АДМІНІСТРАТИВНЕ ПРАВО І ПРОЦЕС; ФІНАНСОВЕ ПРАВО; ІНФОРМАЦІЙНЕ ПРАВО

УДК 342.9:004.056.5:351.814
DOI https://doi.org/10.32782/TNU-2707-0581/2025.3/10

Гнедюк В. Л.
Український науково-дослідний інститут
Спеціальної техніки та судових експертиз
Служби безпеки України

ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Стаття є дослідженням актуального питання правового забезпечення кібербезпеки об'єктів критичної інфраструктури в умовах воєнного стану. З урахуванням зростаючої інтенсивності кібератак на енергетичні, телекомунікаційні, транспортні, фінансові та інші життєво важливі системи, проаналізовано чинне національне законодавство у сфері кібербезпеки, окреслено його сильні сторони та системні вади. Особливу увагу приділено законодавчим актам, що визначають підходи до класифікації об'єктів критичної інфраструктури, регламентації повноважень суб'єктів кібербезпеки, а також особливостям правового режиму у сфері державного та публічно-приватного управління кіберзагрозами. Встановлено, що чинна нормативно-правова база характеризується фрагментарністю, браком підзаконного регулювання та слабкою узгодженістю із міжнародними стандартами. У межах статті розглянуто п'ять ключових проблем: неузгодженість нормативно-правових актів, нечіткість критеріїв віднесення об'єктів до критичної інфраструктури, відсутність ефективної міжвідомчої координації, низький рівень обов'язковості впровадження стандартів кіберзахисту для приватного сектору та кадровий дефіцит. Окремий акцент зроблено на специфіці правового регулювання в умовах гібридної війни, яка вимагає від держави гнучких, адаптивних і швидко реалізованих рішень на рівні нормативного планування. Запропоновано стратегічні напрями вдосконалення правового механізму забезпечення кібербезпеки, серед яких: перегляд підходів до ідентифікації об'єктів критичної інфраструктури, розробка типових вимог до кіберзахисту для окремих галузей, створення оперативного органу при НКЦК з функціями міжвідомчої координації, запровадження інституцій публічно-приватного партнерства, а також гармонізація українського законодавства зі стандартами ЄС (зокрема, NIS2). Зроблено висновок, що подальше удосконалення правового регулювання кібербезпеки в Україні має спиратись на комплексну оцінку ризиків, адаптацію міжнародного досвіду та синергію державних і недержавних ініціатив. Перспективи подальших досліджень полягають у розробці єдиного протоколу реагування на кібератаки, аналізі ролі сектору оборони в кіберзахисті критичної інфраструктури, а також вивченні механізмів правового забезпечення кіберстійкості у галузях із високим рівнем цифрової залежності.

Ключові слова: *кібератаки, критична інфраструктура, кібербезпека, законодавство, військова агресія, державно-приватне партнерство, нормативний акт.*

Постановка проблеми. У контексті повномасштабної військової агресії проти України питання кібербезпеки набуває особливої актуальності, зокрема щодо захисту об'єктів критичної інфраструктури, які становлять основу функціонування держави, суспільства та економіки. Зростання кількості кібератак, спрямованих на енергетичні, транспортні, інформаційні та інші критично важливі системи, засвідчує необхідність перегляду, оновлення та систематизації нормативно-правових підходів до забезпечення кібербезпеки в умовах гібридної війни.

Попри наявність базових законодавчих актів, таких як Закон України «Про основні засади

забезпечення кібербезпеки України» та суміжних нормативно-правових документів, існує низка проблем, пов'язаних із нечіткістю процедур і критеріїв ідентифікації об'єктів критичної інфраструктури, недостатньою узгодженістю між суб'єктами сектора безпеки й оборони, а також фрагментарністю регулювання у сфері публічно-приватного партнерства в галузі кіберзахисту. У реаліях зростаючих загроз постає потреба в концептуальному переосмисленні підходів до правового забезпечення кібербезпеки з урахуванням як міжнародних стандартів, так і специфіки воєнного часу.

Таким чином, наукове осмислення проблематики правового регулювання кібербезпеки об'єктів критичної інфраструктури в Україні в умовах повномасштабної війни є необхідною передумовою формування цілісної та ефективної національної системи кіберзахисту.

Аналіз останніх досліджень і публікацій. Робота ґрунтується на аналізі законодавства України, науково-методичної літератури, наукових статей, періодичних видань та напрацювань сучасних вчених і дослідників, серед них: О. А. Алексеєва, Б. В. Богдан, В. Богом'я, О. І. Скіцько, Р. А. Ширшов, Я. С. Мануілов тощо.

Так, у дослідженні О. А. Алексеєвої [1] розглянуто структурні елементи правового механізму кіберзахисту критичної інфраструктури, визначено його основні вразливості та акцентовано увагу на необхідності законодавчої деталізації процедур взаємодії суб'єктів кібербезпеки у кризових ситуаціях. Б. В. [2] Богдан у своїй праці актуалізує проблематику захисту критичної інформаційної інфраструктури як пріоритетного напряму національної безпеки, наголошуючи на потребі чіткого поділу об'єктів на категорії захисту. Праця О. І. Скіцька та Р. А. Ширшова присвячена аналізу стану правової регламентації кібербезпеки на національному рівні, зокрема функціонуванню профільних інституцій та механізмів моніторингу [10].

Постановка завдання. Метою статті є комплексний аналіз стану правового забезпечення кібербезпеки об'єктів критичної інфраструктури в Україні в умовах воєнного стану, виявлення основних проблем нормативно-правового регулювання у цій сфері та обґрунтування стратегічних напрямів його вдосконалення з урахуванням сучасних викликів гібридної війни, міжнародних стандартів та перспектив євроінтеграції.

Для досягнення цієї мети поставлено такі завдання:

1. Проаналізувати чинне законодавство України у сфері кібербезпеки та визначити його роль у забезпеченні захисту критичної інфраструктури.
2. Виявити основні проблеми нормативно-правового регулювання кібербезпеки об'єктів критичної інфраструктури в умовах гібридної війни.
3. Запропонувати стратегічні напрями вдосконалення правового механізму кіберзахисту з урахуванням специфіки воєнного стану та перспектив євроінтеграції.

Виклад основного матеріалу. 24 лютого 2022 року держава-агресор розпочала повномасштабну військову агресію проти України, що супроводжується масштабним порушенням міжнародного права. У квітні того ж року російською федерацією було здійснено скоординовану та цілеспрямовану кібератаку на об'єкти критичної інфраструктури України. Ворог продовжує реалізацію своєї кіберстратегії на постійній основі, використовуючи кібератаки як елемент гібридної війни. Злочинний план російських хакерських угруповань передбачав виведення з ладу високовольтних електричних підстанцій, користувацьких комп'ютерів, серверів, автоматизованих робочих місць, серверного та мережевого обладнання, що створювало ризики масштабного техногенного колапсу. Така ситуація вимагає суттєвого вдосконалення рівня кіберзахисту, посилення захищеності інформаційних ресурсів та інформаційно-комунікаційних систем об'єктів критичної інфраструктури, доведення їхнього стану до рівня, що забезпечує функціонування безпечного, єдиного, інтегрованого секторного інформаційного та комунікаційного середовища [5, с. 157].

Державна політика у сфері кібербезпеки визначається сукупністю нормативно-правових актів, що формують засади реалізації такої політики, її напрями, принципи та основні завдання. До ключових нормативних документів, що формують базовий рівень такої політики, належать Стратегія кібербезпеки України, закони України «Про основні засади забезпечення кібербезпеки України», «Про національну безпеку України», «Про критичну інфраструктуру», а також постанови Кабінету Міністрів України «Про затвердження Положення про організаційно-технічну модель кіберзахисту», «Деякі питання об'єктів критичної інформаційної інфраструктури», «Про затвердження Порядку проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом», «Про затвердження Загальних вимог до кіберза-

хисту об'єктів критичної інфраструктури» тощо. Більшість норм та положень цих правових актів повністю або частково присвячені проблематиці побудови сучасного та надійного забезпечення кіберзахисту об'єктів критичної інфраструктури [5, с. 156].

Кібербезпека становить невід'ємну частину системи національної безпеки та є ключовим чинником сталого функціонування інформаційного суспільства. Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України», вона розглядається як стан захищеності життєво важливих інтересів особи, суспільства і держави під час використання кіберпростору, що забезпечує національну безпеку та сталий розвиток цифрового середовища [8]. Це визначення узгоджується з міжнародними підходами, зокрема зі стандартами серії ISO / IEC 27000, у яких інформаційна безпека трактується як захист конфіденційності, цілісності та доступності інформації

У цьому контексті кібербезпека об'єктів критичної інфраструктури набуває особливої ваги. Збої у функціонуванні інформаційних систем, що забезпечують роботу таких об'єктів, можуть спричинити серйозні наслідки, серед яких – блокування фінансових операцій, порушення функціонування медичних установ, а також інші кризові ситуації, що становлять пряму загрозу життю, здоров'ю громадян і національній безпеці в цілому [3, с. 38].

В Україні під критичною інфраструктурою розуміється сукупність об'єктів такої інфраструктури до кола яких віднесено: об'єкти інфраструктури, системи, їх частини та їх сукупність, які є важливими для економіки, національної безпеки та оборони, порушення функціонування яких може завдати шкоди життєво важливим національним інтересам [7]. Відповідно до Закону України «Про критичну інфраструктуру» об'єкти критичної інфраструктури – це підприємства, установи й організації незалежно від форми власності, діяльність яких безпосередньо пов'язана з технологічними процесами та / або наданням послуг, що мають велике значення для економіки та промисловості, функціонування суспільства та безпеки населення, виведення з ладу або порушення функціонування яких може справити негативний вплив на стан національної безпеки і оборони України, навколишнього природного середовища, заподіяти майнову шкоду та / або становити загрозу для життя і здоров'я людей. До критичної інфраструктури належать й особливо небезпечні виробництва, аварії на яких викликані будь-якими причинами (природними або техногенними надзвичайними ситуаціями), також можуть обернутися катастрофічними для певних територій і їх населення наслідками [1, с. 170].

Варто зазначити, що ще 29 грудня 2021 року Кабінет Міністрів України затвердив «Положення про організаційно-технічну модель кіберзахисту» постановою № 1426 [6]. Цей документ встановлює три рівні інтегрованої інфраструктури кіберзахисту: організаційно-керівний (представлений основними суб'єктами національної системи кібербезпеки), технологічний (що забезпечує інформаційну взаємодію, безперервний моніторинг і підтримку стійкості кіберпростору), а також базовий (охоплює захищену інформаційну інфраструктуру і суспільство як користувача цієї системи). Організаційно-технічна модель спрямована на підвищення ефективності функціонування кіберзахисту України, посилення координації між головними суб'єктами у цій сфері, зниження вразливості інформаційно-комунікаційних систем та підвищення їхньої кіберстійкості. Водночас вона передбачає створення умов для розвитку державно-приватного партнерства, формування ефективної системи реагування на кіберінциденти, розвиток галузевих команд реагування, синхронізацію їхньої діяльності, а також зміцнення національного кіберпотенціалу, забезпечення конфіденційності, цілісності та доступності інформації та безпеки інформаційно-комунікаційних технологій [6].

Реалізація заходів із кіберзахисту включає низку ключових етапів:

– Ідентифікація, що передбачає виявлення наявних і потенційних кіберзагроз з метою їх своєчасного попередження та нейтралізації;

– Захист, який охоплює розробку та впровадження відповідних методів, засобів і процедур, спрямованих на забезпечення безперебійної та надійної роботи інформаційних, телекомунікаційних, інформаційно-телекомунікаційних і технологічних систем;

– Виявлення, що полягає у проведенні постійного моніторингу, зборі та аналізі нетипових подій у кіберпросторі;

– Реагування, яке включає вжиття заходів для запобігання кіберінцидентам і кібератакам, мінімізації їхніх можливих наслідків, захисту життя і здоров'я громадян, запобігання шкоді майну, а також вдосконалення наявних систем кіберзахисту з урахуванням реальних і потенційних ризиків та необхідності забезпечення пропорційності реагування;

– Відновлення, що передбачає повернення інформаційно-телекомунікаційних та технологічних систем до нормального функціонування після кіберінциденту, відновлення втрачених або пошкоджених даних, а також створення умов для подальшого розслідування обставин інциденту [10, с. 76].

У процесі забезпечення роботи базової інфраструктури кіберзахисту необхідно гарантувати:

– надійний захист національних електронних інформаційних ресурсів, комунікаційних та технологічних систем у кіберпросторі;

– безпеку об'єктів критичної інфраструктури;

– впровадження заходів для формування культури кібербезпеки як на об'єктах критичної інфраструктури, так і на підприємствах усіх форм власності;

– належне інформування громадян про наслідки кіберінцидентів та рівень пов'язаних із ними загроз [5, с. 158].

Пунктом 8 Положення про організаційно-технічну модель кіберзахисту, затвердженого Постановою Кабінету Міністрів України від 29.12.21 р. №1426 [6], визначено, що під час функціонування організаційно-керуючої інфраструктури кіберзахисту відповідальні суб'єкти забезпечення кібербезпеки організовують і проводять огляд стану кіберзахисту критичної інфраструктури. Метою проведення такого огляду є отримання об'єктивної та неупередженої інформації щодо оцінки рівня кібербезпеки та визначення напрямів удосконалення й розвитку системи кібербезпеки об'єктів критичної інфраструктури.

Попри істотні зусилля держави у розбудові нормативної бази кіберзахисту, реалії повномасштабної війни виявили низку критичних проблем у правовому забезпеченні кібербезпеки об'єктів критичної інфраструктури (КІ). Значна частина чинних норм не враховує специфіку новітніх кіберзагроз, характерних для гібридного воєнного середовища, а координація між відповідальними суб'єктами іноді залишається неефективною через нечіткість функціонального розмежування. Окрім того, спостерігається дисбаланс між державним та приватним секторами у впровадженні стандартів кіберзахисту, а також суттєвий кадровий дефіцит, що ускладнює реалізацію відповідної політики на практиці.

1. Фрагментарність законодавства. Незважаючи на наявність базового Закону України «Про основні засади забезпечення кібербезпеки України», система нормативно-правових актів у цій сфері залишається фрагментарною. Значна частина підзаконних документів не має уніфікованого термінологічного апарату, не кореспондує з положеннями міжнародних угод і не адаптована до умов гібридної війни. Особливої уваги потребує інтеграція норм щодо взаємодії цивільного та військового компонентів у питаннях кібербезпеки, а також адаптація законодавства до стандартів ЄС і НАТО.

2. Недостатня деталізація критеріїв віднесення об'єктів до критичної інфраструктури. Повномасштабна агресія російської федерації проти України засвідчила вразливість низки об'єктів, які раніше не розглядалися як критично важливі. Серед них – хмарні сервіси, медійні ресурси, онлайн-банкінг та цифрові платформи логістики. Однак критерії їх віднесення до переліку еритичної інфраструктури залишаються нечіткими, що ускладнює визначення обсягів зобов'язань щодо кіберзахисту та відповідальності суб'єктів у разі порушення норм безпеки [4, с. 96].

3. Відсутність уніфікованого механізму координації між державними органами. Кіберзахист критичної інфраструктури здійснюється силами низки суб'єктів національної системи кібербезпеки, зокрема Державним центром кіберзахисту (Держспецзв'язку), Ситуаційним центром СБУ, Центром кіберзахисту НБУ, Департаментом кіберполіції, підрозділами Міноборони, Генштабу, а також через технологічну платформу Національного координаційного центру кібербезпеки (НКЦК РНБО). Водночас практична взаємодія між цими інституціями часто ускладнена відсутністю єдиного операційного протоколу, що знижує ефективність реагування на складні кібератаки, особливо у міжсекторальному вимірі (наприклад, між енергетикою та зв'язком).

4. Низький рівень обов'язковості впровадження стандартів кіберзахисту. Правовий статус приватних операторів критичної інфраструктури (зокрема, в галузях енергетики, телекомунікацій, логістики) дозволяє їм уникати впровадження повного спектра державних стандартів безпеки. Наявні нормативні акти не встановлюють дієвих санкцій за нехтування вимогами кіберзахисту або за неналежне реагування на інциденти. Внаслідок цього значна частина потенційно вразливих об'єктів залишається поза сферою належного державного контролю.

5. Кадровий дефіцит у сфері кібербезпеки. Однією з найбільш практично відчутних проблем є нестача кваліфікованих кадрів. Частина спеціалістів мобілізована або переміщена до інших

напрямів оборонної діяльності, частина – виїхала за кордон. В умовах зростання кількості та складності кібератак це створює надмірне навантаження на чинні команди реагування (зокрема, у галузевих центрах – таких як кіберцентр «Нафтогазу» або SOC «Укренерго») і підвищує ризик запізнілого або неефективного реагування на інциденти [2, с. 479–480].

Виявлені недоліки чинної нормативної бази свідчать про необхідність її системного оновлення, з урахуванням нових типів загроз, міжнародного досвіду та реалій ведення гібридної війни. У цьому зв'язку доцільно виокремити кілька стратегічних напрямів вдосконалення.

Першочерговим завданням є перегляд підходів до визначення переліку об'єктів критичної інфраструктури з урахуванням цифрової трансформації держави. В умовах кібервійни потребують включення до критичної інфраструктури низка цифрових платформ, інформаційних сервісів та ІТ-інфраструктура, що забезпечують функціонування життєво важливих сфер – фінансової системи, охорони здоров'я, енергетики, логістики. Необхідно закріпити нормативно гнучкий, ризик-орієнтований підхід до класифікації таких об'єктів, передбачивши можливість оперативної зміни їх статусу в разі загострення безпекової ситуації.

Також, для ефективної реалізації базових положень профільних законів слід активізувати розробку та впровадження відповідних підзаконних актів. Йдеться, зокрема, про затвердження типових вимог до кіберзахисту для кожного сектору критичної інфраструктури, єдиної методики оцінки ризиків у кіберпросторі, а також порядку взаємодії державних та недержавних суб'єктів у випадку виявлення кіберінциденту [11, с. 132–133].

З метою підвищення швидкості реагування на кіберзагрози доцільним є створення єдиного координаційного органу оперативного рівня, що діятиме при Національному координаційному центрі кібербезпеки (НКЦК) та матиме повноваження щодо розгортання кризового управління у випадку атак на КІ. Такий орган має бути уповноваженим здійснювати обов'язкову координацію між галузевими командами реагування на інциденти (CERT / SOC), забезпечуючи цілісну систему управління кіберризиками на національному рівні.

З огляду на значну частку об'єктів критичної інфраструктури у приватному секторі, особливо в енергетиці, зв'язку, фінансовій системі, необхідним є закріплення чітких нормативних вимог до суб'єктів господарювання щодо впровадження заходів кіберзахисту. Водночас варто передбачити механізми заохочення приватного сектору до участі в реалізації державної політики кібербезпеки – зокрема, через надання податкових пільг, пріоритетного доступу до державних засобів моніторингу загроз, а також включення до спільних програм навчання та сертифікації кадрів.

Важливо вказати, що зважаючи на стратегічний курс України на євроінтеграцію, важливим є імплементація норм і стандартів Європейського Союзу в галузі кібербезпеки. Зокрема, доцільно враховувати положення Директиви (ЄС) 2022 / 2555 (NIS2) щодо управління ризиками, обміну інформацією про кіберінциденти, відповідальності керівників підприємств, а також мінімальних технічних вимог до операторів критичних послуг [9, с. 233].

Висновки. Правове забезпечення кібербезпеки критичної інфраструктури в умовах воєнного часу набуває ключового значення для національної безпеки України. Дослідження засвідчило наявність концептуальних і практичних прогалин у чинному нормативному регулюванні, що ускладнює ефективне протистояння кіберзагрозам.

У сучасних умовах вимагається перехід від фрагментарного правового підходу до системної, узгодженої моделі регулювання, яка враховує як внутрішні ризики, так і міжнародний досвід. Така трансформація має ґрунтуватися на оновленні законодавства, налагодженні міжсекторальної взаємодії та посиленні інституційної спроможності держави. Формування цілісної системи кіберзахисту критичної інфраструктури має стати одним із стратегічних пріоритетів правової політики в умовах гібридної війни.

Перспективними напрямами наукового осмислення залишаються: глибока оцінка ефективності імплементації директив ЄС у національне законодавство в контексті кібербезпеки; розробка концепції єдиного цифрового протоколу реагування на кібератаки на об'єкти критичної інфраструктури; дослідження правових аспектів участі сил оборони в забезпеченні кіберзахисту в умовах воєнного стану.

Список літератури:

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. Богдан Б. В. Критична інформаційна інфраструктура як об'єкт забезпечення кібербезпеки. *Наукові перспективи. Актуальні питання у сучасній науці.* №3 (33). 2025. С. 473–482. DOI: https://doi.org/10.52058/2786–6300–2025–3 (33)–473–482

3. Богом'я В., Галунько В. Правове регулювання кібербезпеки в контексті захисту критичної інфраструктури. *Information Technology: Computer Science, Software Engineering and Cyber Security.* 2024. № 4. С. 35–42. DOI: https://doi.org/10.32782/IT/2024–4–5.

4. Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест/відп. ред. О. Довгань; упоряд. О. Довгань, Л. Литвинова, С. Дорогих. Державна наукова установа «Інститут інформації, безпеки і права НАПрН України». Національна бібліотека України ім. В. І. Вернадського. Київ, 2023. № 6. 153 с.

5. Мануілов Я. С., Забезпечення кібербезпеки об'єктів критичної інфраструктури в умовах кібервійни. *Інформація і право.* 2023. № 1 (44). С. 154–167.

6. Про затвердження Положення про організаційно-технічну модель кіберзахисту: Постанова Кабінету Міністрів України від 29.12.21 р. № 1426. URL: https://www.kmu.gov.ua/npas/pro-zatverdzhennya-polozhennya-pro-a1426 (дата звернення: 16.05.2025).

7. Про критичну інфраструктуру: Закон України від 16.11.21 р. № 1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882–20#n80 (дата звернення: 15.05.2025).

8. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/go/2163–19 (дата звернення: 14.05.2025).

9. Пядишев В. Г. Кібербезпека критичних інфраструктур: закордонний досвід та українські реалії. *Південноукраїнський правничий часопис.* 2022. № 4. Ч. 3. С. 229–234.

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

11. Хлапонін Ю. І., Козубцова Л. М., Козубцов І. М., Штонда Р. М. Функції системи захисту інформації і кібербезпеки критичної інформаційної інфраструктури. *Кібербезпека: освіта, наука, техніка*. 2022. №3 (15). С. 124–134. DOI: https://doi.org/10.28925/2663–4023.2022.15.1241341.

Gnediuk V. L. LEGAL FRAMEWORK FOR CYBERSECURITY OF CRITICAL INFRASTRUCTURE OBJECTS

The article is a study of the current issue of legal support for cybersecurity of critical infrastructure under martial law. Considering the increasing intensity of cyberattacks on energy, telecommunications, transport, financial, and other vital systems, the national cybersecurity legislation has been analyzed, outlining its strengths and systemic weaknesses. Particular attention is given to legal acts that define approaches to the classification of critical infrastructure objects, regulation of the powers of cybersecurity actors, and the specifics of the legal regime in the field of public and public-private management of cyber threats. It has been established that the existing regulatory framework is characterized by fragmentation, lack of subordinate regulation, and weak harmonization with international standards. The article examines five key problems: inconsistency of legal acts, lack of clear criteria for identifying critical infrastructure, absence of effective interagency coordination, low mandatory implementation of cybersecurity standards in the private sector, and shortage of qualified personnel. Special emphasis is placed on the specifics of legal regulation in a hybrid warfare context, which requires the state to adopt flexible, adaptive, and rapidly implemented solutions at the level of regulatory planning. Strategic directions for improving the legal mechanism of cybersecurity provision are proposed, including: revision of approaches to critical infrastructure identification, development of sector-specific cybersecurity standards, establishment of an operational body under the National Cybersecurity Coordination Center (NCCC) with interagency coordination functions, introduction of public-private partnership institutions, and harmonization of Ukrainian legislation with EU standards (particularly NIS2). It is concluded that further improvement of cybersecurity legal regulation in Ukraine should be based on comprehensive risk assessment, adaptation of international experience, and synergy between state and non-state initiatives. Prospects for further research include the development of a unified cyber incident response protocol, analysis of the defense sector's role in protecting critical infrastructure, and the study of legal mechanisms for ensuring cyber resilience in high digital dependency sectors.

Key words: *cyberattacks, critical infrastructure, cybersecurity, legislation, military aggression, public-private partnership, legal act.*