Адміністративне право і процес; фінансове право; інформаційне право

УДК 004.056.5
DOI 10.33244/2617-4154.4(21).2025.9-17

А. В. Гарбінська-Руденко,
кандидат юридичних наук, доцент,
Державний податковий університет
email: prokyror.irpin@i.ua
ORCID ID 0000-0002-0971-1234;
М. О. Кучко,
здобувачка вищої освіти ННІ права,
Державний податковий університет
email: mariiakuchko@gmail.com
ORCID ID 0009-0004-5639-6152

ВПЛИВ КІБЕРЗАГРОЗ НА НАЦІОНАЛЬНУ БЕЗПЕКУ ДЕРЖАВИ

У статті досліджено трансформацію кіберзагроз 2022–2024 рр. та їхній вплив на національну безпеку України в умовах повномасштабної гібридної агресії. Розкрито теоретико-правові засади аналізу кіберзагроз, визначено їхні ключові види та суб'єктів походження, окреслено особливості технічних, інформаційно-психологічних і змішаних атак. Показано, що кібератаки проти енергетичної, транспортної та урядової інфраструктури мають системний характер, формують стійкі ризики для функціонування державних інституцій та вимагають високого рівня координації між суб'єктами безпеки. Проаналізовано інформаційні операції, спрямовані на підрив громадської довіри, маніпулювання суспільними настроями та послаблення політичної стабільності. Акцентовано на тому, що кіберзагрози мають потужний економічний та оборонний ефект, оскільки здатні порушувати критичні процеси, комунікації та логістичні ланцюги.

Окрему увагу приділено чинним стратегіям протидії, зокрема нормативній базі, діяльності ДССЗЗІ, CERT-UA, НКЦК та правоохоронних органів, а також практиці міжнародної співпраці України з ЄС і НАТО. Доведено, що попри сформовану інституційну інфраструктуру, актуальним залишається питання гармонізації законодавства з Директивою NIS2, посилення галузевих SOC / CSIRT-центрів і вдосконалення механізмів обміну кіберінформацією. Підкреслено перспективність інноваційних рішень, зокрема використання штучного інтелекту, автоматизованих систем реагування та національних кіберполігонів. Зроблено висновок, що підвищення кіберстійкості держави потребує

комплексного поєднання правових, організаційних і технологічних заходів поряд із розвитком культури кібергігієни. Підсумовано, що інноваційні технології та автоматизовані системи реагування мають суттєво підвищити ефективність протидії кіберзагрозам. Акцентовано увагу на тому, що результативність вказаних заходів значно залежить від узгодженості дій усіх суб'єктів забезпечення національної безпеки держави.

Ключові слова: *кіберзагрози, національна безпека, кіберпростір, інформаційні операції, інформаційні системи, кіберзахист.*

Постановка проблеми. Війна росії проти України спричинила різке зростання кількості кіберінцидентів, спрямованих на підрив функціонування державних інституцій, блокування критичних сервісів та дестабілізацію суспільних процесів. Кіберпростір перетворився на повноцінний інструмент ведення війни, де атаки на урядові ресурси, масові фішингові кампанії, втручання у роботу об'єктів критичної інфраструктури та поширення дезінформації використовуються як складові комплексного впливу на державу. У таких умовах будь-яка вразливість інформаційних систем набуває стратегічного значення, адже наслідки успішних кібератак здатні призвести до збоїв у роботі енергетичних, фінансових, транспортних та оборонних секторів, що безпосередньо впливає на стійкість національної безпеки.

Зростання масштабів цифрових загроз виявило ряд системних проблем, які послаблюють спроможність держави ефективно реагувати на сучасні кібероперації. Ідеться про нерівномірний розвиток інфраструктури захисту, потребу в системній модернізації технічних рішень, дефіцит висококваліфікованих фахівців і необхідність гармонізації законодавчих механізмів із міжнародними стандартами. Технологічні зміни випереджають темпи оновлення регуляторної бази, що створює додаткові ризики для захисту державних ресурсів і ускладнює координацію між суб'єктами сектору безпеки та оборони.

Аналіз останніх досліджень і публікацій. Питання кіберзагроз і кібербезпеки розглядаються в працях таких авторів: Д. М. Казмірук [1], Р. Ф. Черниш, О. В. Пірог, П. Ю. Грушевська [4], Г. Ліна, Дж. Керра [8], Т. Кульчицького, К. Резворовича, М. Поваленої, С. Дутчака, Р. Крамар [2] та ін. Незважаючи на широку представленість теми в сучасних дослідженнях, наявні публікації демонструють фрагментарність окремих аспектів цифрової безпеки, швидку змінюваність кіберзагроз і постійне ускладнення їхніх форм. Стрімка еволюція технологій, поява нових типів атак, зростання ролі штучного інтелекту в кібершкідництві та необхідність адаптації до стандартів ЄС обумовлюють потребу в подальших системних дослідженнях.

Метою статті є всебічний аналіз кіберзагроз, спрямованих проти держави, аналіз їхнього впливу на національну безпеку та визначення стратегічних напрямів удосконалення системи протидії.

Виклад основного матеріалу. На сьогодні кіберзагроза є однією із ключових складових загроз національній безпеці, тісно пов'язаних з інформаційною, воєнною, економічною та політичною безпекою держави. Д. М. Казмірук визначає інформаційну

безпеку як системну умову збереження стійкості держави в умовах повномасштабної війни, підкреслюючи, що кіберзагрози є інструментом впливу як на інфраструктуру, так і на масову свідомість [1, с. 22]. Р. Ф. Черниш, О. В. Пірог та П. Ю. Грушевська пропонують розглядати загрози державній безпеці в інформаційній сфері як систему умов і чинників, здатних завдати шкоди життєво важливим інтересам через деструктивний вплив інформації на свідомість і поведінку громадян, а також через ураження інформаційних систем і ресурсів [4, с. 48].

Вважаємо, що під кіберзагрозами потрібно розуміти сукупність потенційних і реальних дій у кіберпросторі, спрямованих на порушення конфіденційності, цілісності й доступності інформаційних ресурсів держави, а також на маніпулювання інформаційними потоками з метою впливу на політичні процеси, економічну стабільність та обороноздатність. У політичному просторі кіберзагрози проявляються не лише у формі атак на інфраструктуру, а й як інструмент політичного тиску, дискредитації інститутів влади та формування вигідних агресору інформаційних наративів.

Варто виділяти три основні групи кіберзагроз. До перших – технічних загроз – належать атаки, безпосередньо спрямовані на інформаційно-комунікаційні системи та мережі: шкідливе програмне забезпечення, DDoS-атаки, несанкціонований доступ, втручання в роботу сервісів критичної інфраструктури. У звітах ENISA підкреслюється, що саме технічні атаки на доступність і цілісність даних (ransomware, порушення роботи DNS, компрометація хмарних сервісів) залишаються серед домінантних загроз для державних органів і провайдерів послуг [6, с. 16].

Другу групу становлять інформаційно-психологічні загрози, фокус яких зміщується з ураження інфраструктури на вплив на індивідуальну та колективну свідомість. Ідеться про цілеспрямовані кампанії дезінформації, маніпулятивне використання соціальних мереж, інформаційно-психологічні операції, спрямовані на деморалізацію населення, підрив довіри до державних інституцій та партнерів, розпалювання внутрішніх конфліктів. Д. М. Казмірук наголошує, що «у воєнних умовах інформаційний компонент набуває екзистенційного значення, оскільки недостовірна або спеціально викривлена інформація здатна суттєво впливати на прийняття рішень на державному рівні» [1, с. 25].

Третя група загроз охоплює змішані, або гібридні, кіберзагрози, які поєднують технічні та інформаційно-психологічні інструменти. У такому форматі технічні атаки на інформаційні системи супроводжуються інформаційними кампаніями, що посилюють панічні настрої або дискредитують здатність держави реагувати на інцидент. Р. Ф. Черниш підкреслює, що «в українських реаліях гібридні кіберзагрози часто синхронізуються з воєнними та політичними подіями, підсилюючи ефект від воєнних дій у фізичному просторі» [4, с. 49].

Динаміка кіберінцидентів після 2022 р. свідчить про системний, а не епізодичний характер загроз (рис. 1.1). За даними Державної служби спеціального зв’язку та захисту інформації, 2022 р. в Україні зареєстровано 2 194 кіберінциденти, що майже утричі перевищує показники 2021 р. Найбільше зросла частка подій, пов’язаних із шкідливим програмним кодом і несанкціонованим збором інформації [7, с. 4].

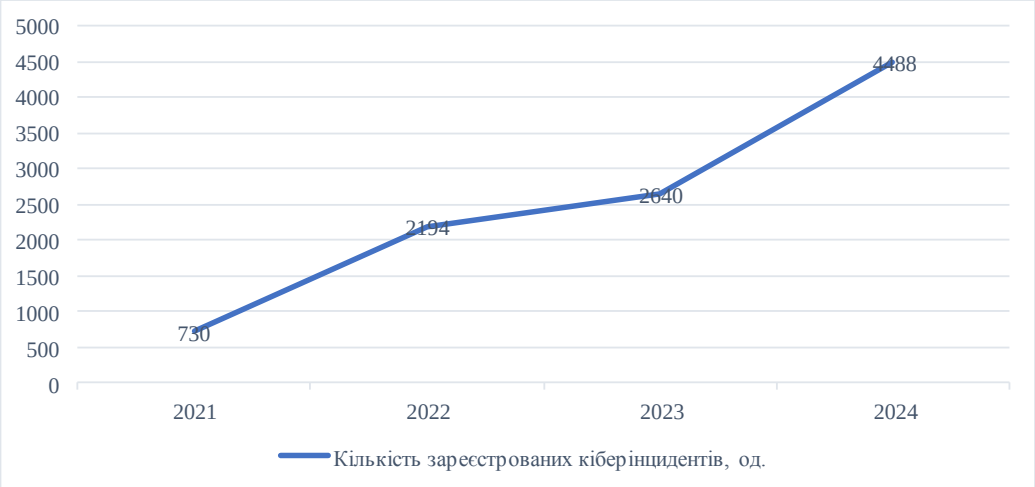

Рисунок 1.1 – Динаміка кіберінцидентів в Україні 2021–2024 рр.
Джерело: складено автором на основі [7; 10].

Упродовж 2023–2024 рр. фіксують подальше нарощування активності ворожих угруповань: кількість атак на українські державні органи, військові структури та об'єкти критичної інфраструктури збільшується, причому значну їх частину здійснюють групи, пов'язані з військовою розвідкою держави-агресора [7, с. 6–7; 10, с. 5]. 2024 року загальна кількість зареєстрованих кібератак на українську інфраструктуру зросла орієнтовно на 70 % порівняно з 2023 р., що свідчить про тривалу ескалацію кіберфронту.

Особливо небезпечним виміром кіберзагроз є атаки на критичну інфраструктуру держави. Енергетичний сектор, транспортні системи, урядові інформаційні ресурси розглядаються противником як пріоритетні цілі, оскільки їхнє виведення з ладу навіть на нетривалий час здатне дестабілізувати функціонування органів державної влади та створити панічні настрої серед населення. Офіційні звіти й технічні розслідування засвідчують застосування проти українських енергетичних компаній шкідливих програм на кшталт wiper, зокрема NikoWiper, які поєднуються з ракетними ударами по енергетичній інфраструктурі [7, с. 8–9].

У спеціалізованих дайджестах Національного координаційного центру кібербезпеки підкреслюється тенденція до координації кібератак із масованими обстрілами об'єктів енергетики, що ускладнює відновлення їхньої роботи та підвищує ризики тривалих перебоїв з електро- й теплопостачанням [10, с. 10–11]. Вразливість транспортної та логістичної інфраструктури проявляється у спробах блокування інформаційних систем перевізників, порушення роботи квиткових сервісів, навігаційних і диспетчерських комплексів, а також у зростанні зацікавленості противника до систем управління залізничними перевезеннями. Урядові інформаційні ресурси залишаються постійними об'єктами фішингових кампаній, DDoS-атак і спроб модифікації контенту, що ставить під загрозу безперервність надання електронних послуг і довіру громадян до державних цифрових сервісів [9, с. 11].

Кібератаки проти критичної інфраструктури України нерідко мають транскордонний ефект. Прикладом поєднання технічної атаки на телекомунікаційну інфраструктуру із широкими геополітичними наслідками став інцидент із атакою на супутникову мережу KA-SAT компанії Viasat у лютому 2022 р. У день початку повномасштабного вторгнення зловмисники застосували шкідливе програмне забезпечення на кшталт wiper, яке вивело з ладу десятки тисяч модемів супутникового зв'язку, що використовувалися, зокрема, для забезпечення військових та урядових комунікацій України, а також спричинило порушення роботи енергетичної інфраструктури в окремих країнах ЄС [9, с. 12].

Інший блок загроз стосується інформаційного суверенітету та масованих інформаційно-психологічних операцій, які супроводжують технічні кібератаки. Аналітичні доповіді Організації Північноатлантичного договору, Європейського Союзу та провідних дослідницьких центрів фіксують систематичне використання державою-агресором інструментів кіберзасобів для поширення дезінформації, підриву довіри до демократичних інститутів, дискредитації Збройних Сил України та її міжнародних партнерів [8, с. 265].

Застосування бот-мереж, фабрик тролів, скоординованих інформаційних кампаній у соціальних мережах поєднується з таргетованим використанням персональних даних, викрадених унаслідок кібершахрайства, для мікротаргетингу та посилення поляризації в суспільстві. Служба безпеки України та кіберполіція регулярно повідомляють про ліквідацію ботоферм, виявлення підроблених петицій, фейкових сайтів органів влади, а також спеціальних операцій, спрямованих на компрометацію акаунтів військовослужбовців і волонтерів через месенджери та соціальні мережі [5, с. 12–13]. Такі кампанії не лише поширюють фейки про хід війни чи внутрішньополітичну ситуацію, а й прагнуть підірвати довіру до офіційних джерел інформації, створити відчуття безперспективності спротиву.

Функціонування соціальних мереж перетворюється на чинник інформаційної безпеки. Алгоритмічні механізми ранжування контенту сприяють вірусному поширенню емоційно забарвлених повідомлень, що використовують пропагандистські наративи, маніпулятивні візуальні матеріали, deepfake-відео та псевдоекспертні оцінки. У результаті формується багаторівнева загроза інформаційному суверенітету держави: від підміни фактів і нав'язування вигідної агресору картини подій до довгострокового викривлення історичної пам'яті й ціннісних орієнтирів суспільства. Така модель інформаційно-психологічного впливу ґрунтується на поєднанні технічних кіберзасобів (злам акаунтів, DDoS ресурсів засобів масової інформації, блокування сайтів) із маніпуляцією смислами, образами та емоціями, що робить її особливо небезпечною в умовах війни [4, с. 49].

Кіберзагрози мають складний економічний, оборонний і політичний вимір. З економічного погляду прямі збитки від зупинки інформаційних систем банків, промислових підприємств, логістичних операторів поєднуються з опосередкованими втратами від порушення ланцюгів постачання, простою виробництва та зниження інвестиційної привабливості держави. Вважаємо, що успішні кібератаки на фінансовий

сектор та енергетику здатні створювати ефект «ланцюгової реакції», коли локальний інцидент провокує ширші макроекономічні дисбаланси.

В оборонній сфері особливу небезпеку становлять спроби враження систем зв'язку, управління військами, логістичних платформ і супутникових каналів передачі даних, що може обмежувати спроможність Збройних Сил України оперативно реагувати на зміну обстановки, координувати дії підрозділів і взаємодіяти з партнерами. Політичний вимір кіберзагроз проявляється у втручанні в електоральні процеси, маніпулюванні громадською думкою щодо зовнішньополітичного курсу держави, дискредитації керівництва та інституцій публічної влади [8, с. 266]. В інформаційному просторі України фіксуються спроби нав'язати суспільству наративи про «неефективність» демократичних інститутів, «непотрібність» євроінтеграції, «безперспективність» продовження оборони, що розглядається як елемент довгострокової стратегії підриву національної стійкості.

Проте, попри відчутний прогрес, все ж існує ряд структурних проблем у забезпеченні кібербезпеки. Правове регулювання кібербезпеки в Україні відстає від фактичної динаміки кіберзлочинності, що породжує «правовий вакуум» у кваліфікації нових видів посягань, пов'язаних, зокрема, із використанням штучного інтелекту, складними розподіленими інфраструктурами та гібридними операціями. А. Давидюк та О. Потій вказують, що «наявна модель кіберуправління характеризується фрагментованістю компетенцій, різним рівнем спроможності секторів, обмеженою інтегрованістю державних SOC-платформ, а також частковою гармонізацією з правом ЄС, насамперед у частині повноцінної імплементації вимог NIS2 щодо обов'язкової оцінки ризиків і звітності операторів критичних послуг» [5, с. 241–242]. Дорадчі аналітичні огляди щодо кібербезпеки України в контексті євроінтеграції підкреслюють, що без завершення адаптації законодавства до NIS2 та побудови дієвого національного механізму нагляду Україна ризикує зберегти «сіру зону» в захисті критичної інфраструктури та фінансового сектору [3].

Висновки. Отже, розвиток стратегій протидії потребує зосередження уваги на декількох групах заходів:

– по-перше, доцільно оновити Закон України «Про основні засади забезпечення кібербезпеки України» [11] з урахуванням сучасних викликів і положень NIS2, чітко розмежувавши категорії операторів основних послуг, цифрових сервісів, критичної та особливо критичної інфраструктури та запровадивши єдині вимоги до risk-based управління, інцидент-репортингу й аудиту безпеки;

– по-друге, потребує подальшої інституційної консолідації система координації між Радою національної безпеки і оборони України, Державною службою спеціального зв'язку та захисту інформації України, Міністерством цифрової трансформації України, Національним банком України, секторними регуляторами й правоохоронними органами, зокрема через формування інтегрованої мережі національних і галузевих центрів реагування на інциденти комп'ютерної безпеки й оперативних центрів безпеки, єдиних стандартів обміну кіберінформацією та спільних протоколів реагування на багатоцільові атаки;

– по-третє, важливо розширити практику комплексних міжвідомчих навчань, кіберполігонів і симуляційних вправ для органів державної влади, операторів енергетичного, транспортного та фінансового секторів, що вже апробується у форматі

міжнародних кібернавчань Locked Shields, спеціалізованих тренінгів CIREX.Cyber.Ransomware, а також національних тренувань.

Аналіз динаміки кіберзагроз і стану національної системи кіберзахисту переконливо показує, що цифровий вимір безпеки став одним із визначальних полів протистояння. Кібератаки останніх років засвідчили: ураження інформаційних систем, порушення роботи критичних сервісів і цілеспрямовані інформаційні операції здатні впливати на державу не менш відчутно, ніж традиційні військові дії. Реакція України на ці виклики поступово набуває комплексного характеру завдяки інституційному посиленню, міжнародній взаємодії й упровадженню сучасних технічних рішень.

Водночас система кіберзахисту потребує подальшого розвитку: гармонізації законодавства з європейськими стандартами, розбудови галузевих центрів реагування, пришвидшення обміну кіберінформацією й розширення кадрового потенціалу. Інноваційні технології та автоматизовані системи реагування здатні суттєво підвищити ефективність протидії кіберзагрозам, однак їхня результативність залежить від узгодженості дій усіх суб'єктів забезпечення національної безпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Казмірук Д. М. Інформаційна безпека як складова національної безпеки в умовах повномасштабної війни. *Політикус.* 2025. № 1. С. 21–26.

2. Правове регулювання кібербезпеки в контексті цифрової трансформації українського суспільства / Кульчицький Т., Резворович К., Повалена М., Дутчак С., Крамар Р. *Lex Humana*. 2024. № 16 (1). С. 443–460.

3. Україна представила проєкт Національної стратегії кібергігієни: новий стандарт цифрової грамотності до 2030 року / Офіційний вебсайт РНБО України. 2025. 13 листопада. URL : https://www.rnbo.gov.ua (дата звернення: 20.11.2025).

4. Chernysh R. F., Piroh O. V., Hrushevska P. Yu. Threats to the state security of Ukraine in the information sphere in the realities of the Russian-Ukrainian war. *The Scientific Journal of the National Academy of the National Guard of Ukraine.* 2024. С. 45–52.

5. Davydiuk O., Potii O. National Cybersecurity Governance: Ukraine. Tallinn: *NATO CCDCOE*. 2024. 38 p.

6. ENISA Threat Landscape 2022 / European Union Agency for Cybersecurity. 2022. 116 p.

7. ENISA Threat Landscape 2023 / ENISA. European Union Agency for Cybersecurity. URL : https://www.enisa.europa.eu (дата звернення: 27.11.2025).

8. Lin H., Kerr J. On cyber-enabled information warfare and information operations. In: Cornish P. (ed.). The Oxford Handbook of Cyber Security. Oxford : Oxford University Press, 2022. P. 251–272.

9. National Coordination Cybersecurity Center. Cyber Digest. April 2024. Київ : РНБО України, 2024. 18 с.

10. National Coordination Cybersecurity Center. Review of Cybersecurity News in Ukraine, Tendencies, and World Events Related to the First World Cyber War. Cyber Digest. February 2023. Київ : РНБО України, 2023. 23 с.

11. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовтня 2017 року № 2163-VIII. URL : https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 27.11.2025).

REFERENCES

1. Kazmiruk D. M. Informatsiina bezpeka yak skladova natsionalnoi bezpeky v umovakh povnomasshtabnoi viiny. *Politykus.* 2025. № 1. S. 21–26.

2. Pravove rehuliuvannia kiberbezpeky v konteksti tsyfrovoi transformatsii ukrainskoho suspilstva / Kulchytskyi T., Rezvorovych K., Povalena M., Dutchak S., Kramar R. *Lex Humana*. 2024. 16 (1). S. 443–460.

3. Ukraina predstavyla proiekt Natsionalnoi stratehii kiberhihiieny: novyi standart tsyfrovoi hramotnosti do 2030 roku / Ofitsiinyi sait RNBO Ukrainy. 2025. 13.11. URL : https://www.rnbo.gov.ua (data zvernennia: 20.11.2025).

4. Chernysh R. F., Piroh O. V., Hrushevska P. Yu. Threats to the state security of Ukraine in the information sphere in the realities of the Russian-Ukrainian war. *The Scientific Journal of the National Academy of the National Guard of Ukraine.* 2024. S. 45–52.

5. Davydiuk O., Potii O. National Cybersecurity Governance: Ukraine. Tallinn : NATO CCDCOE, 2024. 38 p.

6. ENISA Threat Landscape 2022 / European Union Agency for Cybersecurity. 2022. 116 p.

7. ENISA Threat Landscape 2023 / ENISA. European Union Agency for Cybersecurity. URL : https://www.enisa.europa.eu (data zvernennia: 27.11.2025).

8. Lin H., Kerr J. On cyber-enabled information warfare and information operations. In: Cornish P. (ed.). The Oxford Handbook of Cyber Security. Oxford : Oxford University Press, 2022. P. 251–272.

9. National Coordination Cybersecurity Center. Cyber Digest. April 2024. Kyiv : RNBO Ukrainy, 2024. 18 c.

10. National Coordination Cybersecurity Center. Review of Cybersecurity News in Ukraine, Tendencies, and World Events Related to the First World Cyber War. Cyber Digest. February 2023. Kyiv : RNBO Ukrainy, 2023. 23 c.

11. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy : Zakon Ukrainy vid 5 zhovtnia 2017 roku № 2163-VIII. URL : https://zakon.rada.gov.ua/laws/show/2163-19#Text (data zvernennia: 27.11.2025).

A. V. Harbinska-Rudenko, M. O. Kuchko. IMPACT OF CYBER THREATS ON NATIONAL SECURITY OF THE STATE

The article examines the transformation of cyber threats in 2022–2024 and their impact on the national security of Ukraine in the context of full-scale hybrid aggression. The theoretical and legal principles of analyzing cyber threats are revealed, their key types and subjects of origin are identified, and the features of technical, information-psychological and mixed attacks are outlined. It is shown that cyber attacks against energy, transport and government infrastructure are systemic in nature, create persistent risks for the functioning of state institutions and require a high level of coordination between security actors. Information operations aimed at undermining public trust, manipulating public sentiment and weakening

political stability are analyzed. It is emphasized that cyber threats have a powerful economic and defense effect, as they are capable of disrupting critical processes, communications and logistics chains.

Special attention is paid to the current countermeasure strategies, in particular the regulatory framework, the activities of the State Cybersecurity and Information Security Service, CERT-UA, the National Cybersecurity Center and law enforcement agencies, as well as the practice of international cooperation of Ukraine with the EU and NATO. It is proved that despite the established institutional infrastructure, the issue of harmonizing legislation with the NIS2 Directive, strengthening industry SOC / CSIRT centers and improving mechanisms for exchanging cyber information remains relevant. The prospects of innovative solutions are emphasized, in particular the use of artificial intelligence, automated response systems and national cyber training grounds. It is concluded that increasing the cyber resilience of the state requires a comprehensive combination of legal, organizational and technological measures along with the development of a culture of cyber hygiene. It is concluded that innovative technologies and automated response systems should significantly increase the effectiveness of countering cyber threats. Attention is focused on the fact that the effectiveness of these measures depends significantly on the coordination of actions of all entities ensuring the national security of the state.

Keywords: *cyber threats, national security, cyberspace, information operations, information systems, cyber defense.*

Стаття надійшла до редколегії 3 листопада 2025 року