukrainian).

Journal articles

3. Limnéll J, 'The Exploitation of Cyber Domain as Part of Warfare: Russo-Ukrainian War' [2015] 4 (4) International Journal of Cyber-Security and Digital Forensics 521–32 (in English).
4. Tamminga Ol, 'Zum Umgang mit hybriden Bedrohungen. Auf dem Weg zu einer nationalen Resilienzstrategie' (2015) 92 SWP-Aktuell 3 (in German).
5. Tkachuk T, Chystokletov L, Khytra O, Shyshko V, Ostapenko L, 'Philosophical reflections on the information society in the context of a security-creating paradigm' [2021] 13 (1) IJESDF 105–13 (in English).
6. Derev'ianko O, 'Upravlinski aspekty zabezpechennia antykrykhkosti reputatsii pidpryiemstva' (2014) 16 Vcheni zapysky: zb. nauk. prats 78 (in Ukrainian).
7. Dovhan O, Tkachuk T, 'Pravove zabezpechennia informatsiinoi bezpeky derzhavy yak pidhaluz informatsiinoho prava: teoretychnyi dyskurs' [2018] 2 (25) Informatsiia i pravo 84 (in Ukrainian).

8. Melnyk L, Matsenko O, Derykolenko O, Kyrylenko M, Starodub I, 'Ekonomika pidpryiemstv, terytorii ta makroekonomichnykh system v umovakh tsyfrovykh transformatsii: vid stabilnosti y liniinoho myslennia do antykrykhkosti ta neliniinoho, innovatsiinoho myslennia' (2021) 3 Mekhanizm rehuliuvannia ekonomiky 76 (in Ukrainian).
9. Fyliuk H, Siryk T, 'Antykrykhkist yak nova stratehiia dosiahnennia konkurentnykh perevah pidpryiemstva' [2021] 2 (25) Pryazovskyi ekonomichnyi visnyk 54 (in Ukrainian).

Conference papers

10. Radutnyi O, 'Antykrykhkist samorozvytku osobystosti proty chornoho lebedia shtuchnoho intelektu ta tsyfrovoi liudyny' v *Problemy samorozvytku osobystosti v suchasnomu suspilstvi: materialy Mizhnar. nauk. -prakt. konf., 15 lystop. 2019 r.* (Pravo 2019) 133 (in Ukrainian).

Websites

11. Valášek L, 'Stát chystá zákon proti hrozbám z Ruska a Číny. Poslanec ANO svolal jen jeho odpůrce' (*Aktualne.cz,* 20.04.2022) <https://zpravy.aktualne.cz/domaci/stat-pripravuje-zakony-na-hrozby-z-ruska-a-ciny/r~2e536588bfb511ecb5bd0cc47ab5f122> (accessed: 20.08.2022) (in Czech).
12. 'Kanada zaboronyla Huawei buduvaty 5G infrastrukturu' (*Ukrinform,* 20.05.2022) <https://www.ukrinform.ua/rubric-technology/3487472-kanada-zaboronila-huawei-buduvati-5g-infrastrukturu.html> (accessed: 20.08.2022) (in Ukrainian).
13. 'Nassim Taleb pro krykhkist, antykrykhkist ta padinnia velykykh imperii. Lektsiia' (*Forbes Ukraina,* 09.03.2022) <https://forbes.ua/inside/nasim-taleb-pro-krikhkist-antikrikhkist-ta-padinnya-velikikh-imperiy-lektsiya-09032022-4418> (accessed: 20.08.2022) (in Ukrainian).
14. Pentsak Y, 'Knyha: doslidzhennia "antykrykhkosti"' (*LB.ua,* 21.05.2014) <https://lb.ua/economics/2014/05/21/266991_doslidzhennya_antikrihkosti.html> (accessed: 20.08.2022) (in Ukrainian).
15. Zhukov Y, Shepeleva A, 'Khakery Anonymous oholosyly kiberviinu Rosii' (*DW,* 25.02.2022) <https://www.dw.com/uk/khakery-anonymous-oholosyly-kiberviinu-rosii-cherez-yii-napad-na-ukrainu/a-60917117> (accessed: 20.08.2022) (in Ukrainian).
16. 'Ukraina zdobula odrazu dvi mizhnarodni nahorody za efektyvnyi kiberzakhyst' (*Derzhavna sluzhba spetsialnoho zv'iazku ta zakhystu informatsii Ukrainy,* 17.05.2022) <https://cip.gov.ua/ua/news/ukrayina-zdobula-odrazu-dvi-mizhnarodni-nagorodi-za-efektivnii-kiberzakhist> (accessed: 20.08.2022) (in Ukrainian).
17. Valeria R, 'Velykobrytaniia vidmovytsia vid posluh Huawei v 5G' (*ITsider,* 07.07.2020) <https://itsider.com.ua/velykobrytaniya-vidmovytsya-vid-poslug-huawei-v-5g> (accessed: 20.08.2022) (in Ukrainian).

Taras Tkachuk
Natalia Tkachuk

ANTIFRAGILE STRATEGY IN CYBER SECURITY OF UKRAINE: LEGAL ASPECT

Abstract. State cybersecurity directly affects the stability of all critical areas: military, economics, foreign policy, medicine, education and more. The state, represented by the authorities, can implement effective cyberpolicies and use expensive IT systems, but if the state has lower standards of cybersecurity than our international partners, operational processes at the tactical level may be jeopardized. In fact, in this context, the role of the legal factor is paramount. The implementation of tested standards and their implementation in national legislation should be fairly rapid, as well as synchronous with the major players in the international arena.

In the context of a war intensified by total digitalisation, the issues of legal regulation of data preservation, management of IT systems, rapid and effective recovery in the event of cyberattacks are becoming key resources for success in cyber warfare and countering cyberthreats.

All this necessitates the search for new, more effective cybersecurity strategies. The national cybersecurity system must not only meet the challenges and threats of the environment, adapt to new conditions, but also strengthen its own capabilities in the face of unpredictability. In our opinion, one of such topical strategies may be the antifragile strategy.

The aim of the article. The aim of this article is to extrapolate the main threats to cybersecurity of the state, as well as opportunities to counter them on N. Taleb's antifragile strategy. Development on this basis of specific proposals for improving national information legislation in terms of cybersecurity of the state.

The article outlines the characteristic threatening markers of the modern cyber era:

1. Propaganda took new forms both in the context of military aggression and in defense, the active dissemination of misinformation by the aggressor state, distortion of information, as well as justifying or denying the armed aggression of russia against Ukraine.

2. Vulnerability to cyber threats of critical infrastructure, communications systems, space industry, etc.

3. Emergence of new types of threats related to manipulation.

4. The real threats to the global information society and to everyone are: the militarization of cyberspace, the outbreak of large-scale information wars, the spread of extremist and manipulative materials, destructive information and psychological influences on individual, group and public consciousness, the use of artificial intelligence in the military.

The article analyzes the international and national information legislation. On this basis, it is proved that the legal factor is a basic element of the cybersecurity system. In this context, Ukraine needs a number of fundamentally important areas to improve information legislation in the field of cybersecurity.

It is concluded that the black swans risks and threats require cyberspace to be antifragile, the ability to renew and benefit from unexpected shocks. Today we must look for opportunities to act ahead. To do this, we will have to use a comprehensive approach that includes legal, personnel and organizational measures aimed at: analysis

ПРАВО УКРАЇНИ • 2022 • № 8 • 76-94

and assessment not only of well-known risks and threats faced by the cybersecurity system in the past, but also of those related to Black Swans, unpredictable events; development of various forecast scenarios, which seem to be the most significant for the security of states; building operational recovery programs in case of cyber threats; creation of mechanisms of active defense in cyberspace.

The system of these fundamental measures will be our antifragile strategy in the face of both war and the ever-changing risks of our dynamic society.

It is proved that the development of the digital environment, end-to-end digital platforms, technologies, etc. has become the foundation for the emergence and development of new social relations, which needs a clear legal regulation.

At the same time, the new stage of cyber threats, demonstrated during the russian-Ukrainian war, requires further improvement of the strategy to counter them. The national cybersecurity system must not only effectively deter destructive actions in cyberspace, achieve cyber resilience at all levels and the interaction of all actors in cybersecurity, but also strengthen its capabilities in conditions of unpredictability and uncertainty, armed aggression against Ukraine. It should be based on a common international legal framework, the exchange of such threats in real time, the further development of partnerships at all levels: international, state and, especially, state-partnership. Priority of new approaches should be based on legal approaches to the introduction of new information and communication technologies, legal limits of artificial intelligence, Internet of Things, including in the military sphere, strengthening legal responsibility for the use of cyberspace against peace, life and dignity, negative information impacts, conflict resolution, etc.

The processes of technological development of the cybersphere in the coming years will tend to dynamic development in all spheres of society, especially the military, the world is unthinkable without purposeful global informatization. Therefore, information law has a prominent place as a regulator of these processes, as well as a powerful mechanism for improving the protection of social facilities from aggressive cyber influence.

Keywords: anti-fragility; cybersecurity; cyber threats; information law; information legislation.