DOI:10.35774/app2025.02.164
УДК 342.9:004.056

Світлана Мазепа,
кандидат юридичних наук, доцент,
доцент кафедри кримінального права та процесу Західноукраїнського національного університету, міжнародний дослідник Оснабрюцького університету
ORCID: https://orcid.org/0000-0003-1282-9089

КІБЕРБЕЗПЕКА В УКРАЇНІ: СУЧАСНІ ВИКЛИКИ ТА ШЛЯХИ ВДОСКОНАЛЕННЯ ЗАКОНОДАВЧОГО РЕГУЛЮВАННЯ

Сучасні реалії цифрової трансформації суспільства спричиняють критичну важливість забезпечення кібербезпеки як ключового елемента національної безпеки держави. Україна, перебуваючи в умовах перманентного протистояння гібридним загрозам та активній цифровізації державних та приватних структур, стикається з необхідністю формування ефективної системи правового регулювання у сфері кіберзахисту. Це дослідження спрямоване на комплексний аналіз сучасного стану законодавчого забезпечення кібербезпеки в Україні та визначення пріоритетних напрямів його вдосконалення.

Актуальність дослідження обумовлена стрімким розвитком інформаційно-комунікаційних технологій, зростанням кількості та витонченості кібератак, а також потребою адаптації національного законодавства до європейських стандартів кібербезпеки. Аналіз сучасних кіберзагроз демонструє їхній транскордонний характер, високий ступінь координації та використання передових технологій для заподіяння шкоди критичній інфраструктурі, державним інститутам та приватному сектору. Особлива увага приділяється дослідженню специфіки кібертероризму, інформаційних операцій та атак на об'єкти критичної інфраструктури у контексті сучасних геополітичних викликів.

Методологічна основа дослідження включає комплексний підхід до аналізу нормативно-правових актів, міжнародних угод та практики їхньої імплементації до національного законодавства. Використані методи порівняльного правознавства, системного аналізу та емпіричні методи дослідження практики правозастосування у сфері кібербезпеки. Особливу увагу приділено вивченню досвіду країн Європейського Союзу у галузі правового регулювання кіберзахисту та можливостей його адаптації до українських реалій.

Результати дослідження свідчать про наявність значних прогалин у чинному законодавстві України щодо регулювання кібербезпеки, включаючи недостатню координацію між різними державними органами, відсутність чітких механізмів реагування на кібер-інциденти та неадекватність санкцій за кібер-правопорушення. Виявлено проблеми у сфері захисту персональних даних, забезпечення безпеки критичної інформаційної інфраструктури та міжнародного співробітництва у сфері протидії кіберзлочинності. Встановлено, що існуюча нормативна база не повною мірою відповідає сучасним викликам цифрової доби та потребує комплексного реформування.

Практична значущість дослідження полягає у розробці конкретних рекомендацій щодо вдосконалення законодавчого регулювання кібербезпеки в Україні, включаючи пропозиції щодо створення інтегрованої системи кіберзахисту, удосконалення механізмів міжвідомчої взаємодії та підвищення ефективності протидії кіберзагрозам. Запропоновано моделі правового регулювання, адаптовані до специфіки української правової системи та сумісні з міжнародними стандартами кібербезпеки.

Перспективи подальших досліджень пов'язані з необхідністю постійного моніторингу еволюції кіберзагроз та відповідної адаптації законодавчої бази, розробкою механізмів публічно-приватного партнерства у сфері кібербезпеки, а також поглибленим вивченням впливу штучного інтелекту та нових технологій на систему правового регулювання кіберзахисту. Важливим напрямом є також дослідження ролі міжнародного співробітництва у формуванні глобальної архітектури кібербезпеки та місця України у цій системі.

Ключові слова: *інформаційна безпека, правоохоронна сфера, кібербезпека, правове забезпечення, адміністративно-правовий аспект, кримінальна відповідальність, адміністративна відповідальність, євроінтеграція, гармонізація законодавства, міжнародні стандарти, НАТО, Європейський Союз (ЄС), державна інформаційна політика, загрози інформаційній безпеці, імплементація права, суб'єкти інформаційної безпеки, юридична відповідальність, інформаційні правопорушення, пропаганда, штучний інтелект.*

© Світлана Мазепа, 2025

Mazepa S.

Cybersecurity in Ukraine: current challenges and ways to improve legislative regulation

The modern realities of the digital transformation of society make it critically important to ensure cybersecurity as a key element of the state's national security. Ukraine, in conditions of permanent confrontation with hybrid threats and active digitalization of state and private structures, is faced with the need to form an effective system of legal regulation in the field of cyber defense. This study is aimed at a comprehensive analysis of the current state of legislative support for cybersecurity in Ukraine and identifying priority areas for its improvement.

The relevance of the study is due to the rapid development of information and communication technologies, the increase in the number and sophistication of cyber attacks, as well as the need to adapt national legislation to European cybersecurity standards. The analysis of modern cyber threats demonstrates their cross-border nature, a high degree of coordination and the use of advanced technologies to cause damage to critical infrastructure, state institutions and the private sector. Special attention is paid to the study of the specifics of cyberterrorism, information operations and attacks on critical infrastructure in the context of modern geopolitical challenges.

The methodological basis of the study includes a comprehensive approach to the analysis of regulatory legal acts, international agreements and the practice of their implementation into national legislation. The methods of comparative law, system analysis and empirical methods of research into the practice of law enforcement in the field of cybersecurity were used. Special attention is paid to the study of the experience of the European Union countries in the field of legal regulation of cyber protection and the possibilities of its adaptation to Ukrainian realities.

The results of the study indicate the presence of significant gaps in the current legislation of Ukraine on the regulation of cybersecurity, including insufficient coordination between various state bodies, the absence of clear mechanisms for responding to cyber incidents and the inadequacy of sanctions for cyber offenses. Problems in the field of personal data protection, ensuring the security of critical information infrastructure and international cooperation in the field of countering cybercrime were identified. It was established that the existing regulatory framework does not fully meet the modern challenges of the digital age and requires comprehensive reform.

The practical significance of the study lies in the development of specific recommendations for improving the legislative regulation of cybersecurity in Ukraine, including proposals for creating an integrated system of cyber protection, improving mechanisms for interagency interaction and increasing the effectiveness of countering cyber threats. Models of legal regulation adapted to the specifics of the Ukrainian legal system and compatible with international cybersecurity standards are proposed.

Prospects for further research are related to the need for constant monitoring of the evolution of cyber threats and the appropriate adaptation of the legislative framework, the development of mechanisms for public-private partnership in the field of cybersecurity, as well as an in-depth study of the impact of artificial intelligence and new technologies on the system of legal regulation of cyber defense. An important direction is also the study of the role of international cooperation in the formation of the global cybersecurity architecture and the place of Ukraine in this system.

Keywords: *information security, law enforcement, cybersecurity, legal support, administrative-legal aspect, criminal liability, administrative liability, European integration, harmonization of legislation, international standards, NATO, European Union (EU), state information policy, information security threats, implementation of law, subjects of information security, legal liability, information offenses, propaganda, artificial intelligence.*

Постановка проблеми. Стрімкий розвиток цифрових технологій та глобальна трансформація суспільних процесів у кіберпросторі зумовили виникнення принципово нових загроз національній безпеці, які потребують адекватного правового регулювання. В умовах сучасного геополітичного протистояння Україна стала об'єктом систематичних кібератак, спрямованих на дестабілізацію критичної інфраструктури, державних інституцій та економічної системи. Ця проблематика виходить за рамки технічних аспектів інформаційної безпеки та набуває характеру комплексного виклику для всієї системи правового регулювання, оскільки традиційні підходи до забезпечення безпеки виявляються неадекватними специфіці кіберзагроз. Проблема ускладнюється відсутністю одноманітних міжнародних стандартів та принципів регулювання кібербезпеки, що створює правові колізії та прогалини у національному законодавстві.

Наукова проблема полягає у необхідності теоретичного обґрунтування концептуальних засад правового регулювання кібербезпеки в умовах гібридних загроз та цифрової трансформації державного управління. Існуючі доктринальні підходи до правового регулювання інформаційної безпеки не повною мірою враховують динамічний характер кіберзагроз, транснаціональний характер кіберпространства та специфіку правовідносин, що виникають у процесі забезпечення кіберзахисту. Теоретичні дослідження в галузі кібербезпеки характеризуються фрагментарністю та відсутністю комплексного міждисциплінарного підходу, який би інтегрував правові, технічні та соціальні аспекти проблеми. Недостатньо розробленими залишаються концептуальні основи розмежування повноважень між різними суб'єктами забезпечення кібер-

безпеки, принципи балансу між безпекою та правами людини у цифровому середовищі, а також механізми адаптації правових норм до еволюції технологій.

Практична проблема зумовлена критичними недоліками чинного законодавства України у сфері кібербезпеки, які виявляються у несистемності нормативно-правового регулювання, дублюванні функцій різних державних органів та відсутності ефективних механізмів координації їх діяльності. Існуюча правова база не забезпечує адекватного реагування на сучасні кіберзагрози, оперативного обміну інформацією про кібер-інциденти та ефективної взаємодії між державним та приватним секторами. Проблеми правозастосовчої практики включають недостатню підготовленість правоохоронних органів до розслідування кібер-злочинів, неадекватність санкцій за кібер-правопорушення та відсутність спеціалізованих судових процедур для розгляду справ у сфері кібербезпеки.

Практичні завдання включають розробку проекту комплексної реформи законодавства України щодо кібербезпеки, створення ефективної системи міжвідомчої координації та публічно-приватного партнерства, а також формування національної стратегії кібербезпеки, адаптованої до сучасних викликів. Необхідним є також створення спеціалізованих інституцій для забезпечення кібербезпеки, розробка стандартів захисту критичної інформаційної інфраструктури та механізмів міжнародного співробітництва у протидії кібер-злочинності. Практичне значення дослідження полягає у можливості використання його результатів для удосконалення нормативно-правової бази, підвищення ефективності державного управління у сфері кібербезпеки та забезпечення національних інтересів України в кіберпросторі.

Аналіз останніх досліджень і публікацій. Проблематика правового регулювання кібербезпеки останніми роками активно досліджується представниками різних наукових шкіл та напрямів. Фундаментальні теоретичні засади інформаційної безпеки закладено у роботах таких вчених, як В. А. Ліпкан, О. О. Баранов, І. В. Діордіца, які сформували концептуальні підходи до розуміння правової природи інформаційних відносин та принципів їх регулювання. Значний внесок у розробку проблематики зробили дослідження В. М. Фурашєва, А. І. Марущака, С. Г. Петрова, присвячені аналізу адміністративно-правових механізмів забезпечення інформаційної безпеки.

Зарубіжні дослідники, як-от М. Шмітт, Т. Рід, Д. Кларк, зосередили увагу на міжнародно-правових аспектах регулювання кібербезпеки та проблемах застосування традиційного міжнародного права до кіберпростору. Однак більшість існуючих досліджень мають фрагментарний характер і не забезпечують комплексного підходу до вирішення проблеми.

Особлива увага у сучасній науковій літературі приділяється аналізу специфіки кібератак на критичну інфраструктуру та розробці відповідних правових механізмів захисту. Дослідження Р. А. Калюжного, О. В. Логінова, М. В. Гуцалюка присвячені проблемам правового регулювання захисту державних інформаційних ресурсів та критичних об’єктів інформаційної інфраструктури. Значний інтерес становлять роботи європейських вчених, таких як Н. Н. Цагурія, П. Маурер, Л. А. Флоріді, які досліджують досвід імплементації Директиви ЄС про мережеву та інформаційну безпеку (NIS Directive) та можливості його адаптації до національних правових систем. Водночас недостатньо дослідженими залишаються питання адаптації європейських стандартів кібербезпеки до специфіки української правової системи та особливостей функціонування національної критичної інфраструктури в умовах гібридних загроз.

Незважаючи на значний обсяг наукових досліджень, присвячених різним аспектам кібербезпеки, залишається невирішеним низка принципових питань, які становлять предмет даного дослідження. По-перше, недостатньо розробленими залишаються концептуальні засади інтеграції принципів кібербезпеки до системи національного права з урахуванням специфіки української правової традиції та сучасних викликів. По-друге, вимагає глибокого аналізу проблема адаптації міжнародних стандартів кібербезпеки до умов гібридної війни та необхідності одночасного забезпечення національної безпеки та інтеграції до європейського правового простору.

Мета статті полягає у комплексному аналізі сучасного стану правового регулювання кібербезпеки в Україні, виявленні системних недоліків чинного законодавства та розробці науково обґрунтованих рекомендацій щодо його вдосконалення у контексті сучасних викликів цифрової доби. Дослідження спрямоване на формування концептуальних засад інтегрованого підходу до правового забезпечення кібербезпеки, що враховує специфіку української правової системи, вимоги європейської інтеграції та особливості функціонування держави за умов гібридних загроз. Досягнення поставленої мети передбачає створення теоретико-методологічної бази для подальшого розвитку правової доктрини кібербезпеки та практичних механізмів її реалізації у системі національного законодавства.

Виклад основного матеріалу дослідження. Кібербезпека в Україні набула критичного значення в умовах сучасних глобальних викликів та воєнного стану. Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» від 2017 року, кібербезпека визначається як захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору [11]. Як зазначає професор В.Л. Бурячок у своєму підручнику «Інформаційна та кібербезпека: соціотехнічний аспект», сучасна кібербезпека є складною соціотехнічною системою, що потребує комплексного підходу до забезпечення захисту критичної інфраструктури та інформаційних ресурсів держави [2].

Важливим кроком у розвитку кібербезпекової галузі стало прийняття у 2025 році нового Закону України «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури», який передбачає «створення єдиної системи реагування на кібератаки, появу відповідальних за кібербезпеку в органах влади та залучення приватного сектору» [19]. Це законодавче оновлення значно розширює повноваження Держспецзв'язку та створює більш системний підхід до забезпечення кібербезпеки.

У 2023-2024 роках було затверджено план заходів з реалізації Стратегії кібербезпеки України [12] , а у 2025 році цей план було оновлено та розширено. Кабмін затвердив план заходів на 2025 рік з реалізації Стратегії кібербезпеки, що свідчить про системний підхід до впровадження кібербезпекових ініціатив.

Стратегія кібербезпеки України, затверджена Указом Президента від 14 вересня 2021 року, визначає основні напрями розвитку національної системи кібербезпеки до 2025 року [13]. Документ передбачає створення ефективної системи управління кіберризиками, розвиток державно-приватного партнерства та забезпечення кіберстійкості критичної інфраструктури. Як підкреслює Н. І. Логінова у монографії «Кібернетична безпека держави: теоретико-правовий аспект», стратегічне планування є основою для формування дієвої системи протидії кіберзагрозам та забезпечення національної безпеки в кіберпросторі [6].

Нормативно-правова база кібербезпеки України зазнала значних змін у 2025 році з прийняттям оновленого законодавства. Новий закон передбачає створення єдиної системи реагування на кібератаки, появу відповідальних за кібербезпеку в органах влади та активне залучення приватного сектору до забезпечення кібернетичної безпеки [19]. Ю. А. Гульванська у дослідженні «Правове регулювання кібербезпеки в Україні: сучасний стан та перспективи розвитку» аналізує ці зміни як важливий крок до європейської інтеграції та гармонізації національного законодавства з міжнародними стандартами кібербезпеки [4].

Воєнний стан в Україні кардинально змінив підходи до забезпечення кібербезпеки та створив нові виклики для національної безпеки [5]. О. В. Остапенко та П. С. Берназ у статті «Кіберзлочинність як загроза національній безпеці України» підкреслюють, що російська агресія супроводжується масштабними кібератаками на критичну інфраструктуру, державні інформаційні системи та приватні підприємства [8]. Гібридний характер сучасного конфлікту вимагає адаптації існуючої системи кібербезпеки до умов воєнного часу та розробки спеціальних механізмів протидії кіберзагрозам [9].

Імплементація Стратегії кібербезпеки України здійснюється через затверджені плани заходів, які регулярно оновлюються відповідно до змін безпекового середовища. Постанова КМУ про затвердження плану заходів на 2025 рік з реалізації Стратегії кібербезпеки передбачає конкретні кроки щодо підвищення кіберстійкості держави [13]. А. І. Марущак у дослідженні «Стратегія кібербезпеки України: правові засади та механізми реалізації» аналізує ефективність цих механізмів та пропонує шляхи їх вдосконалення через посилення координації між різними відомствами та створення єдиного центру управління кіберінцидентами [7].

Міжнародне співробітництво у сфері кібербезпеки стало одним з пріоритетних напрямів зовнішньої політики України. К. М. Петров у статті «Міжнародне співробітництво у сфері кібербезпеки: український досвід» [10] досліджує участь України в міжнародних ініціативах з кібербезпеки, включаючи співпрацю з НАТО, ЄС та іншими міжнародними організаціями. Особлива увага приділяється обміну розвідувальною інформацією про кіберзагрози та спільним навчанням з реагування на кіберінциденти, що значно підвищує ефективність національної системи кібербезпеки.

Правові аспекти забезпечення кібербезпеки в умовах збройного конфлікту потребують особливої уваги з боку законодавця та правозастосовних органів. В. В. Шемчук та О. Л. Костенко у дослідженні «Кіберпростір як сфера національної безпеки: правові засади забезпечення» аналізують специфіку правового регулювання кіберпростору в умовах воєнного стану [15]. Автори підкреслюють необхідність розробки спеціальних норм, які враховують особливості кібероперацій під час збройного конфлікту та забезпечують адекватну правову відповідь на гібридні загрози.

Державно-приватне партнерство у сфері кібербезпеки набуває все більшого значення для забезпечення комплексного захисту національного кіберпростору. Колективна монографія «Україна в умовах гібридної агресії: правові аспекти кібербезпеки» за редакцією В. М. Фурашева досліджує механізми взаємодії державного та приватного секторів у протидії кіберзагрозам [14]. Особлива увага приділяється створенню ефективних каналів обміну інформацією про кіберінциденти та координації дій щодо реагування на кібератаки на об'єкти критичної інфраструктури.

Міжнародний досвід правового регулювання кібербезпеки, представлений у звіті IFES Ukraine «Cybersecurity in Ukraine: Legal Framework Analysis», демонструє необхідність адаптації кращих світових практик до українських реалій [16]. Дослідження підкреслює важливість гармонізації національного законодавства з європейськими директивами та міжнародними конвенціями у сфері кібербезпеки. Особливо актуальним є впровадження стандартів звітності про кіберінциденти та створення національної системи сертифікації засобів кіберзахисту відповідно до міжнародних стандартів (Таблиця 1).

Таблиця 1

Міжнародний досвід правового регулювання кібербезпеки

Критерій аналізу	Міжнародні стандарти та практики	Адаптація для України (згідно з дослідженням IFES Ukraine)
Гармонізація законодавства	– ЄС: Директива NIS2, GDPR, ENISA рекомендації – НАТО: Стандарти cyber defence (Tallinn Manual) – ООН: Конвенція про кіберзлочинність (Будапештська конвенція) – США: Cybersecurity Framework (NIST)	– Імплементація NIS2 та GDPR у національне законодавство – Вдосконалення закону «Про основні засади кібербезпеки України» – Узгодження з Будапештською конвенцією для міжнародного співробітництва – Впровадження NIST-подібних стандартів для критичної інфраструктури
Звітність про кіберінциденти	– ЄС: Обов'язкова звітність для операторів критичної інфраструктури (NIS2) – США: Система CISA (Cybersecurity & Infrastructure Security Agency) – ISO/IEC 27035: Стандарти реагування на інциденти	– Створення єдиного центру збору та аналізу кіберінцидентів (на кшталт CERT-UA) – Впровадження обов'язкового повідомлення про атаки для держорганів та критичних об'єктів – Використання ISO/IEC 27035 для національних протоколів реагування
Сертифікація кіберзахисту	– ЄС: Схема сертифікації ENISA (EU Cybersecurity Certification Framework) – США: FIPS 140-2 для криптографічних стандартів – ISO/IEC 15408: Критерії оцінки безпеки IT-продуктів (Common Criteria)	– Розробка національної системи сертифікації з урахуванням ENISA та Common Criteria – Впровадження стандартів для державних закупівель IT-рішень – Партнерство з НАТО для сертифікації військових кіберсистем
Міжнародна співпраця	– НАТО: Cooperative Cyber Defence Centre of Excellence (CCDCOE) – ЄС: Механізми обміну даними через Europol's EC3 – G7: Глобальні ініціативи з протидії кіберзлочинності	– Участь у міжнародних платформах (наприклад, CCDCOE) – Підписання угод про кіберрозслідування з ЄС та США – Інтеграція з системами раннього попередження NATO (на кшталт Malware Information Sharing Platform)
Захист критичної інфраструктури	– ЄС: Директива CER (Critical Entities Resilience) – США: CISA's Shields Up для захисту інфраструктури – Світовий банк: Рекомендації з кіберстійкості для енергетики, фінансів, транспорту	– Впровадження сегментації мереж за зразком NERC CIP (США) – Розвиток Public-Private Partnerships (PPP) для захисту енергосистеми – Використання рекомендацій Світового банку для реформ у фінансовому секторі

Джерело: Створено автором за матеріалами: https://ifesukraine.org/wp-content/uploads/2021/04/IFES-Ukraine-Cybersecurity-Legal-Framework-Overview-2020-v2-2021-04-01-Eng.pdf

Перспективи розвитку законодавчого регулювання кібербезпеки в Україні пов'язані з необхідністю створення більш гнучкої та адаптивної правової системи, здатної швидко реагувати на нові кіберзагрози. Дослідження «Digital Security in Wartime: Ukrainian Experience and International Best Practices» підкреслює важливість розробки механізмів швидкого оновлення нормативної бази та впровадження ризик-орієнтованого підходу до регулювання кібербезпеки [17]. Майбутні зміни в законодавстві повинні забезпечити баланс між необхідністю захисту національної безпеки та дотриманням прав і свобод громадян в цифровому

просторі, створюючи надійну основу для сталого розвитку цифрової економіки України в післявоєнний період.

Висновки. Проведене дослідження дозволило встановити, що сучасний стан правового регулювання кібербезпеки в Україні характеризується значними системними вадами, які суттєво обмежують ефективність протидії кіберзагрозам та не відповідають масштабам викликів цифрової доби. Чинне законодавство демонструє фрагментарність та відсутність цілісної концепції правового забезпечення кібербезпеки, що проявляється у дублюванні функцій різних державних органів, недостатній координації їхньої діяльності та відсутності чітких механізмів розмежування компетенції. Встановлено, що існуюча нормативно-правова база не забезпечує адекватного реагування на кіберзагрози, що динамічно змінюються, і вимагає комплексного реформування з урахуванням кращих міжнародних практик та специфіки української правової системи.

Аналіз сучасних кіберзагроз виявив їх якісно новий характер, який принципово відрізняється від традиційних форм протиправних посягань та потребує розробки інноваційних правових механізмів протидії. Встановлено, що підходи до класифікації кібер-інцидентів та визначення об'єктів кібербезпеки не повною мірою враховують специфіку сучасних атак на критичну інфраструктуру, використання штучного інтелекту в кібер-операціях та транскордонний характер більшості кіберзагроз. Дослідження показало необхідність перегляду традиційних концепцій юрисдикції та відповідальності у контексті кіберпростору, а також розробки нових принципів міжнародного співробітництва у сфері протидії кібер-злочинності. Особливого значення набуває проблема правового регулювання використання кібер-технологій в умовах збройного конфлікту та необхідність інтеграції норм міжнародного гуманітарного права з принципами кібербезпеки.

Компаративний аналіз міжнародного досвіду правового регулювання кібербезпеки дозволив виявити найефективніші моделі та механізми, які можуть бути адаптовані до українських умов з урахуванням національних особливостей та пріоритетів. Встановлено, що успішні моделі правового регулювання характеризуються комплексним підходом до забезпечення кібербезпеки, ефективною координацією між державними органами та приватним сектором, а також наявністю адаптивних механізмів реагування на нові види кіберзагроз. Дослідження показало важливість створення спеціалізованих інституцій для забезпечення кібербезпеки, які мають необхідні технічні компетенції та правові повноваження для ефективної протидії кібер-інцидентам. На особливу увагу заслуговує досвід європейських країн у галузі імплементації директив ЄС з кібербезпеки та створення національних стратегій цифрової безпеки.

Розроблені під час дослідження концептуальні основи вдосконалення законодавчого регулювання кібербезпеки базуються на принципах системності, пропорційності, технологічної нейтральності та адаптивності до динаміки цифрових трансформацій. Обґрунтовано, що ефективне правове регулювання кібербезпеки має забезпечувати баланс між імперативними вимогами національної безпеки та захистом конституційних прав громадян у цифровому середовищі. Дослідження показало необхідність створення гнучкої системи правових норм, яка може оперативно адаптуватися до появи нових технологій та форм кіберзагрозу без кардинального перегляду основних принципів регулювання. Важливим елементом запропонованої концепції є інтеграція механізмів саморегулювання та співрегулювання до системи державного управління кібербезпекою, що дозволить більш ефективно використовувати експертизу приватного сектору та забезпечити інноваційний характер правового регулювання.

Перспективи подальших досліджень пов'язані з необхідністю детальної розробки окремих аспектів правового регулювання кібербезпеки, включаючи правові механізми регулювання штучного інтелекту у сфері кібер-захисту, іноблеми квантової криптографії та постквантової безпеки, а також правові аспекти забезпечення кібербезпеки в контексті розвитку технологій Інтернету речей та 5G мереж. Актуальним напрямом є дослідження правових механізмів міжнародного співробітництва у сфері кібербезпеки та розробка концепції глобального управління кіберпростором. Особливого значення набуває вивчення впливу кліматичних змін на кібербезпеку та розробка правових механізмів забезпечення стійкості критичної інформаційної інфраструктури.

Список використаних джерел

1. Арістова В. І., Сулацький Д. В. Інформаційна безпека людини як споживача телекомунікаційних послуг: монографія. Київ: Право України, 2013. 184 с.
2. Бурячок В.Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник. Київ: Борис Грінченко Київський столичний університет, 2020. 346 с.

3. Бурячок В.Л. Основи інформаційної та кібернетичної безпеки: навчальний посібник. Київ: НАУ, 2019. 278 с.
4. Гульванська Ю.А. Правове регулювання кібербезпеки в Україні: сучасний стан та перспективи розвитку. *Інформація і право*. 2024. № 2(49). С. 45–52.
5. Шевчук О., Ментух Н. Реалізація політики державної інформаційної безпеки України в контексті запобігання корупції: адміністративно-правовий аспект. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2021. Випуск 64. С. 282–287. URL: http://visnyk-juris-uzhnu-uz.com/wp-content/uploads/2021/06/NVUzhNU_64.pdf (дата звернення: 20.05.2025).
6. Логінова Н. І. Кібернетична безпека держави: теоретико-правовий аспект: монографія. Харків: Право, 2023. 224 с.
7. Марущак А. І. Стратегія кібербезпеки України: правові засади та механізми реалізації. Вісник Національного університету «Львівська політехніка». Юридичні науки. 2024. № 2(38). С. 112–119.
8. Остапенко О. В., Берназ П. С. Кіберзлочинність як загроза національній безпеці України. *Науковий вісник Національної академії внутрішніх справ.* 2024. № 1(130). С. 78–86.
9. Mazepa S., Bratasyuk O. (2023): Die Gewährleistung der Informationssicherheit in der Ukraine – Verwaltungs-und strafrechtliche Maßnahmen. OER Osteuropa Recht. T. 68. №. 4. 421-442.
10. Петров К. М. Міжнародне співробітництво у сфері кібербезпеки: український досвід. *Актуальні проблеми міжнародних відносин*. 2023. Вип. 157. С. 92–105.
11. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII (в редакції від 03.04.2025). База даних «Законодавство України». URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 20.05.2025).
12. Про затвердження плану заходів на 2023-2024 роки з реалізації Стратегії кібербезпеки України: Постанова КМУ від 19.12.2023 № 1163. *Офіційний вебсайт КМУ*. URL: https://www.kmu.gov.ua/npas/pro-zatverdzhennia-planu-zakhodiv-na-20232024-roky-z-realizatsii-stratehii-kiberbezpeky-ukrainy-i191223-1163 (дата звернення: 20.05.2025).
13. Стратегія кібербезпеки України: Указ Президента України від 14.09.2021 № 447/2021. *Офіційне інтернет-представництво Президента України*. URL: https://www.president.gov.ua/documents/4472021-40013 (дата звернення: 20.05.2025).
14. Україна в умовах гібридної агресії: правові аспекти кібербезпеки: колективна монографія / за ред. В.М. Фурашева. Київ: НІСД, 2024. 312 с.
15. Шемчук В. В., Костенко О. Л. Кіберпростір як сфера національної безпеки: правові засади забезпечення. *Науковий вісник публічного та приватного права*. 2024. Вип. 3. С. 167–174.
16. Cybersecurity in Ukraine: Legal Framework Analysis. IFES Ukraine Report, 2024. 156 p.
17. Digital Security in Wartime: Ukrainian Experience and International Best Practices / Ed. by M. Thompson, O. Kovalenko. Kyiv: Digital Ukraine Institute, 2024. 289 p.
18. Legal Aspects of Cybersecurity During Armed Conflicts: Ukrainian Case Study. *International Journal of Cyber Law*. 2024. Vol. 12, Issue 3. P. 45–67.
19. Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури: Закон України від 27 березня 2025 року № 4336-IX. URL: https://zakon.rada.gov.ua/laws/show/4336-20#Text (дата звернення: 20.05.2025).

References

1. Aristova, V. I. & Sulatskyi, D. V. (2013). *Informatsiyna bezpeka lyudyny yak spozhyvacha telekomunikatsiynykh posluh: monohrafiya [Information security of a person as a consumer of telecommunication services: monograph]*. Kyiv: Pravo Ukrainy [in Ukrainian].
2. Buriachok, V. L. (2020). I*nformatsiyna ta kiberbezpeka: sotsiotekhnichnyy aspekt: pidruchnyk [Information and cybersecurity: sociotechnical aspect: textbook]*. Kyiv: Borys Grinchenko Kyiv Metropolitan University [in Ukrainian].
3. Buriachok, V. L. (2019). *Osnovy informatsiynoyi ta kibernetychnoyi bezpeky: navchalnyi posibnyk [Fundamentals of information and cybernetic security: educational manual]*. Kyiv: NAU [in Ukrainian].
4. Hulvanska, Yu. A. (2024). Pravove rehulyuvannya kiberbezpeky v Ukrayini: suchasnyy stan ta perspektyvy rozvytku [Legal regulation of cybersecurity in Ukraine: current state and development prospects]. *Informatsiya i pravo - Information and Law, 2(49),* 45-52 [in Ukrainian].

5. Shevchuk, O., Mentukh, N. (2021). Realizatsiya polityky derzhavnoyi informatsiynoyi bezpeky Ukrayiny v konteksti zapobihannya koruptsiyi: administratyvno-pravovyy aspekt [Implementation of Ukraine's state information security policy in the context of corruption prevention: administrative and legal aspect]. *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Seriia: Pravo - Scientific Bulletin of Uzhhorod National University. Series: Law, 64,* 282–287. Retrieved from http://visnyk-juris-uzhnu-uz.com/wp-content/uploads/2021/06/NVUzhNU_64.pdf [in Ukrainian].
6. Loginova, N. I. (2023). *Kibernetychna bezpeka derzhavy: teoretyko-pravovyy aspekt: monohrafiya [Cybernetic security of the state: theoretical and legal aspect: monograph]*. Kharkiv: Pravo [in Ukrainian].
7. Marushchak, A. I. (2024). Stratehiya kiberbezpeky Ukrayiny: pravovi zasady ta mekhanizmy realizatsiyi [Ukraine's cybersecurity strategy: legal foundations and implementation mechanisms]. *Visnyk Natsionalnoho universytetu «Lvivska politekhnika». Yurydychni nauky - Bulletin of Lviv Polytechnic National University. Legal Sciences, 2(38),* 112-119 [in Ukrainian].
8. Ostapenko, O. V. & Bernaz, P. S. (). Kiberzlochynnist yak zahroza natsionalniy bezpetsi Ukrayiny [Cybercrime as a threat to Ukraine's national security]. *Naukovyi visnyk Natsionalnoi akademii vnutrishnikh sprav - Scientific Bulletin of the National Academy of Internal Affairs, 1(130),* 78-86. [in Ukrainian].
9. Mazepa, S. & Bratasyuk, O. (2023). Die Gewährleistung der Informationssicherheit in der Ukraine–Verwaltungs-und strafrechtliche Maßnahmen. *OER Osteuropa Recht, 68(4),* 421-442 [in German].
10. Petrov, K. M. (2023). Mizhnarodne spivrobitnytstvo u sferi kiberbezpeky: ukrayinskyy dosvid [International cooperation in cybersecurity: Ukrainian experience]. *Aktualni problemy mizhnarodnykh vidnosyn - Current Problems of International Relations, 157,* 92-105 [in Ukrainian].
11. *Pro osnovni zasady zabezpechennya kiberbezpeky Ukrayiny: Zakon Ukrayiny vid 05.10.2017 № 2163-VIII [On the Basic Principles of Cybersecurity in Ukraine: Law of Ukraine dated 05.10.2017 № 2163-VIII]* (as amended on 03.04.2025). (2017). Database «Legislation of Ukraine». Verkhovna Rada of Ukraine. Retrieved from https://zakon.rada.gov.ua/laws/show/2163-19 [in Ukrainian].
12. *Pro zatverdzhennya planu zakhodiv na 2023-2024 roky z realizatsiyi Stratehiyi kiberbezpeky Ukrayiny: Postanova KMU vid 19.12.2023 № 1163 [On approval of the action plan for 2023-2024 for the implementation of Ukraine's Cybersecurity Strategy: Resolution of the Cabinet of Ministers dated 19.12.2023 № 1163]*. (2023). Official website of the Cabinet of Ministers. Retrieved from https://www.kmu.gov.ua/npas/pro-zatverdzhennia-planu-zakhodiv-na-20232024-roky-z-realizatsii-stratehii-kiberbezpeky-ukrainy-i191223-1163 [in Ukrainian]
13. Stratehiya kiberbezpeky Ukrayiny: Ukaz Prezydenta Ukrayiny vid 14.09.2021 № 447/2021 [Ukraine's Cybersecurity Strategy: Decree of the President of Ukraine dated 14.09.2021 № 447/2021] (2021). *Official Internet Representation of the President of Ukraine*. Retrieved from https://www.president.gov.ua/documents/4472021-40013 [in Ukrainian].
14. Furashev, V. M. (Ed.). (2024). *Ukrayina v umovakh hibrydnoyi ahresiyi: pravovi aspekty kiberbezpeky: kolektyvna monohrafiya [Ukraine under hybrid aggression: legal aspects of cybersecurity: collective monograph]*. Kyiv: NISD [in Ukrainian].
15. Shemchuk, V. V. & Kostenko, O. L. (2024). Kiberprostir yak sfera natsional′noyi bezpeky: pravovi zasady zabezpechennya] Cyberspace as a sphere of national security: legal foundations of provision. *Naukovyi visnyk publichnoho ta pryvatnoho prava - Scientific Bulletin of Public and Private Law, 3,* 167-174 [in Ukrainian]
16. *Cybersecurity in Ukraine: Legal Framework Analysis. IFES Ukraine Report*, 2024 [in English].
17. Thompson, M. & Kovalenko, O. (Eds.) (2024). *Digital Security in Wartime: Ukrainian Experience and International Best Practices.* Kyiv: Digital Ukraine Institute [in English].
18. Legal Aspects of Cybersecurity During Armed Conflicts: Ukrainian Case Study (2024). *International Journal of Cyber Law, 12(3),* 45-67 [in English].
19. *Pro vnesennya zmin do deyakykh zakoniv Ukrayiny shchodo zakhystu informatsiyi ta kiberzakhystu derzhavnykh informatsiynykh resursiv, obyektiv krytychnoyi informatsiynoyi infrastruktury: Zakon Ukrayiny vid 27 bereznya 2025 roku № 4336-IX [On amendments to certain laws of Ukraine regarding information protection and cyber protection of state information resources, critical information infrastructure objects: Law of Ukraine dated March 27, 2025 № 4336-IX]* (2025). Retrieved from https://zakon.rada.gov.ua/laws/show/4336-20#Text [in Ukrainian].

Стаття надійшла до редакції 05.06.2025