УДК 351.746.1:004:35.07

https://doi.org/10.62664/cpa.2026.01.14

Ганна КИРИЧЕНКО,
доцент кафедри міжнародних відносин
та політичного консалтингу,
Відкритий міжнародний університет розвитку людини «Україна»,
кандидат наук з державного управління
ORCID ID https://orcid.org/0000-0003-1067-8758

ДЕРЖАВНЕ РЕГУЛЮВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ЦИФРОВІЗАЦІЇ: ПРАВОВИЙ ТА ІНСТИТУЦІЙНИЙ АСПЕКТ

У статті досліджено особливості державного регулювання інформаційної безпеки в умовах інтенсивної цифровізації суспільства та зростання масштабів інформаційних загроз, що супроводжують процеси цифрової трансформації державного управління і суспільних відносин. Розкрито сутність інформаційної безпеки як важливого складника національної безпеки держави та визначено її роль у системі публічного управління в контексті забезпечення стабільності суспільного розвитку, захисту національних інтересів, підтримання інформаційного суверенітету держави та мінімізації ризиків деструктивного інформаційного впливу. Установлено, що сучасні процеси цифровізації, поряд із розширенням можливостей використання інформаційно-комунікаційних технологій, формують нові виклики, пов'язані із кіберзагрозами, інформаційними маніпуляціями, поширенням дезінформації, втручанням у функціонування державних інформаційних систем та порушенням безпеки персональних даних.

Особливої уваги надано аналізу правових та інституційних аспектів формування та реалізації державної політики у сфері захисту інформаційного простору. Визначено, що сучасна система державного регулювання інформаційної безпеки потребує комплексного нормативно-правового забезпечення, здатного оперативно реагувати на динамічні зміни цифрового середовища та адаптуватися до нових викликів і ризиків. Проаналізовано сучасний стан нормативно-правового забезпечення інформаційної безпеки, охарактеризовано основні законодавчі акти та стратегічні документи, що регулюють діяльність у сфері інформаційної та кібербезпеки, а також визначено ключові напрями їх удосконалення в умовах розвитку цифрових технологій та інтеграції України до європейського правового простору.

Обґрунтовано, що ефективне державне регулювання інформаційної безпеки можливе лише за умов комплексного поєднання правових норм, інституційних механізмів та сучасних технологічних інструментів. Доведено, що забезпечення стійкості інформаційного середовища держави вимагає не лише модернізації законодавчої бази, а й посилення інституційної спроможності органів публічного управління, розвитку кадрового потенціалу, підвищення рівня цифрової компетентності та формування ефективної системи стратегічного управління інформаційною безпекою. Зроблено висновок про потребу дальшого вдосконалення правового регулювання, зміцнення інституційної спроможності органів публічного управління та формування стійкої системи захисту інформаційного простору держави в умовах глобальних цифрових трансформацій і зростання масштабів сучасних інформаційних викликів.

Ключові слова: *державне регулювання, національна безпека, інформаційна безпека, публічне управління, інформація, правові механізми, цифровізація, інституційні механізми.*

Hanna KYRYCHENKO,
Associate Professor of the Department
of International Relations and Political Consulting,
Open International University of Human Development «Ukraine»,
PhD in Public Administration
ORCID ID https://orcid.org/0000-0003-1067-8758

STATE REGULATION OF INFORMATION SECURITY IN THE CONTEXT OF DIGITALIZATION: LEGAL AND INSTITUTIONAL ASPECTS

The article examines the peculiarities of state regulation of information security under conditions of intensive digitalization of society and the growing scale of information threats accompanying the processes of digital transformation in public administration and social relations. The essence of information security as an important component of the national security system is revealed, and its role within the public administration system is defined in the context of ensuring social stability, protecting national interests, maintaining state information sovereignty, and minimizing the risks of destructive information influence. It has been established that contemporary digitalization processes, alongside expanding opportunities for the use of information and communication technologies, generate new challenges related to cyber threats, information manipulation, the dissemination of disinformation, interference in the functioning of state information systems, and violations of personal data security.

Particular attention is devoted to the analysis of legal and institutional aspects of the formation and implementation of state policy in the field of information space protection. It has been determined that the modern system of state regulation of information security requires comprehensive legal and regulatory support capable of responding promptly to dynamic changes in the digital environment and adapting to

emerging challenges and risks. The current state of legal and regulatory support for information security has been analyzed, and the main legislative acts and strategic documents governing activities in the fields of information and cybersecurity have been characterized. Furthermore, key directions for their improvement have been identified in the context of technological development and Ukraine's integration into the European legal framework.

It is substantiated that effective state regulation of information security is possible only through the integrated combination of legal norms, institutional mechanisms, and modern technological tools. It has been demonstrated that ensuring the resilience of the state information environment requires not only the modernization of the legislative framework but also strengthening the institutional capacity of public administration bodies, developing human resources, enhancing digital competencies, and establishing an effective system of strategic information security management. It is concluded that there is a need for further improvement of legal regulation, strengthening the institutional capacity of public administration bodies, and developing a sustainable system for protecting the state information space in the context of global digital transformations and the increasing scale of contemporary information challenges.

Keywords: *state regulation, national security, information security, public administration, information, legal mechanisms, digitalization, institutional mechanisms.*

Постановка проблеми. Сучасний етап розвитку суспільства характеризується стрімким поширенням цифрових технологій, що охоплюють практично всі сфери суспільного життя – економіку, державне управління, освіту, фінансову систему та комунікації. Процеси цифровізації створюють нові можливості для розвитку держави, водночас породжуючи значну кількість нових ризиків та загроз у сфері інформаційної безпеки. Зростання обсягів інформаційних потоків, поширення цифрових платформ, соціальних мереж та

глобальних інформаційних систем призводить до підвищення вразливості інформаційного простору держави. У сучасних умовах інформаційна безпека стає одним із ключових компонентів національної безпеки, оскільки інформаційні загрози можуть мати суттєвий вплив на політичну стабільність, економічний розвиток та суспільну безпеку держави. Особливої актуальності ця проблема набуває в умовах гібридних конфліктів, інформаційних війн, кіберзлочинності та масового поширення дезінформації. У таких умовах держава повинна забезпечити ефективне функціонування механізмів захисту інформаційного простору та створити дієву систему протидії інформаційним загрозам.

Водночас ефективність державної політики у сфері інформаційної безпеки значною мірою залежить від рівня розвитку правових та інституційних механізмів її реалізації. Наявність сучасної нормативно-правової бази, чітке визначення повноважень органів державної влади, налагоджена система координації їх діяльності та взаємодії з іншими суб'єктами інформаційної безпеки є потрібними умовами формування ефективної системи державного регулювання у цій сфері. Однак, швидкий розвиток цифрових технологій часто випереджає процеси правового регулювання та інституційного реформування, що створює додаткові виклики для державного управління.

У зв'язку з цим виникає потреба комплексного дослідження правових та інституційних аспектів державного регулювання інформаційної безпеки в умовах цифровізації, визначення основних проблем та пошуку шляхів удосконалення механізмів реалізації державної політики у цій сфері.

Аналіз останніх досліджень і публікацій. Сучасні дослідження акцентують увагу на тому, що інформаційна безпека стала невіддільним складником національної безпеки, що вимагає впровадження нових підходів до протидії кіберзлочинності та захисту критичної інфраструктури [4, 9]. У науковому дискурсі вагоме місце посідають питання адаптації національного кримінального законодавства до міжнародних стандартів, зокрема шляхом

імплементації положень Конвенції про кіберзлочинність, що дозволяє ефективніше кваліфікувати правопорушення у цифровому просторі [4, 6]. Важливим вектором досліджень є вивчення можливостей застосування міжнародних стандартів серії ISO/IEC 27000 для побудови систем управління інформаційною безпекою на державному рівні [6, 10]. Окремі науковці наголошують на потребі чіткого законодавчого закріплення ролі та функцій офіцерів з інформаційної безпеки (CISO), оскільки саме їхня діяльність є критичною для забезпечення операційної стійкості організацій у контексті постійних кіберзагроз [3, 7]. Крім того, у сучасних публікаціях обґрунтовується доцільність впровадження архітектури «нульової довіри» як стандарту захисту, що мінімізує ризики внутрішніх загроз в урядових мережах [9, 10]. Не оминається увагою і проблематика правового регулювання новітніх технологій, таких як Інтернет речей (IoT), де вразливості пристроїв потребують встановлення жорстких вимог до виробників та імпортерів обладнання [8]. Водночас аналітики наголошують, що забезпечення персональних даних громадян за стандартами, аналогічними до GDPR, є обов'язковою умовою для інтеграції України до європейського правового простору та підвищення загальної довіри до державних цифрових сервісів [5].

Метою статті є дослідження особливостей державного регулювання інформаційної безпеки в умовах цифровізації, а також аналіз правових та інституційних механізмів забезпечення ефективного функціонування системи захисту інформаційного простору держави.

Виклад основного матеріалу. Правовий вимір державного регулювання інформаційної безпеки полягає у формуванні несуперечливої, актуальної та гнучкої нормативно-правової бази, що б випереджала або принаймні адекватно реагувала на виклики цифровізації. Правові механізми включають у себе Конституцію, закони, підзаконні акти, доктрини та стратегії, що визначають правила поведінки в інформаційному просторі, установлюють відповідальність за їх порушення та регламентують діяльність суб'єктів забезпечення безпеки.

Особливістю сучасного правового регулювання є потреба балансування між двома фундаментальними цінностями: забезпеченням національної безпеки, з одного боку, та дотриманням права на свободу слова, вільний доступ до інформації та захист персональних даних – з іншого. Жорстке державне втручання може призвести до цензури та порушення демократичних прав, тоді як надмірна лібералізація створює сприятливе середовище для поширення дезінформації, кіберзлочинності та підриву державного суверенітету. В Україні, як і в більшості розвинених держав, правова база у цій сфері формується на кількох рівнях. На концептуально-стратегічному рівні діють Стратегія національної безпеки, Стратегія кібербезпеки та Стратегія інформаційної безпеки [1]. Такі документи визначають концептуальні засади, вектори розвитку та пріоритетні завдання для органів публічного управління. Базовий законодавчий рівень формують закони, що закріплюють основні дефініції, принципи захисту даних та об’єкти критичної інформаційної інфраструктури. На міжнародно-правовому рівні відбувається адаптація національного законодавства до норм міжнародного права, зокрема імплементація європейських стандартів захисту даних та кібербезпеки. Головною проблемою правового аспекту залишається технологічне відставання закону від реальності, що вимагає впровадження адаптивного законодавства, де закони встановлюють лише загальні принципи та цілі, а конкретні технічні вимоги та стандарти оперативно оновлюються [2].

Наявність досконалого законодавства не гарантує інформаційної безпеки без дієвої системи органів, здатних імплементувати ці норми на практиці. Інституційний аспект включає в себе сукупність державних органів, установ, організацій, а також недержавних суб’єктів, що здійснюють діяльність із забезпечення інформаційної безпеки. У системі публічного управління архітектура інституційних механізмів повинна будуватися на принципах чіткого розподілу повноважень, уникнення дублювання функцій та забезпечення оперативної координації. Така система має багаторівневу структуру: від

координаційного та стратегічного рівня до рівня формування політики та операційно-виконавчого рівня, де спеціалізовані органи здійснюють безпосередній технічний захист, протидію кіберзлочинності та розвідувально-підривній діяльності. Сучасна парадигма державного регулювання вимагає відмови від винятково монопольного контролю держави над інформаційним простором і активного залучення приватного сектору та громадянського суспільства.

Ефективність державного регулювання досягається винятково в синергії правових та інституційних аспектів. Правовий статус інституцій, межі їх компетенції та порядок взаємодії мають бути жорстко регламентовані законом, щоб уникнути зловживань та забезпечити прозорість публічного управління. Особливої актуальності набуває питання захисту критичної інформаційної інфраструктури, що стає головною мішенню в умовах сучасних гібридних протистоянь. Державне регулювання у цій сфері повинно забезпечувати не лише превентивні заходи, але й надійні алгоритми швидкого відновлення після кібератак. Тотальна цифровізація фінансового, енергетичного, транспортного та медичного секторів робить державу вкрай вразливою до будь-яких збоїв у роботі систем. Відповідно, інституційний дизайн має передбачати створення спеціалізованих центрів реагування на кіберінциденти, що функціонуватимуть у тісній взаємодії з власниками таких об’єктів. Водночас правові механізми повинні чітко визначати критерії віднесення об’єктів до критичної інфраструктури та встановлювати обов’язкові стандарти безпеки для їх операторів, незалежно від форми власності. Ще одним критичним напрямом є боротьба з когнітивними загрозами та інформаційно-психологічними операціями (ІПСО), що масово поширюються через соціальні мережі та месенджери. В умовах вільного обігу інформації публічне управління стикається зі складним демократичним парадоксом: як ефективно протидіяти деструктивним наративам ворога, не перетворюючись при цьому на тоталітарну систему цензури, що вимагає впровадження інноваційних інструментів

моніторингу на основі штучного інтелекту, активного розвитку загальнонаціональної медіаграмотності та стимулювання технологічних гігантів до саморегулювання під наглядом державних інституцій. Отже, лише комплексний, збалансований підхід, що органічно поєднує адаптивне правове поле та потужну, децентралізовану інституційну базу, здатний перетворити інформаційну безпеку з суто теоретичного концепту на реальний фундамент стійкості держави в епоху всеосяжної цифровізації [3].

Переходячи до детального аналізу, варто зазначити, що державне регулювання інформаційної безпеки в умовах тотальної цифровізації перестає бути статичною функцією контролю і перетворюється на динамічний процес управління ризиками, де правові та інституційні компоненти мають працювати як єдиний, безперебійний механізм. Сучасні правові механізми забезпечення інформаційної безпеки проходять етап складної трансформації від загальних декларативних норм до вузькоспеціалізованих техніко-юридичних регламентів. Ключовою проблемою тут є дуалізм права в цифрову епоху: потреба одночасного регулювання як змісту інформаційних потоків, так і технічної інфраструктури, що їх забезпечує. На рівні національного законодавства особлива увага надається гармонізації із міжнародними стандартами, зокрема імплементації положень Конвенції про кіберзлочинність [4], що вимагає від держави не лише криміналізації нових видів правопорушень, таких як несанкціоноване втручання в роботу систем штучного інтелекту, а й створення процесуальних можливостей для оперативного збору та легалізації цифрових доказів. Правовий аспект також охоплює сферу національної безпеки через призму захисту державного суверенітету в кіберпросторі. Поняття кіберсуверенітету нині передбачає право держави контролювати інформаційні потоки в межах своєї національної доменної зони та технічних мереж, що потребує чіткого законодавчого закріплення меж втручання та гарантій захисту прав користувачів.

Окремим блоком правового регулювання стає сфера захисту персональних даних, де в контексті цифровізації держава зобов'язана створити правовий панцир навколо приватної інформації громадян, запроваджуючи норми, аналогічні до європейського регламенту GDPR [5]. Інституційна динаміка в сучасних умовах вимагає створення гнучкої екосистеми безпеки, де центром системи в Україні є Рада національної безпеки і оборони, що через Національний координаційний центр кібербезпеки забезпечує стратегічний менеджмент, тоді як основний тягар операційної роботи лягає на Державну службу спеціального зв'язку та захисту інформації та Службу безпеки України. ДССЗЗІ виконує роль технічного регулятора, що формує державну політику у сфері криптографічного та технічного захисту, створюючи стандарти для хмарних сервісів та державних реєстрів. Водночас СБУ та Кіберполіція фокусуються на правоохоронній та контррозвідувальній діяльності, нейтралізуючи ворожі агентурні мережі та припиняючи діяльність ботоферм. Одним із найскладніших аспектів є побудова механізмів взаємодії між державними інституціями та приватним сектором, оскільки більша частина інформаційної інфраструктури належить бізнесу. Модель державно-приватного партнерства стає критично важливою, передбачаючи спільний моніторинг загроз у режимі реального часу та регулярні кібернавчання для тестування стійкості мереж. Публічне управління також має залучати громадянське суспільство через механізми медіаграмотності, оскільки кожен громадянин зі смартфоном є потенційним об'єктом атаки.

Новітні виклики, пов'язані зі штучним інтелектом, вимагають термінового правового регулювання відповідальності за шкоду, заподіяну автономними алгоритмами. Когнітивна безпека стає новим пріоритетом, де державне регулювання має балансувати між протидією деструктивним наративам та збереженням свободи слова. Важливим аспектом правового регулювання є інтеграція до національного законодавства міжнародних стандартів серії ISO/IEC 27000 [6], що слугують правовим фундаментом для побудови систем управління інформаційною безпекою. В умовах цифровізації держава повинна

вимагати від органів публічного управління обов’язкової сертифікації за цими стандартами, що дозволить уніфікувати вимоги до захисту даних. Секторальний аспект безпеки стосується захисту публічних реєстрів, де правовий механізм має забезпечувати принцип мінімізації даних та суворого розмежування прав доступу, установлюючи персональну кримінальну відповідальність адміністраторів за недбалість. Ефективність регулювання також залежить від трансформації кримінально-процесуального законодавства щодо роботи з цифровими слідами, які є вкрай нестійкими. Додатково варто наголосити на концепції цифрової стійкості (резильєнтності), що поступово замінює класичну парадигму захисту. Правове регулювання має змістити фокус із побудови непереборних бар’єрів на створення нормативних протоколів швидкого відновлення функціональності систем після успішного зламу, що вимагає інституційного закріплення ролі офіцерів з інформаційної безпеки (CISO) у кожному органі публічного управління, які мали б прямий канал комунікації з національними центрами реагування [7]. Важливим напрямом є правове визначення статусу метаданих. В умовах цифровізації саме метадані часто стають об’єктом розвідувального аналізу, тому їх правовий захист має бути прирівняно до захисту змісту повідомлень. Інституційний аспект також включає розбудову системи кібердипломатії. Держава має активно формувати міжнародні правові альянси для атрибуції кібератак (встановлення винуватця) та колективного накладання санкцій на агресорів у цифровому просторі. Так це вимагає створення спеціалізованих підрозділів у структурі Міністерства закордонних справ, які б координували свої дії з технічними фахівцями спецслужб.

На окрему увагу заслуговує питання правового регулювання інтернету речей (IoT) [8], де мільярди підключених пристроїв стають потенційними точками входу для атак на державні мережі. Держава повинна встановити жорсткі правові стандарти безпеки для виробників та імпортерів цифрового обладнання, забороняючи використання пристроїв із вразливими заводськими

налаштуваннями в органах публічної влади. Інституційна спроможність системи забезпечення безпеки напряму залежить від фінансової автономії: правові механізми мають передбачати цільове виділення відсотків від доходів від цифрових послуг на розвиток кіберзахисту. Також критичним є впровадження регуляторних «пісочниць» – спеціальних правових режимів, де нові технології захисту можуть тестуватися в реальних умовах без ризику порушення загальних бюрократичних процедур, що дозволить державі швидше адаптувати інновації штучного інтелекту для потреб національної безпеки.

З погляду публічного управління, цифровізація вимагає переходу до архітектури «нульової довіри» [9], де кожен запит на доступ до інформації, навіть усередині урядової мережі, підлягає суворій верифікації. Правове закріплення такої архітектури на рівні державних стандартів мінімізує ризики внутрішніх загроз. Водночас етичні аспекти використання ШІ для моніторингу безпеки мають бути чітко регламентовані, щоб уникнути перетворення інструментів захисту на інструменти тотального стеження, що суперечить демократичним цінностям. Таким чином, інституційний дизайн має включати систему незалежного нагляду за діяльністю самих органів інформаційної безпеки. Завершуючи аналіз, варто наголосити, що лише через неперервну правову модернізацію, зміцнення кадрового потенціалу інституцій та розвиток культури цифрової гігієни держава здатна забезпечити сталий розвиток у цифрову епоху. Вибудовування такої багаторівневої системи є не просто технічним завданням, а фундаментальною умовою збереження державності в умовах глобальних інформаційних протистоянь, де право стає головним щитом, а інституції – надійним «мечем» національних інтересів.

Дальший розвиток системи державного регулювання інформаційної безпеки в умовах цифровізації потребує не лише вдосконалення законодавчої бази, але й підвищення інституційної спроможності органів публічного управління. Правовий аспект у цій сфері передбачає формування комплексної системи нормативно-правових актів, що повинні регулювати не лише технічні

питання захисту інформації, а й соціальні, політичні та економічні процеси, пов’язані з обігом інформації у цифровому середовищі. Особливого значення набуває розроблення правових норм, спрямованих на регулювання діяльності цифрових платформ, соціальних мереж та інших інтернет-ресурсів, що відіграють важливу роль у формуванні інформаційного простору. У сучасних умовах правове регулювання інформаційної безпеки має базуватися на принципах системності, адаптивності та відповідності міжнародним стандартам. Системність означає узгодженість усіх нормативних актів у сфері інформаційної політики, кібербезпеки та захисту персональних даних [10]. Адаптивність передбачає здатність законодавства швидко реагувати на технологічні зміни, появу нових цифрових сервісів та інструментів комунікації. Водночас інтеграція до європейського правового простору вимагає гармонізації національного законодавства з правовими актами Європейського Союзу, що стосуються кібербезпеки, цифрового управління та захисту даних.

Важливим елементом правового механізму є встановлення чіткої відповідальності за порушення у сфері інформаційної безпеки. Ідеться не лише про кримінальну або адміністративну відповідальність за кіберзлочини, а й про запровадження спеціальних правових режимів контролю за обігом інформації, що становить державну таємницю або стосується критичної інформаційної інфраструктури. Водночас законодавство повинно забезпечувати баланс між інтересами безпеки держави та дотриманням прав і свобод людини, зокрема права на приватність, свободу слова та доступ до інформації. Інституційний аспект державного регулювання інформаційної безпеки передбачає формування ефективної системи органів державної влади, що відповідають за реалізацію відповідної політики. У цьому контексті особливого значення набуває чітке визначення повноважень та компетенцій кожного суб’єкта забезпечення інформаційної безпеки. Координація діяльності між різними державними структурами є потрібною умовою ефективного реагування на сучасні інформаційні загрози, зокрема кіберзлочинність, інформаційні операції та

поширення дезінформації. Окрему роль відіграє також розвиток міжвідомчої взаємодії та співпраці з міжнародними партнерами. У сучасному глобалізованому інформаційному середовищі більшість загроз має транснаціональний характер, що зумовлює потребу участі держави в міжнародних механізмах кібербезпеки та інформаційного співробітництва. Така взаємодія сприяє обміну досвідом, технологіями та інформацією про нові кіберзагрози.

Крім того, важливим елементом інституційного розвитку є формування професійного кадрового потенціалу у сфері інформаційної безпеки. Органи державної влади повинні забезпечувати підготовку фахівців, здатних ефективно працювати з сучасними інформаційними технологіями, аналізувати кіберзагрози та розробляти механізми їх нейтралізації. Підвищення рівня цифрової компетентності державних службовців та розвиток спеціалізованих освітніх програм сприятимуть зміцненню інституційної спроможності держави. Таким чином, ефективне державне регулювання інформаційної безпеки в умовах цифровізації можливе лише за умови гармонійного поєднання правових та інституційних механізмів. Законодавча база створює нормативні межі функціонування системи безпеки, тоді як інституційна структура забезпечує практичну реалізацію державної політики у цій сфері.

Висновки. Отже, цифровізація сучасного суспільства суттєво трансформує підходи до забезпечення національної безпеки, ставлячи на перший план питання захисту інформаційного простору держави. У цих умовах державне регулювання інформаційної безпеки набуває комплексного характеру та передбачає поєднання правових і інституційних механізмів публічного управління. Правовий аспект полягає у формуванні ефективної, узгодженої та адаптивної нормативно-правової бази, що регулює процеси обігу інформації, захисту даних та протидії кіберзагрозам. Інституційний аспект, своєю чергою, пов’язано із створенням та розвитком системи державних органів і механізмів координації їх діяльності, спрямованих на реалізацію державної політики у сфері

інформаційної безпеки. Ефективність державного регулювання залежить від здатності держави оперативно реагувати на нові виклики цифрового середовища, удосконалювати правові інструменти, зміцнювати інституційну спроможність органів влади та розвивати міжнародне співробітництво у сфері кібербезпеки. Лише комплексний підхід до поєднання правових норм, інституційних структур і сучасних технологічних рішень здатний забезпечити належний рівень захисту інформаційного простору та сприяти зміцненню національної безпеки держави в умовах глобальної цифрової трансформації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Заява Ради національної безпеки і оборони України. *Рада національної безпеки і оборони України*. URL: https://www.rnbo.gov.ua/ua/Diialnist/4976.html?PRINT.

2. Пашковський М. Проблеми адаптації положень загальної частини чинного та перспективного кримінального законодавства України до кримінального права ЄС. *Центр політико-правових реформ*. 2021. URL: https://pravo.org.ua/blogs/problemy-adaptatsiyi-polozhen-zagalnoyi-chastyny-chynnogo-ta-perspektyvnogo-kryminalnogo-zakonodavstva-ukrayiny-do-kryminalnogo-prava-yes.

3. Хто такий CISO і навіщо він компанії. *DOU*. 2022. URL: https://dou.ua/forums/topic/38449.

4. Конвенція про кіберзлочинність : Міжнародний документ від 23.11.2001. *Законодавство України*. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text.

5. Що таке GDPR? *Безоплатна правнича допомога*. URL: https://legalaid.ua/ua/shho-take-gdpr.

6. Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013, IDT) : ДСТУ ISO/IEC 27001:2015. *Будстандарт*. URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=66893.

7. З кого спитати : хто такі CISO і чому в Україні нікому відповідати за кібербезпеку. *Українська експортно-кредитна конфедерація*. URL: https://www.uekka.org.ua/novina/z-kogo-spitati-hto-tak%D1%96-ciso-%D1%96-chomu-v-ukrayin%D1%96-n%D1%96komu-v%D1%96dpov%D1%96dati-za-k%D1%96berbezpeku.html.

8. Інтернет речей (Internet of Things, IoT). *IT-Enterprise*. URL: https://www.it.ua/knowledge-base/technology-innovation/internet-veschej-internet-of-things-iot.

9. What is Zero Trust Architecture? *Microsoft Security*. URL: https://www.microsoft.com/en-us/security/business/security-101/what-is-zero-trust-architecture.

10. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. *Законодавство України*. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

REFERENCES

1. Zaiava Rady natsionalnoi bezpeky i oborony Ukrainy. (2026). Rada natsionalnoi bezpeky i oborony Ukrainy [Statement of the National Security and Defense Council of Ukraine. National Security and Defense Council of Ukraine]. URL: https://www.rnbo.gov.ua/ua/Diialnist/4976.html?PRINT. [in Ukrainian]

2. Pashkovskyi, M. (2021). Problemy adaptatsii polozhen zahalnoi chastyny chynnoho ta perspektyvnoho kryminalnoho zakonodavstva Ukrainy do kryminalnoho prava YeS. Tsentr polityko-pravovykh reform [Pashkovskyi M. Problems of adaptation of the provisions of the general part of the current and perspective criminal legislation of Ukraine to the EU criminal law. Centre for Policy and Legal Reform]. URL: https://pravo.org.ua/blogs/problemy-adaptatsiyi-polozhen-zagalnoyi-chastyny-chynnogo-ta-perspektyvnogo-kryminalnogo-zakonodavstva-ukrayiny-do-kryminalnogo-prava-yes. [in Ukrainian]

3. Khto takyi CISO i navishcho vin kompanii. (2022). DOU [Who is a CISO and why a company needs one. DOU]. URL: https://dou.ua/forums/topic/38449. [in Ukrainian]

4. Konventsiia pro kiberzlochynnist (2001) : Mizhnarodnyi dokument vid 23.11.2001. Zakonodavstvo Ukrainy [Convention on Cybercrime : International document dated 23.11. Legislation of Ukraine]. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text. [in Ukrainian]

5. Shcho take GDPR? Bezoplatna pravnycha dopomoha [What is GDPR? Free Legal Aid]. URL: https://legalaid.ua/ua/shho-take-gdpr. [in Ukrainian]

6. Informatsiini tekhnolohii. Metody zakhystu. Systemy upravlinnia informatsiinoiu bezpekoiu. Vymohy (ISO/IEC 27001:2013, IDT) : DSTU ISO/IEC 27001:2015. Budstandart [Information technology. Security techniques. Information security management systems. Requirements (ISO/IEC 27001:2013, IDT) : DSTU ISO/IEC 27001:2015. Budstandart]. URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=66893. [in Ukrainian]

7. Z koho spytaty : khto taki CISO i chomu v Ukraini nikomu vidpovidaty za kiberbezpeku. Ukrainska eksportno-kredytna konfederatsiia [Whom to ask : who are CISOs and why there is no one in Ukraine to be responsible for cybersecurity. Ukrainian Export-Credit Confederation]. URL: https://www.uekka.org.ua/novina/z-kogo-spitati-hto-tak%D1%96-ciso-%D1%96-chomu-v-ukrayin%D1%96-n%D1%96komu-v%D1%96dpov%D1%96dati-za-k%D1%96berbezpeku.html. [in Ukrainian]

8. Internet rechei (Internet of Things, IoT). IT-Enterprise [Internet of Things (IoT). IT-Enterprise]. URL: https://www.it.ua/knowledge-base/technology-innovation/internet-veschej-internet-of-things-iot. [in Ukrainian]

9. What is Zero Trust Architecture? Microsoft Security. URL: https://www.microsoft.com/en-us/security/business/security-101/what-is-zero-trust-architecture. [in English]

10. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy (2017) : Zakon Ukrainy vid 05.10.2017 № 2163-VIII. Zakonodavstvo Ukrainy [On the Basic Principles of Ensuring Cybersecurity of Ukraine : Law of Ukraine dated 05.10.2017 No. 2163-VIII. Legislation of Ukraine]. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text. [in Ukrainian]

Дата першого надходження статті до видання: 20.03.2026
Дата прийняття статті до друку після рецензування: 18.04.2026
Дата публікації (оприлюднення) статті: 29.05.2026