

УДК 343.9:004.056(477)

DOI 10.33244/2617-4154.3(24).2026.118-128

О. С. Яра,

*доктор юридичних наук, професор, декан юридичного факультету,
Національний університет біоресурсів і природокористування України*

O. S. Yara,

*Doctor of Law, Professor, Dean of the Faculty of Law,
National University of Life and Environmental Sciences of Ukraine
email: yara_o@nubip.edu.ua*

ORCID 0000-0002-7245-9158;

М. А. Дейнега,

*доктор юридичних наук, доцент,
професор кафедри цивільного і господарського права,
Національний університет біоресурсів і природокористування України*

M. A. Deineha,

*Doctor of Law, Associate Professor,
Professor of the Department of Civil and Economic Law,
National University of Life and Environmental Sciences of Ukraine
email: marinad@meta.ua*

ORCID 0000-0002-4785-7509;

О. А. Улютіна,

*кандидат юридичних наук, професор,
професор кафедри адміністративного та фінансового права,
Національний університет біоресурсів і природокористування України*

O. A. Uliutina,

*Candidate of Legal Sciences, Professor,
Professor of the Department of Administrative and Financial Law,
National University of Life and Environmental Sciences of Ukraine
email: ulutina@nubip.edu.ua*

ORCID 0000-0003-1982-9911;

О. В. Калмикова,

*кандидат юридичних наук, професор,
професор кафедри адміністративного та фінансового права,
Національного університету біоресурсів і природокористування України*

O. V. Kalmykova,

*Candidate of Legal Sciences, Professor,
Professor of the Department of Administrative and Financial Law,
National University of Life and Environmental Sciences of Ukraine
email: artolena11@ukr.net*

ORCID 0000-0003-2041-8925



Ця робота ліцензується відповідно до [Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License](https://creativecommons.org/licenses/by-nc-nd/4.0/).

© Яра О. С., Дейнега М. А., Улютіна О. А., Калмикова О. В., 2026

ОСОБЛИВОСТІ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УМОВАХ ВОЄННОГО СТАНУ В УКРАЇНІ

LEGAL REGULATION OF CYBERSECURITY UNDER MARTIAL LAW IN UKRAINE

Метою статті є дослідження особливостей правового забезпечення кібербезпеки в Україні в умовах воєнного стану, визначення сучасного стану нормативно-правового регулювання в цій сфері, а також окреслення основних проблем і напрямів його вдосконалення з урахуванням міжнародних стандартів.

Методологічну основу дослідження становлять загальнонаукові та спеціально-юридичні методи, зокрема системно-структурний, формально-юридичний, порівняльно-правовий і метод аналізу нормативно-правових актів, що дали змогу комплексно дослідити особливості функціонування національної системи кібербезпеки в умовах воєнних загроз.

У статті проаналізовано сутність поняття «кібербезпека» та її роль у системі національної безпеки України. Досліджено основні нормативно-правові акти, що регулюють сферу кіберзахисту, зокрема особливості розвитку законодавства у 2022–2025 роках під впливом повномасштабної збройної агресії російської федерації. Визначено особливості правового регулювання захисту державних інформаційних ресурсів, об'єктів критичної інфраструктури, механізмів реагування на кіберінциденти та взаємодії суб'єктів національної системи кібербезпеки. Окрему увагу приділено аналізу міжнародних підходів, а саме положень Директиви ЄС NIS2, рекомендацій ENISA, стандартів НАТО та ISO / IEC у сфері інформаційної безпеки.

За результатами дослідження встановлено, що в умовах воєнного стану кібербезпека стала одним із ключових напрямів забезпечення національної безпеки держави. Водночас існує потреба в подальшому вдосконаленні правового регулювання, зокрема щодо розмежування повноважень суб'єктів кібербезпеки, посилення захисту критичної інфраструктури, удосконалення механізмів обміну інформацією про кіберзагрози та гармонізації законодавства України з правом Європейського Союзу.

Зроблено висновок, що ефективне правове забезпечення кібербезпеки в умовах воєнного стану потребує комплексного підходу, поєднання національних механізмів захисту із міжнародними стандартами та розвитку стійкої системи реагування на сучасні кіберзагрози.

Ключові слова: кібербезпека, воєнний стан, національна безпека, кіберзахист, критична інфраструктура, кіберзагрози, правове забезпечення, інформаційна безпека, кіберінциденти, цифрова безпека.

The purpose of the article is to examine the specific features of legal regulation of cybersecurity in Ukraine under martial law, determine the current state of regulatory and legal framework in this area, and identify the main challenges and directions for its improvement in accordance with international standards.

The methodological basis of the research consists of general scientific and special legal methods, including systemic-structural, formal-legal, comparative-legal methods, as well as the method of analysis of regulatory legal acts, which enabled a comprehensive study of the functioning of the national cybersecurity system under conditions of military threats.

The article analyzes the essence of the concept of “cybersecurity” and its role in the national security system of Ukraine. The main regulatory legal acts governing the field of cyber protection are examined, including the specifics of legislative development during 2022–2025 under the influence of the full-scale armed aggression of the Russian Federation. The study identifies the peculiarities of legal regulation regarding the protection of state information resources, critical infrastructure facilities, mechanisms for responding to cyber incidents, and interaction between entities within the national cybersecurity system. Particular attention is paid to the analysis of international approaches, including the provisions of the EU NIS2 Directive, ENISA recommendations, NATO standards, and ISO/IEC standards in the field of information security.

The results of the study demonstrate that, under martial law, cybersecurity has become one of the key areas of ensuring national security of the state. At the same time, further improvement of legal regulation remains necessary, particularly regarding the delineation of powers among cybersecurity entities, strengthening the protection of critical infrastructure, improving mechanisms for exchanging information on cyber threats, and harmonizing Ukrainian legislation with European Union law.

It is concluded that effective legal regulation of cybersecurity under martial law requires a comprehensive approach, combining national protection mechanisms with international standards and developing a resilient system for responding to contemporary cyber threats.

Keywords: *cybersecurity, martial law, national security, cyber protection, critical infrastructure, cyber threats, legal regulation, information security, cyber incidents, digital security.*

Постановка проблеми. Повномасштабна військова агресія проти України зумовила суттєве зростання ролі кібербезпеки як складової національної безпеки держави. В умовах воєнного стану кіберпростір став одним із ключових середовищ ведення гібридної війни, у межах якої здійснюються кібератаки на об'єкти критичної інфраструктури, державні інформаційні ресурси, фінансовий сектор і системи електронного врядування. Поширення кіберзагроз створює ризики порушення функціонування державних інституцій, витоку інформації, дестабілізації суспільних процесів і зниження рівня обороноздатності країни.

За таких умов особливого значення набуває формування ефективної системи правового забезпечення кібербезпеки, здатної оперативно реагувати на сучасні виклики та забезпечувати належний рівень захисту інформаційного простору держави. Важливим аспектом є адаптація національного законодавства до умов воєнного стану, удосконалення механізмів взаємодії

між суб'єктами забезпечення кібербезпеки, а також гармонізація правових норм із міжнародними стандартами й практиками Європейського Союзу та НАТО. У сучасних умовах правове регулювання кібербезпеки виходить за межі технічного захисту інформації та охоплює питання державного управління, оборони, захисту критичної інфраструктури й цифрового суверенітету.

Незважаючи на поступове вдосконалення нормативно-правової бази у сфері кібербезпеки, сучасні умови воєнного стану вимагають переосмислення підходів до правового забезпечення захисту інформаційного простору держави. Динамічний розвиток цифрових технологій, збільшення кількості кіберінцидентів і трансформація характеру кіберзагроз актуалізують потребу у формуванні ефективних правових механізмів реагування, здатних забезпечити належний рівень кіберстійкості держави. У зв'язку з цим особливої актуальності набуває дослідження особливостей правового забезпечення кібербезпеки в умовах воєнного стану, а також визначення напрямів удосконалення державної політики в цій сфері.

Аналіз останніх досліджень і публікацій свідчить про посилення наукового інтересу до проблем правового забезпечення кібербезпеки в умовах сучасних воєнних та інформаційних загроз. Значна кількість наукових праць присвячена питанням функціонування національної системи кібербезпеки, захисту інформаційного простору держави, удосконалення механізмів державного управління у сфері кіберзахисту, а також адаптації законодавства України до міжнародних стандартів. Так, О. Горун досліджує особливості нормативно-правового забезпечення національної системи кібербезпеки та механізми державного регулювання в цій сфері [1]. С. Красніков у своїх наукових працях розглядає питання протидії сучасним кіберзагрозам, розвитку кібергігієни та забезпечення безпеки критичної інформаційної інфраструктури [2]. О. Капля приділяє увагу проблемам адміністративно-правового забезпечення інформаційної безпеки та особливостям захисту інформаційного простору в умовах воєнного стану [3]. С. Мазепа досліджує сучасні виклики у сфері кібербезпеки та напрями вдосконалення законодавчого регулювання в контексті європейської інтеграції України [4]. О. Колесник розглядає кібербезпеку як складову системи національної безпеки держави та аналізує правові аспекти протидії кіберзагрозам в умовах гібридної війни [5]. Окремої уваги заслуговують дослідження О. Федорченка, присвячені проблемам координації діяльності суб'єктів забезпечення національної системи кібербезпеки. Автор аналізує особливості взаємодії державних органів у сфері кіберзахисту, питання координації діяльності суб'єктів сектору безпеки й оборони, а також проблеми дублювання повноважень у процесі реалізації державної політики забезпечення кібербезпеки. Важливе значення в працях дослідника приділяється питанням захисту критичної інфраструктури та потреби у формуванні ефективного механізму міжвідомчої координації у сфері кібербезпеки [6].

Виділення невирішених раніше частин загальної проблеми. Попри значну кількість наукових досліджень, питання особливостей правового забезпечення кібербезпеки саме в умовах воєнного стану потребують подальшого комплексного наукового опрацювання, зокрема в частині адаптації правових механізмів до нових викликів кіберпростору,

забезпечення ефективної координації суб'єктів кібербезпеки та вдосконалення системи реагування на кіберінциденти.

Метою статті є дослідження особливостей правового забезпечення кібербезпеки в умовах воєнного стану в Україні, аналіз сучасних механізмів державного регулювання у сфері кіберзахисту, а також визначення основних проблем і напрямів удосконалення правових механізмів забезпечення кібербезпеки в умовах сучасних воєнних та інформаційних загроз.

Виклад основного матеріалу. Дослідження особливостей правового забезпечення кібербезпеки в умовах воєнного стану потребує насамперед визначення сутності поняття «кібербезпека», оскільки саме ця категорія є базовою для формування системи правового регулювання у відповідній сфері. У сучасних умовах розвитку цифрового суспільства кібербезпека є не лише складовою інформаційної безпеки, а й одним із ключових елементів забезпечення національної безпеки держави, особливо в умовах збройної агресії та активізації гібридних загроз у кіберпросторі.

Відповідно до положень ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України» кібербезпека визначається як захищеність життєво важливих інтересів людини й громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства й цифрового комунікативного середовища, своєчасне виявлення, запобігання та нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі [7]. Наведене визначення свідчить про комплексний характер кібербезпеки, яка охоплює як технічні, так і організаційно-правові механізми захисту інформаційного середовища держави.

Схожий підхід простежується і в положеннях Стратегії здійснення цифрового розвитку, цифрових трансформацій і цифровізації системи управління державними фінансами на період до 2030 року, де кібербезпека розглядається як стан захищеності даних в електронній формі від несанкціонованого доступу, використання або інших протиправних дій, а також як сукупність заходів, спрямованих на забезпечення такого захисту [8]. Отже, сучасне розуміння кібербезпеки виходить далеко за межі виключно технічного захисту інформаційних систем і охоплює комплекс правових, організаційних та інституційних механізмів забезпечення стійкості держави до сучасних кіберзагроз. У зв'язку з цим важливого значення набуває формування ефективної нормативно-правової основи, яка визначає засади функціонування національної системи кібербезпеки, повноваження її суб'єктів і механізми реагування на кіберінциденти.

Нормативно-правову основу забезпечення кібербезпеки в Україні становить комплекс законодавчих і підзаконних нормативно-правових актів, спрямованих на регулювання відносин у сфері захисту інформаційного простору, критичної інфраструктури та національної безпеки держави. Базовим нормативним актом є Конституція України, яка визначає захист суверенітету, територіальної цілісності, економічної та інформаційної безпеки однією із найважливіших функцій держави [9]. Важливе значення в системі правового регулювання має Закон України «Про національну безпеку України», який визначає кібербезпеку як складову національної безпеки та окреслює основні напрями державної політики у сфері протидії кіберзагрозам [10].

Яра О. С., Дейнега М. А., Улютіна О. А., Калмикова О. В.
Особливості правового забезпечення кібербезпеки в умовах воєнного стану в Україні

Оскільки положення Закону України «Про основні засади забезпечення кібербезпеки України» вже були розглянуті під час визначення поняття кібербезпеки, доцільно зазначити, що саме цей нормативно-правовий акт формує основу функціонування національної системи кібербезпеки та визначає ключові напрями державної політики у сфері кіберзахисту. Норми Закону регламентують діяльність суб'єктів забезпечення кібербезпеки, засади їх взаємодії та координації, а також механізми захисту державних інформаційних ресурсів і інформаційно-комунікаційних систем від сучасних кіберзагроз [7].

Вагому роль у системі нормативно-правового забезпечення кібербезпеки відіграють закони України «Про захист інформації в інформаційно-комунікаційних системах» [11], «Про інформацію» [12], «Про державну таємницю» [13], «Про критичну інфраструктуру» [14], а також «Про електронні комунікації» [15]. Сукупність зазначених нормативно-правових актів формує базову правову основу функціонування національної системи кібербезпеки та забезпечує регулювання окремих напрямів захисту інформаційного простору держави. Водночас важливе значення в системі правового забезпечення кібербезпеки мають стратегічні документи, які визначають пріоритети державної політики у сфері кіберзахисту та напрями розвитку національної системи кібербезпеки.

Особливого значення в умовах воєнного стану набуває Стратегія кібербезпеки України, затверджена Указом Президента України, яка визначає основні напрями реалізації державної політики у сфері кібербезпеки, пріоритети розвитку національної системи кіберзахисту та механізми взаємодії суб'єктів сектору безпеки й оборони [16]. У межах реалізації Стратегії особлива увага приділяється захисту державних інформаційних ресурсів, об'єктів критичної інфраструктури, розвитку системи реагування на кіберінциденти та підвищенню рівня кіберстійкості держави в умовах збройної агресії.

Крім національного законодавства, важливе значення для розвитку системи кібербезпеки України мають міжнародні стандарти та рекомендації Європейського Союзу й НАТО у сфері кіберзахисту. У процесі адаптації національного законодавства враховуються положення міжнародних документів щодо захисту інформаційного простору, протидії кіберзлочинності, забезпечення функціонування критичної інфраструктури та розвитку механізмів міжнародного співробітництва у сфері кібербезпеки. Це сприяє гармонізації українського законодавства із міжнародними стандартами та посиленню спроможності держави реагувати на сучасні кіберзагрози в умовах воєнного стану.

Після запровадження правового режиму воєнного стану в Україні відбулося суттєве посилення нормативно-правового регулювання у сфері кібербезпеки, що було обумовлено зростанням кількості кібератак на державні інформаційні ресурси, об'єкти критичної інфраструктури та інформаційно-комунікаційні системи органів державної влади. В умовах повномасштабної збройної агресії кібербезпека фактично стала одним із ключових елементів забезпечення національної безпеки та цифрової стійкості держави.

Упродовж 2022–2025 років було ухвалено низку нормативно-правових актів та управлінських рішень, спрямованих на посилення механізмів кіберзахисту. Зокрема, було розширено повноваження Державної служби спеціального зв'язку та захисту інформації України у сфері реагування на кіберінциденти й координації діяльності суб'єктів

національної системи кібербезпеки. Водночас посилено механізми захисту державних реєстрів, інформаційних систем та об'єктів критичної інфраструктури, що функціонують в умовах підвищеного рівня кіберзагроз.

Особливого значення набули рішення Ради національної безпеки і оборони України щодо забезпечення кіберстійкості держави, удосконалення системи обміну інформацією про кіберінциденти та розвитку міжвідомчої координації у сфері кібербезпеки. Крім того, в умовах воєнного стану було активізовано процес гармонізації національного законодавства із європейськими стандартами у сфері кіберзахисту та цифрової безпеки, що пов'язано з потребою в підвищенні ефективності реагування на сучасні гібридні та кібернетичні загрози.

Подальший розвиток правового забезпечення кібербезпеки в Україні пов'язаний із ухваленням Закону України від 27 березня 2025 року щодо посилення захисту інформації та кіберзахисту державних інформаційних ресурсів і об'єктів критичної інформаційної інфраструктури [17]. Зазначеним Законом передбачено створення національних систем реагування на кіберінциденти та кібератаки, удосконалення механізмів обміну інформацією про кіберзагрози, а також запровадження системи оцінювання стану кіберзахисту.

Крім того, законодавчі зміни спрямовані на впровадження механізмів управління ризиками ланцюгів постачання, розвиток комплексних систем захисту інформації та адаптацію процедур підтвердження відповідності до сучасних міжнародних стандартів у сфері кібербезпеки. Важливим нововведенням стало також розширення кола основних суб'єктів національної системи кібербезпеки за рахунок залучення Міністерства цифрової трансформації України та Міністерства закордонних справ України до реалізації державної політики у сфері кіберзахисту.

Варто зазначити, що з початком повномасштабного вторгнення російської федерації в Україну суттєво зросла кількість кібератак на державні інформаційні ресурси, об'єкти критичної інфраструктури, телекомунікаційні системи та інформаційні сервіси. Кібератаки фактично стали складовою гібридної війни, спрямованої на дестабілізацію функціонування державних інституцій, порушення інформаційної безпеки та створення панічних настроїв у суспільстві.

Ще до безпосереднього початку повномасштабних бойових дій було зафіксовано масштабні кібератаки на українську інформаційну інфраструктуру. Зокрема, за даними агентства Reuters, США та Європейський Союз офіційно звинуватили російську федерацію в здійсненні масштабного кібератакування супутникової мережі Viasat, яке відбулося 24 лютого 2022 року за годину до початку військового вторгнення [18]. Внаслідок атаки було виведено з ладу десятки тисяч супутникових терміналів, що негативно вплинуло на роботу комунікаційних систем як в Україні, так і в окремих країнах Європи.

Зазначені обставини підтверджують, що кіберпростір став одним із ключових напрямів ведення сучасної війни, а забезпечення кібербезпеки – важливим елементом національної безпеки держави в умовах воєнного стану.

Водночас сучасний розвиток системи правового забезпечення кібербезпеки в Україні значною мірою орієнтований на адаптацію міжнародних стандартів та європейських підходів у сфері кіберзахисту. Як зазначається у звіті IFES Ukraine «Cybersecurity in

Ukraine: Legal Framework Analysis», ефективне функціонування національної системи кібербезпеки потребує гармонізації українського законодавства з міжнародними нормативними та інституційними стандартами [19].

Особливе значення в цьому контексті мають положення Директиви ЄС NIS2, рекомендації ENISA, стандарти НАТО у сфері cyber defence, а також положення Будапештської конвенції про кіберзлочинність. Важливими напрямками вдосконалення національного законодавства визначаються запровадження єдиних стандартів реагування на кіберінциденти, розвиток системи обов'язкової звітності про кібератаки, удосконалення механізмів міжвідомчого обміну інформацією та створення національної системи сертифікації засобів кіберзахисту відповідно до міжнародних стандартів.

Крім того, доцільним є подальше впровадження міжнародних стандартів ISO / IEC у сфері управління інформаційною безпекою, посилення співпраці України з європейськими та євроатлантичними структурами у сфері кіберзахисту, а також розвиток механізмів державно-приватного партнерства для забезпечення кіберстійкості об'єктів критичної інфраструктури. Важливим напрямом залишається інтеграція України до міжнародних платформ обміну інформацією про кіберзагрози та вдосконалення національної системи реагування на кіберінциденти з урахуванням практик ЄС та НАТО.

Водночас, незважаючи на суттєве оновлення нормативно-правової бази у сфері кібербезпеки, сучасний стан правового регулювання в Україні все ще характеризується наявністю окремих проблем організаційного, інституційного та правозастосовного характеру. Насамперед це стосується недостатнього рівня координації між суб'єктами національної системи кібербезпеки, складності оперативного обміну інформацією про кіберінциденти, а також відсутності повної уніфікації процедур реагування на кіберзагрози відповідно до міжнародних стандартів.

Особливої актуальності зазначені проблеми набули в умовах воєнного стану, коли кібератаки стали одним із ключових інструментів гібридної війни. Постійне зростання кількості атак на державні інформаційні ресурси, енергетичну інфраструктуру, банківський сектор, телекомунікаційні мережі та цифрові сервіси свідчить про потребу в подальшому посиленні механізмів правового регулювання та інституційного забезпечення кібербезпеки. У сучасних умовах забезпечення кіберстійкості держави вже не може розглядатися виключно як технічне питання, оскільки воно безпосередньо пов'язане із функціонуванням системи державного управління, національної безпеки та обороноздатності держави.

Окремої уваги потребує питання забезпечення кібербезпеки об'єктів критичної інфраструктури. Повномасштабна збройна агресія РФ продемонструвала вразливість енергетичного сектору, транспортної інфраструктури, систем зв'язку та державних реєстрів до сучасних кіберзагроз. У зв'язку з цим важливого значення набуває формування комплексної системи захисту критичної інфраструктури, яка повинна поєднувати нормативно-правові, організаційні, технічні та інформаційні механізми забезпечення кіберстійкості держави.

Актуальність зазначених проблем підтверджується також сучасними міжнародними дослідженнями у сфері кібербезпеки, які вказують на зростання кількості комплексних кібератак на державні інформаційні системи та об'єкти критичної інфраструктури в умовах геополітичної нестабільності [20].

Яра О. С., Дейнега М. А., Улютіна О. А., Калмикова О. В.

Особливості правового забезпечення кібербезпеки в умовах воєнного стану в Україні

Важливим напрямом подальшого розвитку правового забезпечення кібербезпеки є також удосконалення механізмів державно-приватного партнерства у сфері кіберзахисту. У сучасних умовах значна частина об'єктів критичної інфраструктури перебуває у сфері діяльності приватного сектору, що потребує належного нормативного врегулювання питань взаємодії державних органів та приватних операторів у процесі запобігання кіберзагрозам і реагування на кіберінциденти.

У зв'язку з цим доцільним є подальше вдосконалення законодавства України у сфері кібербезпеки за рахунок гармонізації національних нормативно-правових актів із законодавством Європейського Союзу, розширення міжнародного співробітництва з державами-членами НАТО та ЄС, розвитку механізмів обміну інформацією про кіберзагрози, а також запровадження сучасних стандартів кіберзахисту для державних органів та об'єктів критичної інфраструктури. Важливим напрямом залишається також підвищення рівня цифрової грамотності населення та формування ефективної системи підготовки фахівців у сфері кібербезпеки.

Отже, в умовах воєнного стану кібербезпека перетворилась на один із ключових елементів забезпечення національної безпеки держави. Сучасна система правового забезпечення кібербезпеки в Україні перебуває на етапі активного розвитку та адаптації до нових викликів, пов'язаних із гібридною агресією та стрімким зростанням кількості кіберзагроз. Ухвалення нових нормативно-правових актів, посилення міжвідомчої координації та імплементація міжнародних стандартів сприяють формуванню комплексної системи кіберзахисту держави. Водночас подальше вдосконалення правового регулювання в цій сфері залишається вагомим умовою забезпечення кіберстійкості України в сучасних умовах.

Висновки. В умовах воєнного стану кібербезпека стала одним із ключових елементів забезпечення національної безпеки України. Зростання кількості кібератак на державні інформаційні ресурси, об'єкти критичної інфраструктури та інформаційно-комунікаційні системи зумовило потребу в удосконаленні механізмів правового регулювання у сфері кіберзахисту та адаптації національного законодавства до сучасних викликів.

У результаті дослідження встановлено, що система правового забезпечення кібербезпеки в Україні формується комплексом нормативно-правових актів і стратегічних документів, які регулюють питання захисту інформаційного простору, діяльності суб'єктів національної системи кібербезпеки та реагування на кіберінциденти. Особливого значення в умовах збройної агресії набули нормативні зміни, спрямовані на посилення захисту державних інформаційних ресурсів, розвиток системи кіберстійкості та вдосконалення міжвідомчої координації у сфері кіберзахисту.

Перспективними напрямами подальшого розвитку правового забезпечення кібербезпеки є гармонізація національного законодавства із міжнародними стандартами ЄС і НАТО, удосконалення механізмів обміну інформацією про кіберзагрози, розвиток державно-приватного партнерства та посилення захисту об'єктів критичної інфраструктури. Реалізація зазначених заходів сприятиме підвищенню рівня цифрової стійкості держави й ефективності протидії сучасним кіберзагрозам.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Горун О. В. Правове забезпечення національної системи кібербезпеки. *Інформація і право*. 2024. № 1. С. 45–52. URL : <https://il.ippi.org.ua/article/view/317971>
2. Красніков С. О. Кібергігієна як чинник запобігання кіберзагрозам. *Нове українське право*. 2023. № 6. С. 118–124. URL : <https://newukrainianlaw.in.ua/index.php/journal/article/view/689>
3. Капля О. М. Правове регулювання інформаційної безпеки громадянина під час дії воєнного стану. *Експерт: парадигми юридичних наук і державного управління*. 2023. № 2. С. 67–74. URL : https://www.researchgate.net/publication/368975228_PRAVOVE_REGULUVANNA_INFORMACIYNOI_BEZPEKI_GROMADANINA_PID_CAS_DII_VOENNOGO_STANU
4. Мазепа С. В. Кібербезпека в Україні: сучасні виклики та шляхи вдосконалення законодавчого регулювання. *Актуальні проблеми правознавства*. 2024. № 1. С. 133–140. URL : <https://appj.wunu.edu.ua/index.php/appj/article/view/2142>
5. Колесник О. О. Нормативно-інституційні засади формування національної системи кібербезпеки України. *Право та державне управління*. 2025. № 1. С. 437–445. URL : https://pdu-journal.kpu.zp.ua/archive/1_2025/63.pdf
6. Федорченко О. С. Удосконалення координації діяльності суб'єктів забезпечення національної системи кібербезпеки. *Нове українське право*. 2024. № 5. С. 71–77. URL : <https://newukrainianlaw.in.ua/index.php/journal/article/view/670>
7. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL : <https://zakon.rada.gov.ua/laws/show/2163-19>
8. Про схвалення Стратегії здійснення цифрового розвитку, цифрових трансформацій і цифровізації системи управління державними фінансами на період до 2030 року : розпорядження Кабінету Міністрів України від 17.11.2021 № 1467-р. URL : <https://zakon.rada.gov.ua/laws/show/1467-2021-%D1%80/ed20250513>
9. Конституція України : Закон України від 28.06.1996 № 254к/96-ВР. URL : <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text>
10. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII. URL : <https://zakon.rada.gov.ua/laws/show/2469-19#Text>
11. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР. URL : <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text>
12. Про інформацію : Закон України від 02.10.1992 № 2657-XII. URL : <https://zakon.rada.gov.ua/laws/show/2657-12#Text>
13. Про державну таємницю : Закон України від 21.01.1994 № 3855-XII. URL : <https://zakon.rada.gov.ua/laws/show/3855-12#Text>
14. Про критичну інфраструктуру : Закон України від 16.11.2021 № 1882-IX. URL : <https://zakon.rada.gov.ua/laws/show/1882-20#Text>
15. Про електронні комунікації : Закон України від 16.12.2020 № 1089-IX. URL : <https://zakon.rada.gov.ua/laws/show/1089-20#Text>

Яра О. С., Дейнега М. А., Улютіна О. А., Калмикова О. В.

Особливості правового забезпечення кібербезпеки в умовах воєнного стану в Україні

16. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України № 447/2021. URL : <https://zakon.rada.gov.ua/laws/show/447/2021#top>
17. Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури : Закон України від 27.03.2025 № 4336-IX. URL : <https://zakon.rada.gov.ua/laws/show/4336-20#Text>
18. Війна росії проти України почалася з кібернападу на супутники за годину до вторгнення були знищені «десятки тисяч» терміналів Viasat / itc.ua.ITC.ua. URL : <https://itc.ua/ua/novini/vijna-rosiyi-proti-ukrayini-pochalasya-zkibernapadu-na-suputniki-za-godinu-do-vtorgnennyabuli-znishheni-desyatki>
19. Cybersecurity in Ukraine: Legal Framework Analysis / IFES Ukraine. 2021. URL : IFES Ukraine
20. ENISA Threat Landscape 2024. European Union Agency for Cybersecurity. URL : ENISA Threat Landscape 2024

Дата надходження 15.05.2026

Дата прийняття після рецензування 10.07.2026

Дата рекомендації 27.08.2026

Дата публікації 30.09.2026