УДК 004.42:005.8
DOI https://doi.org/10.32782/IT/2024-4-5

Володимир БОГОМ'Я
доктор технічних наук, професор, професор кафедри кібербезпеки, інформаційних технологій та економіки, Київський університет інтелектуальної власності та права Національного університету «Одеська юридична академія», Харківське шосе, 210, Київ, Україна, 02121
***ORCID:** 0000-0003-4403-3130*

Валентин ГАЛУНЬКО
доктор філософії з галузі права, доцент кафедри адміністративного права, інтелектуальної власності та цивільно-правових дисциплін, Київський університет інтелектуальної власності та права Національного університету «Одеська юридична академія», Харківське шосе, 210, Київ, Україна, 02121
***ORCID:** 0000-0002-8133-6766*

Бібліографічний опис статті*:* Богом'я, В., Галунько, В. (2024). Правове регулювання кібербезпеки в контексті захисту критичної інфраструктури*. Information Technology: Computer Science, Software Engineering and Cyber Security,* 4, 35–42, doi: https://doi.org/10.32782/IT/2024-4-5

ПРАВОВЕ РЕГУЛЮВАННЯ КІБЕРБЕЗПЕКИ В КОНТЕКСТІ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

В статті здійснено аналіз дослідження забезпечення кібербезпеки об'єктів критичної інфраструктури (далі – КІ), яке є одним з найважливіших викликів для сучасності. Кібератаки на об'єкти критичної інфраструктури можуть мати руйнівні наслідки для національної безпеки, економіки та суспільства. З огляду на зростання кількості та витонченості кіберзагроз, особливого значення набуває ефективне правове регулювання у цій сфері.

***Мета роботи.** Комплексний аналіз національного правового регулювання кібербезпеки з точки зору захисту критичної інфраструктури, виявлено проблеми в чинному законодавстві та надано конкретні рекомендації щодо його вдосконалення з урахуванням сучасних викликів та міжнародного досвіду. Для досягнення поставленої мети було використано наступний комплекс наукових методів Зокрема, аналіз та синтез нормативно-правових актів, проаналізовано тексти законів, стратегій та стандартів у сфері кібербезпеки та захисту інформаційної безпеки.*

***Методологія.** Розгляд правового регулювання як складної системи, що складається із взаємопов'язаних елементів методом узагальнення формулюючи загальність висновків на основі аналізу та синтезу. Основні закони, що регулюють питання кібербезпеки КІ в Україні. Особливу увагу приділено аналізу визначень ключових термінів, розподілу повноважень між державними органами, встановленню вимог до кіберзахисту та визначенню відповідальності за порушення у сфері кібербезпеки.*

***Наукова новизна.** комплексний аналіз правового регулювання кібербезпеки критичної інфраструктури в Україні з урахуванням, зокрема, поточних викликів, спричинених збройним нападом російської федерації, та міжнародного досвіду, і виявляє низку проблем у чинному законодавстві. Деякі ключові терміни не мають чіткого визначення, що ускладнює правозастосування, що існують проблеми з координацією між різними державними органами, відповідальними за кібербезпеку інформації та комунікацій, а також що існуючі механізми контролю за дотриманням законодавства є неефективними. Підвищення ефективності захисту об'єктів критичної інфраструктури від кіберзагроз, а також розглядають необхідність диференціації регуляторних підходів відповідно до критичності об'єкта.*

***Висновки.** Проведене дослідження дозволило зробити низку важливих висновків щодо поточного стану правового регулювання кібербезпеки критичної інфраструктури в Україні та визначити основні напрями його вдосконалення.*

Зокрема, необхідно уточнити термінологію, оптимізувати розподіл повноважень між органами державної влади, посилити вимоги до кібербезпеки та підвищити відповідальність за порушення. Реалізація запропонованих заходів дозволить підвищити рівень захисту критичної інфраструктури України від кіберзагроз.

***Ключові слова:** кібербезпека, критична інфраструктура, правове регулювання, кіберзагрози, законодавство, відповідальність, державні органи, міжнародний досвід, кіберзахист.*

Volodymyr BOHOMIA
Doctor of Technical Sciences, Professor, Professor at the Department of Cyber Security, Information Technology and Economics, Kyiv University of Intellectual Property and Law of the National University «Odessa Law Academy», 210, Kharkivske highway, Kyiv, Ukraine, 02121, bog2603@ukr.net
***ORCID:** 0000-0003-4403-3130*

Valentyn HALUNKO
PhD in law, Associate Professor at the Department of Administrative Law, Intellectual Property and Civil-Law Disciplines, Kyiv University of Intellectual Property and Law of the National University «Odessa Law Academy», 210, Kharkivske highway, Kyiv, Ukraine, 02121, valentinvalentin0987@gmail.com
***ORCID:** 0000-0002-8133-6766*

To cite this article: Bohomia, V., Halunko, V. (2024). Pravove rehuliuvannia kiberbezpeky v konteksti zakhystu krytychnoi infrastruktury [Legal regulation of cybersecurity in the context of critical infrastructure protection]. *Information Technology: Computer Science, Software Engineering and Cyber Security,* 4, 35–42, doi*:* https://doi.org/10.32782/IT/2024-4-5

LEGAL REGULATION OF CYBERSECURITY IN THE CONTEXT OF CRITICAL INFRASTRUCTURE PROTECTION

The article analyses the study of ensuring cybersecurity of critical infrastructure (hereinafter – CI), which is one of the most important challenges for today. Cyberattacks on critical infrastructure facilities can have devastating consequences for national security, the economy and society. Given the growing number and sophistication of cyber threats, effective legal regulation in this area is of particular importance.

***Objective.** To provide a comprehensive analysis of the national legal regulation of cybersecurity in terms of critical infrastructure protection, to identify problems in the current legislation and to provide specific recommendations for its improvement, taking into account current challenges and international experience. To achieve this goal, the following set of scientific methods was used In particular, the analysis and synthesis of legal acts, the texts of laws, strategies and standards in the field of cybersecurity and information security protection were analysed.*

***Scientific novelty.** a comprehensive analysis of the legal regulation of critical infrastructure cybersecurity in Ukraine, taking into account, in particular, the current challenges caused by the armed attack of the Russian Federation and international experience, and identifies a number of problems in the current legislation. Some key terms are not clearly defined, which complicates law enforcement, that there are problems with coordination between different government agencies responsible for cybersecurity of information and communications, and that existing mechanisms for monitoring compliance with the law are ineffective. Improving the effectiveness of protecting critical infrastructure against cyber threats, and considering the need to differentiate regulatory approaches according to the criticality of the facility.*

***Conclusions.** This study has made it possible to draw a number of important conclusions about the current state of legal regulation of critical infrastructure cybersecurity in Ukraine and to identify the main areas for its improvement.*

In particular, it is necessary to clarify the terminology, optimise the distribution of powers between public authorities, strengthen cybersecurity requirements and increase liability for violations. Implementation of the proposed measures will increase the level of protection of Ukraine's critical infrastructure from cyber threats.

***Key words:** critical infrastructure, cyber defence, cyber threats, cybersecurity, government agencies, international experience, legal regulation, legislation, liability.*

Актуальність проблеми. В умовах стрімкого розвитку інформаційних технологій та глобальної цифровізації, кібербезпека набуває стратегічного значення для забезпечення стабільного функціонування та захисту національних інтересів. Кіберпростір становить невід'ємною частиною сучасного світу, забезпечуючи функціонування критично важливих сфер суспільного життя, таких як наприклад енергетика, транспорт, фінанси, телекомунікації, охорона здоров'я тощо. Сукупність цих об'єктів визначається як критична інфраструктура (далі – КІ). Критична інфраструктура є особливо вразливою до кібератак через свою складність, взаємозалежність та потенційно катастрофічні наслідки від збоїв у її роботі. Кібератаки на КІ можуть призвести не лише до задання економічного дисбалансу надаючи значущих збитків та, і порушення надання важливих послуг, і, до загрози життя та здоров'я громадян, тобто дестабілізації ситуації в країні в цілому. Каскадний ефект від ураження одного елемента КІ може призвести до збоїв у роботі інших секторів, що підкреслює необхідність комплексного та надійного захисту в кіберпросторі. Збройна агресія російської федерації проти України у 2022 році суттєво змінила ландшафт кіберзагроз. Кіберпростір став ареною активних

бойових дій, де кібератаки використовуються як інструмент гібридної війни для досягнення військових та політичних цілей. Збільшилась кількість цілеспрямованих та скоординованих атак, спрямованих на дестабілізацію роботи органів виконавчої влади, порушення функціонування об'єктів КІ та поширення дезінформації. Враховуючи зазначені фактори, ефективне правове регулювання кібербезпеки КІ є критично важливим для забезпечення національної безпеки та стабільного функціонування держави в цілому. Необхідно створити чітку та дієву правову базу, яка б визначала обов'язки суб'єктів КІ, повноваження, механізмів тощо.

Аналіз останніх досліджень і публікацій. Визначено та класифіковано у яких присвячені роботи таких українських вчених, як: О. Алексеєва (Алексеєва О.А., 2023), Б. Ворович, С. Єсімов, Х. Кайдрович, Ю. Кемська (Ковалів М., Скриньковський Р., Назар Ю., та ін., 2021), С. Князь, М. Ковалів, І. Красницький, Ю. Назар, В. Пядишев (Пядишев В. Г., 2022), П. Рогов, О. Скіцько, Р. Скриньковський, В. Ткаченко (Рогов П. Д. Ворович Б. О., Ткаченко В. А., 2017), Р. Ширшов (Скіцько О. І., Ширшов Р. А., 2024), і також які досліджували іноземний досвід: Б. Леонов, В. Серьогін (Леонов Б. Д., Шостак Р. М., Серьогін В. С., 2020), Р. Шостак із зарубіжних дослідників можна зазначити Д. Фідлера (Fidler D., 2015) та ін.

Метою статті є аналіз ключових нормативно-правових актів України, що регулюють кібербезпеку критичної інфраструктури, з метою виявлення прогалин та колізій у законодавчому регулюванні та формулювання рекомендацій щодо їх усунення.

Виклад основних положень. Особливого значення захисту критичної інфраструктури набув в 1990-х роках у США відповідь на тероризм і зростаючий зв'язок між критичною інфраструктурою і кібертехнологіями та глобальне поширення інтернету, в той же час які розробляли міжнародне право для регулювання цього процесу. Поширення попередніх комунікаційних технологій підштовхнуло до створення міжнародного права та інституцій щодо посилення захисту КІ. Як наслідок, держави світу почали використовувати міжнародно-правові механізми для зміцнення кіберзахисту своєї національної критичної інфраструктури (Fidler D., 2015).

Виявимо розуміння до понять кібербезпеки в контексті захисту критичної інфраструктури потрібно дамо виділити особливу роль термінувань таких понять як критична інфраструктура, кібербезпека, кібератака, кіберзагроза та кіберінцидент. Так, Закон України від 16.11.2021 року «Про критичну інфраструктуру» визначає дефініцію що, критична інфраструктура – це сукупність об'єктів національної критичної інфраструктури і критичної інформаційної інфраструктури. Що, є об'єктами національної критичної інфраструктури – це об'єкти, системи, служби та послуги, необхідні для підтримання життєдіяльності суспільства та функціонування держави, порушення функціонування яких призведе до негативних наслідків для національної безпеки, економіки та/або соціальної сфери. Критична інформаційна інфраструктура – це сукупність інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем та електронних комунікаційних мереж, що забезпечують функціонування об'єктів критичної інфраструктури (Про критичну інфраструктуру: Закон України від 16.11.2021 № 1882-IX, 2025). З міжнародних стандартів таких як Директива ЄС 2022/2555 (NIS2) та NIST Cybersecurity Framework (США) охоплюють широкий спектр секторів, включаючи енергетику, транспорт, охорону здоров'я, цифрову інфраструктуру, публічного адміністрування та інші. Визначаються за критеріями розміру та важливості послуг фокусується на системах та активах, порушення яких може мати руйнівні наслідки для національної безпеки, економіки, громадського здоров'я та безпеки (NIST, 2025; NIS 2, 2025).

Кібербезпека є невід'ємною складовою національної безпеки та сталого розвитку інформаційного суспільства. Згідно з Законом України «Про основні засади забезпечення кібербезпеки України», кібербезпека визначається як захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та національна безпека України. Це визначення кореспондується з міжнародними підходами, зокрема зі стандартами ISO/IEC 27000, які визначають інформаційну безпеку як захист конфіденційності, цілісності та доступності інформації (Антимонопольний комітет України. 2021; Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017). В цьому контексті критичної інфраструктури кібербезпека набуває особливого значення. Збої в роботі інформаційних систем, що забезпечують функціонування об'єктів КІ, можуть призвести до серйозних наслідків, таких як наприклад: блокування фінансових операцій; порушення функціонування систем охорони здоров'я; інші критичні ситуації, що загрожують життю та здоров'ю громадян, а також національній безпеці.

Отже, кібербезпека в КІ тісно пов'язана з іншими видами безпеки, такими як фізична безпека (захист об'єктів від фізичного доступу), інформаційна безпека (захист інформації від несанкціонованого доступу, використання, розкриття, зміни або знищення) та операційна безпека (забезпечення безпеки операційних процесів). Ефективний захист КІ можливий лише за умови комплексного підходу, який враховує всі ці аспекти.

Кібератака являє собою навмисну дію в кіберпросторі, спрямовану на порушення конфіденційності, цілісності, доступності інформації, що обробляється в інформаційно-комунікаційних системах, або на порушення безпеки, сталого та штатного режиму функціонування цих систем. Кіберзагроза, згідно з Законом України «Про основні засади забезпечення кібербезпеки України», визначається як наявні та потенційні явища і чинники, що створюють небезпеку життєво важливим інтересам людини і громадянина, суспільства та держави під час використання кіберпростору. Це визначення охоплює широкий спектр потенційних негативних впливів, від технічних вразливостей до навмисних дій зловмисників. Міжнародні стандарти також приділяють увагу цьому поняттю. Зокрема, ISO/IEC 27005:2022 (Information security, cybersecurity and privacy protection – Guidance on managing information security risks) визначає загрозу як «потенційну причину небажаної події, яка може призвести до шкоди системам або організації», підкреслюючи ймовірнісний характер загрози та її потенційні наслідки (Будстандарт online, 2025). Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» кіберінцидент визначається як порушення нормального функціонування інформаційно-телекомунікаційних систем, електронних комунікаційних мереж та об'єктів критичної інформаційної інфраструктури або доступності, цілісності, конфіденційності та автентичності електронних інформаційних ресурсів, що обробляються в них. Визначається як подія або серія кіберподій, що призвела або може призвести до порушення. Це визначення охоплює широкий спектр подій, від індивідуальних спроб несанкціонованого доступу до складних організованих атак, і відповідає міжнародним стандартам, хоча й має певні відмінності (Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017).

Розглянемо детальніше основні положення вищезазначених нормативно-правових актів: Закон України «Про основні засади забезпечення кібербезпеки України»: визначає кібербезпеку як захищеність людини і громадянина під час використання кіберпростору. Визначаючи її як захист життєво важливих інтересів суспільства та держави. Встановлює основні принципи державної політики у сфері кібербезпеки: законність, пріоритетність захисту прав і свобод людини і громадянина, комплексність, безперервність, пропорційність та міжнародне співробітництво. Суб'єкти забезпечення кібербезпеки є: Президент України, Верховна Рада України, Кабінет Міністрів України, Рада національної безпеки і оборони України, Служба безпеки України, ДССЗЗІ, НКРЗІ, інші державні органи, органи місцевого самоврядування, підприємства тощо. ДССЗЗІУ відповідає за три основні сфери кібербезпеки: запобігання кіберзагрозам, виявлення та нейтралізація кіберзагроз, реагування на кіберінциденти та відновлення об'єктів кіберзахисту (Державна служба спеціального зв'язку та захисту інформації України, 2025). Важливо, що він визначає мандат Національного координаційного центру кібербезпеки як головного органу, що координує діяльність національної системи кібербезпеки.

Аналіз закону показує, що він створює загальні рамки для регулювання кібербезпеки, але не містить детальних вимог щодо захисту інформації та комунікацій.

Закон України «Про критичну інфраструктуру» визначає «критичну інфраструктуру» як сукупність об'єктів, систем, служб і споруд, необхідних для забезпечення життєдіяльності суспільства і виконання державою своїх функцій (Про критичну інфраструктуру : Закон України від 16.11.2021). Він визначає критерії віднесення об'єктів до критичної інфраструктури з урахуванням їх важливості для національної безпеки, економіки та соціальної сфери. Енергетика, транспорт, інформаційно-комунікаційні технології, банківська справа та фінанси, охорона здоров'я, водопостачання та водовідведення, питне водопостачання, цивільний захист, хімічна промисловість, космічна діяльність, електронні комунікації, поштовий зв'язок та паливно-енергетичний комплекс. Закон також визначає обов'язки розвідувальних органів щодо забезпечення кібербезпеки, включаючи проведення оцінки ризиків, здійснення заходів кіберзахисту, реагування на кіберінциденти та інформування компетентних органів про кіберінциденти. Передбачається створення Національної системи захисту розвідувальних органів, яка включає розвідувальні органи, державні установи та інші організації.

Отже, закон встановлює конкретні вимоги до захисту інформаційної інфраструктури та відіграє важливу роль у регулюванні кібербезпеки інформаційної інфраструктури.

Стратегія кібербезпеки України (Про затвердження Порядку проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом : Постанова Кабінету Міністрів України; Порядок від 11.11.2020): визначає стратегічні цілі та завдання держави у сфері кібербезпеки, включаючи забезпечення захисту національних інтересів у кіберпросторі, розвиток національної системи кібербезпеки, протидію кіберзлочинності та міжнародне співробітництво. Стратегія визначає пріоритетні напрями державної політики у сфері кібербезпеки, в тому числі у сфері захисту інформаційно-комунікаційних технологій (КІ). Стратегія є важливим документом стратегічного планування, який визначає загальний напрям розвитку системи кібербезпеки України.

Постанови Кабінету Міністрів України: розвивають положення закону та визначають конкретні механізми реалізації державної політики у сфері кібербезпеки інформаційно-комунікаційної інфраструктури (Про затвердження плану заходів на 2023-2024 роки з реалізації Стратегії кібербезпеки України : Розпорядження Кабінету Міністрів України; План, Заходи від 19.12.2023).

Наприклад: Постанова Кабінету Міністрів України від 19 червня 2019 року № 512 «Про затвердження Порядку формування переліку об’єктів критичної інфраструктури» (Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури : Постанова Кабінету Міністрів України; Вимоги, Перелік від 19.06.2019).

В контексті захисту критичної інфраструктури вчена Алексєєва О.А. комплексно підійшла до правового забезпечення кібербезпеки об’єктів критичної інфраструктури, враховуючи як національне законодавство, так і зарубіжний досвід, зокрема, США та ЄС. Акцентується увага на актуальності питання в умовах кібервійни з росією та необхідності вдосконалення нормативно-правової бази. Важливим аспектом є аналіз законопроекту № 8087, який спрямований на посилення кіберзахисту, але автор вказує на необхідність внесення змін відповідно до європейських стандартів та інтересів бізнесу. Авторка обґрунтовано зазначає питання відсутності узгодженої державної політики та недостатньої міжвідомчої координації у сфері захисту ІКТ та наголошує на важливості державно-приватного співробітництва. Водночас наголошується на необхідності адаптації іноземного досвіду до українських реалій та врахуванні історичних особливостей управління технічною безпекою. Загалом у дослідженні представлено системний підхід до аналізу проблеми, визначено ключові виклики та запропоновано конкретні напрями вдосконалення системи кіберзахисту КІ України (Алексеєва О. А., 2023; Про внесення змін до деяких законів України щодо невідкладних заходів посилення спроможностей із кіберзахисту державних інформаційних ресурсів та об’єктів критичної інформаційної інфраструктури: проєкт закону України).

Можна погодитися з вченими Скіцьком О.І. та Ширшовим Р.А. автори справедливо підкреслюють, що проблема кіберзахисту об’єктів критичної інфраструктури в Україні значно загострилася в умовах тотальної агресії російської федерації. Зокрема, підкреслюється, що об’єкти критичної інфраструктури, такі як енергетичні, телекомунікаційні, медійні та фінансові компанії, є основними цілями кібератак, що підтверджує їх стратегічну важливість в умовах військових дій. Автори обґрунтовано доводять, що з огляду на мінливу динаміку нормативно-правової бази необхідний комплексний підхід до управління кібербезпекою інформаційно-комунікаційних об’єктів. Запропонований комплексний підхід, спрямований на зменшення вразливостей, пом’якшення наслідків інцидентів та ефективну протидію кіберзагрозам, є логічним і відповідає сучасним вимогам у сфері кібербезпеки. Так, автори чітко окреслюють ключові виклики та пропонують практичні шляхи їх подолання. Це важливо для забезпечення стійкості критичної інфраструктури України в умовах гібридної війни (Скіцько О. І., Ширшов Р. А., 2024).

В умовах глобалізації та транснаціонального характеру кіберзагроз вивчення міжнародного досвіду та активна участь у міжнародному співробітництві мають важливе значення для забезпечення ефективної кібербезпеки КІ. Директива (ЄС) 2022/2555 (NIS2) (6) є ключовим законодавчим актом ЄС у сфері кібербезпеки. Вона замінила попередню Директиву NIS та значно розширила її сферу дії, охоплюючи більшу кількість секторів та суб’єктів. Основні положення NIS2: розширена сфера застосування: охоплює такі критичні сектори, як енергетика, транспорт, охорона здоров’я, цифрова інфраструктура, державне управління, космос, виробництво та харчова промисловість; диференційований підхід: різні вимоги до різних суб’єктів господарювання, залежно від розміру суб’єкта господарювання та важливості його послуг. Розрізняють «основні» та «критичні» організації; посилені вимоги до управління ризиками: вимагає впровадження комплексних заходів з управління ризиками кібербезпеки, включаючи оцінку

ризиків, впровадження технічних та організаційних заходів безпеки та реагування на інциденти; повідомлення про інциденти: встановлює зобов'язання повідомляти про кіберінциденти, що дозволяє швидко реагувати на загрози та обмінюватися інформацією; нагляд та санкції. Передбачає механізми нагляду та санкції за недотримання Директиви NIS2 є важливим кроком у гармонізації законодавства ЄС у сфері кібербезпеки та сприятиме підвищенню рівня інформаційної безпеки в Європі.

Таким чином, Директива (ЄС) 2022/2555 (NIS2) є ключовим інструментом регулювання кібербезпеки в ЄС та значно розширює сферу застосування до секторів та суб'єктів у порівнянні з попередньою версією. Основними аспектами NIS2 є розширення сфери застосування на ключові сектори економіки, диференційований підхід до вимог відповідно до розміру та важливості суб'єкта.

NIST CSF – це стандарт, розроблений Національним інститутом стандартів і технологій США (NIST), який надає організаціям структурований підхід до управління ризиками кібербезпеки, включаючи захист КІ (NIST CSF 2.0, 2024).

Держави-члени НАТО вважають кібербезпеку важливим елементом колективної оборони і приділяють їй значну увагу. НАТО розробила низку документів та ініціатив у цій сфері. План дій з кіберзахисту: визначає конкретні заходи і завдання з посилення кіберсил і засобів Альянсу. Центр передового досвіду з кіберзахисту (CCDCOE): проводить дослідження, навчання та обмін досвідом у сфері кіберзахисту; країни НАТО активно співпрацюють у сфері кібербезпеки, обмінюючись інформацією про загрози та проводячи спільні навчання (About us, 2025).

Українське законодавство має певні спільні риси з міжнародними стандартами, але є й відмінності. Акцент на управлінні ризиками, вимоги до звітності про інциденти. Недостатня деталізація вимог до кіберзахисту для різних секторів інформаційної безпеки, відсутність диференційованого підходу до різних типів суб'єктів. Для вдосконалення українського законодавства доцільно врахувати кращі практики ЄС та США. Зокрема: запровадження диференційованого підходу до регулювання кібербезпеки КІ відповідно до рівня важливості об'єкта регулювання. Запровадити диференційований підхід до регулювання кібербезпеки КІ залежно від рівня важливості об'єкта. Посилити вимоги до інформування про інциденти та обміну інформацією. Посилення міжнародного співробітництва у сфері кібербезпеки. Україна бере активну участь у міжнародному співробітництві у сфері кібербезпеки та співпрацює з такими міжнародними організаціями, як ООН, ОБСЄ, Рада Європи, НАТО та ЄС. Розробка та імплементація міжнародних стандартів і норм у сфері кібербезпеки.

Висновки. По-перше, в умовах глобальної діджиталізації та зростання кіберзагроз, особливо в умовах збройної агресії російської федерації, захист критичної інфраструктури має стратегічне значення для національної безпеки та стабільного функціонування держави. Ефективне правове регулювання є ключовим елементом у забезпеченні такого захисту.

Аналіз чинного законодавства України свідчить про наявність базової правової бази. Водночас були виявлені прогалини та суперечності, які потребують вирішення. Серед них відсутність чіткого диференційованого підходу до різних типів організацій КІ, а також необхідність посилення міжвідомчої координації та обміну інформацією щодо кіберінцидентів.

Вивчення міжнародного досвіду може допомогти визначити найкращі практики та сфери для вдосконалення українського законодавства. Диференціювати підхід до регулювання кібербезпеки відповідно до критичності об'єкта.

ЛІТЕРАТУРА:

1. Алексеєва О. А. Правове забезпечення кібербезпеки об'єктів критичної інфраструктури. *Інформація і право*. 2023. № 4 (47). С. 168–176. DOI: https://doi.org/10.37750/2616-6798.2023.4(47).291633.

2. АМКУ долучається до автоматизованого обміну індикаторами кіберзагроз та інформацією про кіберінциденти. *Антимонопольний комітет України*. 2021. URL: https://amcu.gov.ua/news/amku-doluchayetsya-do-avtomatizovanogo-obminu-indikatorami-kiberzagroz-ta-informaciyeyu-pro-kiberincidenti.

3. Діяльність Адміністрації Держспецзв'язку у сфері кіберзахисту. *Державна служба спеціального зв'язку та захисту інформації України*. 2025. URL: https://cip.gov.ua/ua/statics/cyber-protection.

4. ДСТУ ISO/IEC 27005:2023 Інформаційна безпека, кібербезпека та захист конфіденційності. Настанова керування ризиками інформаційної безпеки (ISO/IEC 27005:2022, IDT). *Будстандарт online*. 2025. URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=104400.

5. Ковалів М., Скриньковський Р., Назар Ю., Єсімов С., Красницький І., Кайдрович Х., Князь С., Кемська Ю. Правове забезпечення кібербезпеки критичної інформаційної інфраструктури України. *Traektoriâ Nauki = Path of Science*. 2021. No 4, Vol. 7. С. 2011–2018. DOI: https://10.22178/pos.69-12

6. Комісія УСПП з питань науки та ІТ зробила переклад Директиви NIS2. *I-UA.tv*. 2023. URL: https://i-ua.tv/tech/82418-komisiia-uspp-z-pytan-nauky-ta-it-zrobyla-pereklad-dyrektyvy-nis2.

7. Леонов Б. Д., Шостак Р. М., Серьогін В. С. Розвиток методичного забезпечення антитерористичної захищеності об'єктів критичної інфраструктури (на прикладі США). *Інформація і право*. 2020. № 3 (34). С. 88–95. URL: https://ippi.org.ua/sites/default/files/12_18.pdf.

8. Про внесення змін до деяких законів України щодо невідкладних заходів посилення спроможностей із кіберзахисту державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури: проєкт закону України (реєстр. № 8087 від 29.09.22 р.). 2025. URL: https://itd.rada.gov.ua/billInfo/Bills/pubFile/1490881

9. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури : Постанова Кабінету Міністрів України; Вимоги, Перелік від 19.06.2019 № 518. База даних «Законодавство України». Верховна Рада України. 2025. URL: https://zakon.rada.gov.ua/go/518-2019-%D0%BF.

10. Про затвердження плану заходів на 2023-2024 роки з реалізації Стратегії кібербезпеки України : Розпорядження Кабінету Міністрів України; План, Заходи від 19.12.2023 № 1163-р. База даних «Законодавство України». Верховна Рада України. 2025. URL: https://zakon.rada.gov.ua/go/1163-2023-%D1%80.

11. Про затвердження Порядку проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом : Постанова Кабінету Міністрів України; Порядок від 11.11.2020 № 1176. База даних «Законодавство України». Верховна Рада України. 2025. URL: https://zakon.rada.gov.ua/go/1176-2020-%D0%BF.

12. Про критичну інфраструктуру : Закон України від 16.11.2021 № 1882-IX. База даних «Законодавство України». Верховна Рада України. 2025. URL: https://zakon.rada.gov.ua/go/1882-20.

13. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. База даних «Законодавство України». Верховна Рада України. 2025. URL: https://zakon.rada.gov.ua/go/2163-19.

14. Пядишев В. Г. Кібербезпека критичних інфраструктур: закордонний досвід та українські реалії. *Південноукраїнський правничий часопис*. 2022. № 4. Ч. 3. С. 229–234. URL: http://www.sulj. oduvs.od.ua/archive/2022/4/part_3/38.pdf.

15. Рогов П. Д. Ворович Б. О., Ткаченко В. А. Шляхи Забезпечення кібернетичної безпеки об'єктів критичної інформаційної інфраструктури держави у воєнній сфері. *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського*. 2017. № 1. С. 64–72. URL: http:// nbuv.gov.ua/UJRN/Znpcvsd_2017 _1_13.

16. Скіцько О. І., Ширшов Р. А. Нормативно-правове забезпечення кібербезпеки об'єктів критичної інфраструктури. *Науковий вісник Львівського державного університету внутрішніх справ. Серія юридична*. 2024. № 2. С. 73–79. DOI: https://doi.org/10.32782/2311-8040/2024-2-11.

17. About us. *The NATO Cooperative Cyber Defence Centre of Excellence*. 2025. URL: https://ccdcoe.org/about-us/.

18. Cybersecurity Framework. NIST. 2025. URL: https://www.nist.gov/cyberframework.

19. Fidler D. Whither the Web?: International Law, Cybersecurity, and Critical Infrastructure Protection. *16 Georgetown Journal of International Affairs 8*. 2015. P. 8–20. URL: https://www.repository.law.indiana.edu/facpub/2452.

20. NIS 2: Огляд Директиви ЄС про кібербезпеку. *GigaCloud*. 2025. URL: https://gigacloud.ua/blog/navchannja/nis-2-ogljad-direktivi-es-pro-kiberbezpeku.

21. NIST CSF 2.0 шість функцій кібербезпеки. *Itspecialist*. 2024. URL: https://my-itspecialist.com/nist-csf-2.0-six-cybersecurity-functions.

REFERENCES:

1. Alexeyeva, O. A. (2023). Pravove zabezpechennia kiberbezpeky obiektiv krytychnoi infrastruktury [Legal support of cybersecurity for critical infrastructure objects]. *Information and Law*, 4(47), 168–176. https://doi.org/10.37750/2616-6798.2023.4(47).291633 [in Ukrainian].

2. Antimonopoly Committee of Ukraine. (2021). AMKU doluchaietsia do avtomatyzovanoho obminu indykatoramy kiberzahroz ta informatsiieiu pro kiberintsydenty [AMCU joins the automated exchange of cyber threat indicators and cyber incident information]. Retrieved from: https://amcu.gov.ua/news/amku-doluchayetsya-do-avtomatizovanogo-obminu-indikatorami-kiberzagroz-ta-informaciyeyu-pro-kiberincidenti [in Ukrainian].

3. Diialnist Administratsii Derzhspetszviazku u sferi kiberzakhystu [Activities of the State Special Communications Service of Ukraine in the field of cyber defense]. (2025). *State Service of Special*

Communications and Information Protection of Ukraine. Retrieved from: https://cip.gov.ua/ua/statics/cyber-protection [in Ukrainian].

4. Budstandard Online. (2025). DSTU ISO/IEC 27005:2023 *Information security, cybersecurity, and privacy protection. Guidelines for information security risk management (ISO/IEC 27005:2022, IDT).* Retrieved from: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=104400.

5. Kovaliv, M., Skrynkovskyi, R., Nazar, Y., Yesimov, S., Krasnytskyi, I., Kaidrovych, K., Kniaz, S., & Kemska, Y. (2021). Pravove zabezpechennia kiberbezpeky krytychnoi informatsiinoi infrastruktury Ukrainy [Legal support of cybersecurity for critical information infrastructure of Ukraine]. Traektoriâ Nauki = Path of Science, 7 (4), 2011–2018. https://doi.org/10.22178/pos.69-12 [in Ukrainian].

6. I-UA.tv. (2023). *The USPP Commission on Science and IT has translated the NIS2 Directive*. Retrieved from: https://i-ua.tv/tech/82418-komisiia-uspp-z-pytan-nauky-ta-it-zrobyla-pereklad-dyrektyvy-nis2 [in Ukrainian].

7. Leonov, B. D., Shostak, R. M., & Seryogin, V. S. (2020). Rozvytok metodychnoho zabezpechennia antyterorystychnoi zakhyshchenosti obiektiv krytychnoi infrastruktury (na prykladi SShA). [Development of methodological support for anti-terrorist protection of critical infrastructure objects (on the example of the USA)]. *Information and Law*, 3(34), 88–95. Retrieved from: https://ippi.org.ua/sites/default/files/12_18.pdf [in Ukrainian].

8. Verkhovna Rada of Ukraine. (2025). *On amendments to some laws of Ukraine regarding urgent measures to strengthen the capabilities of cybersecurity of state information resources and critical information infrastructure objects: Draft Law of Ukraine (Reg. No. 8087 of 29.09.22).* Retrieved from: https://itd.rada.gov.ua/billInfo/Bills/pubFile/1490881 [in Ukrainian].

9. Cabinet of Ministers of Ukraine. (2019). *On approval of the General requirements for cybersecurity of critical infrastructure objects: Resolution No. 518 of 19.06.2019*. Retrieved from: https://zakon.rada.gov.ua/go/518-2019-%D0%BF [in Ukrainian].

10. Cabinet of Ministers of Ukraine. (2023). *On approval of the action plan for 2023-2024 for the implementation of the Cybersecurity Strategy of Ukraine: Order No. 1163-r of 19.12.2023*. Retrieved from: https://zakon.rada.gov.ua/go/1163-2023-%D1%80 [in Ukrainian].

11. Cabinet of Ministers of Ukraine. (2020). *On approval of the Procedure for conducting a review of the state of cybersecurity of critical information infrastructure, state information resources, and information, the protection of which is required by law: Resolution No. 1176 of 11.11.2020*. Retrieved from: https://zakon.rada.gov.ua/go/1176-2020-%D0%BF [in Ukrainian].

12. Verkhovna Rada of Ukraine. (2021). *On critical infrastructure: Law of Ukraine No. 1882-IX of 16.11.2021*. Retrieved from: https://zakon.rada.gov.ua/go/1882-20 [in Ukrainian].

13. Verkhovna Rada of Ukraine. (2017). *On the basic principles of ensuring cybersecurity of Ukraine: Law of Ukraine No. 2163-VIII of 05.10.2017*. Retrieved from: https://zakon.rada.gov.ua/go/2163-19 [in Ukrainian].

14. Pyadyshev, V. G. (2022). Kiberbezpeka krytychnykh infrastruktur: zakordonnyi dosvid ta ukrainski realii [Cybersecurity of critical infrastructures: Foreign experience and Ukrainian realities]. *Pivdennoukrainskyi Pravnychyi Chasopys*, 4(3), 229–234. Retrieved from: http://www.sulj.oduvs.od.ua/archive/2022/4/part_3/38.pdf [in Ukrainian].

15. Rohov, P. D., Vorovych, B. O., & Tkachenko, V. A. (2017). Shliakhy Zabezpechennia kibernetychnoi bezpeky obiektiv krytychnoi informatsiinoi infrastruktury derzhavy u voiennii sferi [Ways to ensure cyber security of critical information infrastructure objects of the state in the military sphere]. *Collection of Scientific Works of the Center for Military-Strategic Studies of the National Defense University of Ukraine named after Ivan Chernyakhovskyi*, 1, 64–72. Retrieved from: http://nbuv.gov.ua/UJRN/Znpcvsd_2017_1_13 [in Ukrainian].

16. Skitsko, O. I., & Shirshov, R. A. (2024). Normatyvno-pravove zabezpechennia kiberbezpeky obiektiv krytychnoi infrastruktury [Regulatory and legal support of cybersecurity for critical infrastructure objects]. *Scientific Bulletin of Lviv State University of Internal Affairs. Legal Series*, 2, 73–79. https://doi.org/10.32782/2311-8040/2024-2-11 [in Ukrainian].

17. NATO Cooperative Cyber Defence Centre of Excellence. (2025). *About us*. Retrieved from: https://ccdcoe.org/about-us/.

18. NIST. (2025). *Cybersecurity Framework*. Retrieved from: https://www.nist.gov/cyberframework.

19. Fidler, D. (2015). Whither the Web?: International Law, Cybersecurity, and Critical Infrastructure Protection. *Georgetown Journal of International Affairs*, 16, 8–20. Retrieved from: https://www.repository.law.indiana.edu/facpub/2452.

20. GigaCloud. (2025). *NIS 2: Overview of the EU Cybersecurity Directive*. Retrieved from: https://gigacloud.ua/blog/navchannja/nis-2-ogljad-direktivi-es-pro-kiberbezpeku.

21. Itspecialist. (2024). *NIST CSF 2.0: Six cybersecurity functions*. Retrieved from: https://my-itspecialist.com/nist-csf-2.0-six-cybersecurity-functions.