УДК 351.746.1:35.07(477)

https://doi.org/10.62664/cpa.2026.01.11

Дмитро ДРИГА,
здобувач вищої освіти за третім
(освітньо-науковим) рівнем вищої освіти,
Інститут права та суспільних відносин,
ЗВО «Відкритий міжнародний університет розвитку людини «Україна»
ORCID ID https://orcid.org/0000-0003-4426-7551

ДЕРЖАВНЕ РЕГУЛЮВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УКРАЇНІ

У науковій статті досліджено особливості державного регулювання інформаційної безпеки України в умовах сучасних геополітичних трансформацій, цифровізації суспільства та зростання масштабів інформаційних загроз. Обґрунтовано, що в сучасних умовах інформація перетворюється не лише на стратегічний ресурс суспільного розвитку, а й на важливий інструмент політичного впливу, засіб ведення гібридного протиборства та чинник забезпечення національної безпеки держави. Установлено, що інформаційна безпека є важливим складником системи публічного управління, оскільки її забезпечення безпосередньо пов'язане із захистом національних інтересів, підтриманням інформаційного суверенітету та стійкості інформаційного простору держави.

Розглянуто державне регулювання інформаційної безпеки як комплексний управлінський процес, спрямований на формування нормативно-правових, інституційних та організаційних механізмів захисту інформаційного середовища. Визначено, що сучасні процеси цифрової трансформації поряд із

розширенням можливостей використання інформаційно-комунікаційних технологій формують нові виклики, пов'язані з поширенням дезінформації, інформаційними маніпуляціями, кіберзагрозами, втручанням у функціонування державних інформаційних систем та порушенням безпеки персональних даних.

Особлива увага надається аналізу правових механізмів забезпечення інформаційної безпеки та особливостям інституційного забезпечення державної політики у відповідній сфері. Обґрунтовано потребу системного вдосконалення нормативно-правової бази відповідно до сучасних викликів цифрового середовища, а також посилення координації діяльності органів публічного управління. Наголошено на важливості розвитку міжвідомчої взаємодії, міжнародного співробітництва та впровадження сучасних цифрових технологій у сфері захисту інформаційного простору. Зроблено висновок, що ефективне державне регулювання інформаційної безпеки потребує комплексного поєднання правових, інституційних та технологічних механізмів, спрямованих на забезпечення стійкості держави в умовах сучасних інформаційних викликів.

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

Dmytro DRYHA,
PhD student
(third, educational and research level of higher education),
Institute of Law and Social Relations,
Higher Education Institution Open International University
of Human Development «Ukraine»
ORCID ID https://orcid.org/0000-0003-4426-7551

STATE REGULATION
OF INFORMATION SECURITY IN UKRAINE

The scientific article examines the peculiarities of state regulation of information security in Ukraine under conditions of contemporary geopolitical transformations, societal digitalization, and the growing scale of information threats. It is substantiated that under modern conditions, information is becoming not only a strategic resource for social development but also an important instrument of political influence, a means of conducting hybrid confrontation, and a factor in ensuring national security. It has been established that information security is an important component of the public administration system, as its provision is directly related to the protection of national interests, maintenance of information sovereignty, and ensuring the resilience of the state's information environment.

State regulation of information security is considered as a comprehensive managerial process aimed at establishing legal, institutional, and organizational mechanisms for protecting the information environment. It has been determined that contemporary processes of digital transformation, along with expanding opportunities for the use of information and communication technologies, generate new challenges related to the dissemination of disinformation, information manipulation, cyber threats, interference in the functioning of state information systems, and violations of personal data security.

Particular attention is paid to the analysis of legal mechanisms for ensuring information security and the institutional aspects of implementing state policy in this area. The necessity of systematically improving the legal and regulatory framework in accordance with the challenges of the modern digital environment, as well as strengthening coordination among public administration bodies, is substantiated. The importance of enhancing interagency cooperation, international collaboration, and the implementation of modern digital technologies in the field of information space protection is emphasized. It is concluded that effective state regulation of information security requires a comprehensive combination of legal, institutional, and

technological mechanisms aimed at ensuring state resilience under contemporary information challenges.

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

Постановка проблеми. У сучасному вимірі державотворення проблематика інформаційної безпеки трансформувалася з вузько технологічної категорії у фундаментальну основу національної безпеки України. Інформація сьогодні постає не лише ресурсом розвитку, а й потужною зброєю, інструментом гібридного впливу та ареною геополітичного протиборства. В умовах повномасштабної збройної агресії інформаційна безпека перетворилася на питання екзистенційного виживання держави, оскільки лінія фронту пролягає не лише на полі бою, а й у свідомості громадян та комп'ютерних мережах об'єктів критичної інфраструктури. Попри формування ієрархічної системи нормативних актів, державне регулювання стикається з низкою критичних викликів. По-перше, законодавче поле потребує перманентного оновлення через появу технологій deepfake, використання анонімних Telegram-каналів та криптовалют для підривної діяльності. По-друге, існує значна проблема відомчої розрізненості, дублювання функцій та дефіциту висококваліфікованих кадрів у державному секторі. Окремої уваги потребує той факт, що чинні бюрократичні процедури сертифікації комплексних систем захисту інформації (КСЗІ) часто не встигають за динамікою ІТ-розробок, що створює колізії при впровадженні інноваційних рішень, таких як екосистема «Дія».

Аналіз останніх досліджень і публікацій. Проблематика державного регулювання інформаційної безпеки України активно досліджується у сучасній науковій літературі, оскільки вона є важливою складовою національної безпеки держави в умовах цифровізації та гібридних загроз [1; 3]. Науковці зазначають, що ефективне функціонування системи інформаційної безпеки потребує комплексного нормативно-правового регулювання, розвитку інституційної

системи кіберзахисту та впровадження сучасних технологічних рішень [1; 5; 7]. Важливе місце у дослідженнях займає аналіз законодавчого забезпечення кібербезпеки, зокрема положень Закону України «Про основні засади забезпечення кібербезпеки України», що визначає принципи державної політики у цій сфері та механізми взаємодії між державними органами і приватним сектором [1]. Окремої уваги науковці надають розвитку національної системи реагування на кіберінциденти та діяльності спеціалізованих структур, зокрема команди CERT-UA [5].

Крім того, сучасні дослідження акцентують увагу на потребі гармонізації українського законодавства із міжнародними та європейськими стандартами у сфері захисту інформації та персональних даних, зокрема впровадженні положень GDPR та Директиви ЄС NIS2 [2; 8]. Крім того, у наукових працях аналізуються новітні технологічні виклики, пов'язані з розвитком криптографічних засобів захисту інформації, штучного інтелекту та цифрових технологій, що можуть створювати нові ризики для інформаційної безпеки держави [7; 9].

Метою дослідження є комплексний аналіз трансформації державного регулювання інформаційної безпеки України та визначення шляхів удосконалення правових механізмів у цій сфері.

Виклад основного матеріалу. Публічне управління інформаційною сферою еволюціонує від класичного адміністративно-командного впливу до моделі багаторівневого врядування, де держава постає координатором, об'єднуючи зусилля урядових структур, приватного сектору (зокрема IT-компаній та телекомунікаційних провайдерів), громадянського суспільства та міжнародних партнерів. Такий підхід зумовлено тим, що держава фізично не здатна самостійно контролювати весь обсяг інформаційних потоків і потребує синергії з неурядовими акторами. Державне регулювання в цьому контексті охоплює широкий спектр завдань: від розроблення стратегічних доктринальних документів до впровадження конкретних технічних стандартів

криптографічного захисту, протидії кіберзлочинності та нейтралізації інформаційно-психологічних операцій (ІПСО) противника. Особливого значення набуває створення стійкої архітектури кібербезпеки, що передбачає проактивний моніторинг загроз, оперативне реагування на інциденти та відновлення систем після потенційних атак. Правові механізми державного регулювання інформаційної безпеки в Україні формують ієрархічну систему нормативних актів, що визначають правила поведінки всіх суб'єктів інформаційних відносин. Базовим рівнем є Конституція України, що гарантує право на інформацію, проте водночас допускає його обмеження в інтересах національної безпеки та територіальної цілісності. Ключову роль відіграють закони України «Про національну безпеку України», «Про інформацію», «Про захист інформації в інформаційно-комунікаційних системах» та «Про основні засади забезпечення кібербезпеки України» [1]. Саме ці документи встановлюють дефінітивний апарат, визначають повноваження державних органів та закріплюють засади державно-приватного партнерства у сфері кіберзахисту. Проте законодавче поле не є статичним; воно потребує перманентного оновлення як відповідь на появу нових викликів, таких як технології deepfake, поширення ворожої пропаганди через анонімні Telegram-канали чи використання криптовалют для фінансування підривної діяльності. Важливим вектором удосконалення правових механізмів є їх синхронізація з європейським законодавством, зокрема імплементація Директиви ЄС про безпеку мереж та інформаційних систем та Загального регламенту про захист даних (GDPR), що є обов'язковою умовою на шляху євроінтеграції України [2].

Інституційний вимір публічного управління інформаційною безпекою подано розгалуженою мережею державних органів, кожен із яких має свою специфічну зону відповідальності. Стратегічне керівництво та координацію здійснює Рада національної безпеки і оборони (РНБО) України та створений при ній Національний координаційний центр кібербезпеки. Важливу роль відіграє Служба безпеки України, що займається контррозвідувальним захистом

інтересів держави у сфері інформаційної безпеки, виявленням та нейтралізацією агентурних мереж ворога, що діють в інфопросторі. Державна служба спеціального зв'язку та захисту інформації (Держспецзв'язок) постає головним органом у системі кіберзахисту державних електронних інформаційних ресурсів та об'єктів критичної інфраструктури. Окреме місце посідає Міністерство цифрової трансформації, що відповідає за формування політики цифровізації та підвищення цифрової грамотності населення, що є превентивним механізмом захисту від соціальної інженерії та кібершахрайства. Ефективність державного регулювання залежить від того, наскільки злагоджено ці органи взаємодіють між собою, обмінюються розвідувальними даними та координують зусилля з кіберпідрозділами Збройних сил України, особливо в умовах воєнного стану. Водночас актуальною залишається проблема подолання відомчої розрізненості, дублювання функцій та дефіциту висококваліфікованих кадрів у державному секторі, що часто не витримує конкуренції за таланти з комерційним IT-ринком.

Аналіз поточного стану вітчизняного інформаційного простору свідчить про те, що держава стикається з гібридними загрозами, які вимагають нестандартних управлінських рішень. Традиційні методи цензури чи прямого блокування ресурсів часто виявляються неефективними в епоху VPN-сервісів та децентралізованих мереж [3]. Саме тому акцент у державному регулюванні поступово зміщується з реактивних заборон на проактивну стратегію: розвиток стратегічних комунікацій, формування потужного національного наративу, підтримку незалежного медіаринку та розвиток критичного мислення у громадян. Інформаційна стійкість суспільства стає найкращим щитом проти ворожої дезінформації. Держава має створити умови, за яких громадяни зможуть самостійно верифікувати інформацію, розпізнавати маніпуляції та уникати інформаційних пасток. У цьому контексті правові механізми повинні заохочувати фактчекінг, підтримувати освітні ініціативи з медіаграмотності та встановлювати жорстку відповідальність для колаборантів і поширювачів пропаганди країни-агресора. Таким чином, державне регулювання

інформаційної безпеки в Україні постає як динамічний процес узгодження технологічних, правових, інституційних та соціальних аспектів, спрямований на гарантування суверенітету держави в інформаційному просторі та захист демократичних цінностей у цифровому світі.

Державне регулювання інформаційної безпеки в Україні за останні роки пройшло шлях від фрагментарних заходів реагування до формування цілісної стратегічної архітектури. Фундаментальною основою цього процесу є Стратегія інформаційної безпеки, затверджена Указом Президента України 2021 року, що визначила ключові вектори протидії загрозам у глобальному та національному вимірах [4]. Документ фактично заклав нову філософію публічного управління, де пріоритетом є не лише захист технічних систем, а й забезпечення інформаційної стійкості (резільєнтності) всього суспільства. Правовий механізм реалізації цієї стратегії спирається на чітку ієрархію нормативних актів, де особливе місце посідає Закон України «Про основні засади забезпечення кібербезпеки України», що не просто окреслює межі відповідальності, а й впроваджує термінологію, гармонізовану з міжнародними стандартами, зокрема щодо об’єктів критичної інформаційної інфраструктури. Державне регулювання у цьому контексті передбачає встановлення жорстких вимог до захисту систем енергопостачання, банківського сектору та державного управління, оскільки будь-яка успішна кібератака на ці сфери може призвести до дестабілізації національної безпеки в цілому.

Окремим важливим аспектом публічного управління є розмежування повноважень між суб’єктами владних повноважень, що забезпечує комплексність підходу. Служба безпеки України, виконуючи функції контррозвідувального захисту, зосереджує зусилля на виявленні зовнішніх джерел загроз, припиненні діяльності хакерських угруповань, афілійованих з іноземними спецслужбами, та боротьбі з тероризмом у цифровому середовищі. Водночас Державна служба спеціального зв’язку та захисту інформації України постає як технічний регулятор, що формує стандарти криптографічного та

технічного захисту інформації (КЗІ та ТЗІ), а також забезпечує функціонування Урядової команди реагування на комп'ютерні надзвичайні події CERT-UA [5]. У цьому зв'язку важливо розуміти, що правові механізми державного регулювання включають не лише примус чи контроль, а й стимулювання. Ідеться про створення умов для розвитку вітчизняного ринку засобів захисту інформації, що є критичним для забезпечення технологічного суверенітету, оскільки використання програмного чи апаратного забезпечення, розробленого в країнах-агресорах або країнах з недемократичними режимами, створює системні ризики «бекдорів» (прихованих вразливостей), що можуть бути активовані у вирішальний момент [6].

Процес державного регулювання також нерозривно пов'язано із захистом державної таємниці та службової інформації. У цьому контексті правові механізми забезпечують баланс між секретністю та прозорістю державного апарату. Сучасне публічне управління вимагає переходу до електронного документообігу, що, своєю чергою, ставить нові завдання перед системою технічного захисту. Запровадження комплексних систем захисту інформації (КСЗІ) є обов'язковою умовою для легітимізації будь-якої державної інформаційної системи [7]. Проте наукова дискусія вказує на те, що чинні бюрократичні процедури сертифікації КСЗІ часто не встигають за динамікою ІТ-розробок, що створює правові колізії при впровадженні інноваційних хмарних рішень чи мобільних сервісів, таких як екосистема «Дія». Тому державне регулювання потребує переходу до більш гнучких моделей, заснованих на оцінці ризиків (ризикоорієнтований підхід), що широко застосовується в країнах НАТО та ЄС.

Інформаційно-психологічний вимір безпеки є чи не найбільш складним сегментом державного регулювання. На відміну від кіберзахисту, де існують об'єктивні технічні параметри, сфера змісту інформації межує з фундаментальними правами людини на свободу думки та слова. Публічне управління тут стикається з викликом: як протидіяти ворожій пропаганді та

дезінформації, не перетворюючись на інструмент цензури. Правові механізми України в цьому напрямі еволюціонували через запровадження санкцій щодо пропагандистських ресурсів, заборону трансляції певних медіа та посилення кримінальної відповідальності за виправдання збройної агресії. Проте стратегічним напрямом є не лише заборона, а й розвиток стратегічних комунікацій держави. Так це передбачає здатність державних органів оперативно та прозоро надавати суспільству достовірну інформацію, випереджаючи ворожі вкиди. Важливим інструментом тут постає Центр протидії дезінформації при РНБО та Центр стратегічних комунікацій та інформаційної безпеки при МКІП, що здійснюють моніторинг інфополя, викривають фейки та формують контрнаративи.

Міжнародне співробітництво є ще одним наріжним каменем державного регулювання інформаційної безпеки України. Ураховуючи транскордонний характер інформаційних загроз, жодна держава не може бути безпечною в ізоляції. Україна активно інтегрується до європейського кібербезпекового простору, приєднуючись до Будапештської конвенції про кіберзлочинність та впроваджуючи нормативи Директиви NIS [8]. Публічне управління в Україні нині значною мірою орієнтується на стандарти ISO/IEC 27001, що дозволяє говорити про єдину «мову безпеки» із західними партнерами, що сприяє не лише отриманню технічної допомоги, а й обміну розвідувальними даними про нові типи вірусів чи методи хакерських атак у режимі реального часу. Таким чином, правові механізми стають мостом для інтеграції України до колективної системи безпеки демократичного світу.

Наступним рівнем аналізу є роль правових механізмів у забезпеченні інформаційної безпеки на місцевому рівні. Публічне управління не обмежується лише центральними органами влади; воно охоплює органи місцевого самоврядування, що володіють значними обсягами персональних даних громадян та керують комунальною інфраструктурою. Державне регулювання має забезпечити єдині стандарти безпеки для всієї вертикалі управління,

оскільки вразливість у мережі маленької територіальної громади може стати вхідною точкою для масштабної атаки на загальнодержавні реєстри.

Отже, правові механізми повинні включати чіткі регламенти аудиту інформаційної безпеки та відповідальність посадових осіб за недотримання встановлених норм. Ефективність державного регулювання також прямо залежить від фінансового та ресурсного забезпечення. Публічне управління у цій сфері вимагає значних інвестицій у «залізо», софт та, найголовніше, у людський капітал. Підготовка фахівців із кібербезпеки в системі вищої освіти та постійне підвищення кваліфікації державних службовців є невід'ємною частиною державної політики. Особливої уваги в контексті сучасного державного регулювання потребує аспект стрімкої інтеграції штучного інтелекту (ШІ) в інформаційний простір. Сьогодні ШІ постає не лише об'єктом захисту, а й суб'єктом загрози. Використання генеративних моделей для створення гіперреалістичних дипфейків та автоматизованих бот-мереж, здатних імітувати людську поведінку, створює виклики, що неможливо нівелювати лише класичними методами моніторингу. Правове регулювання має еволюціонувати вбік «алгоритмічної прозорості», де держава встановлює вимоги до маркування контенту, створеного ШІ, та визначає юридичну відповідальність за використання автоматизованих систем для дестабілізації суспільно-політичної ситуації, що вимагає від публічного управління не просто технічного оснащення, а розроблення етичних та правових стандартів «відповідального ШІ», що корелюють із напрацюваннями Європейського Союзу (EU AI Act) [9].

Паралельно з цим ефективність державного регулювання критично залежить від глибини державно-приватного партнерства. В умовах кібервійни кордон між державним сектором та приватним ІТ-бізнесом стає дедалі прозорішим. Держава має відігравати роль не лише контролера, а й фасилітатора, створюючи умови для залучення «етичних хакерів» та приватних кіберлабораторій до захисту національних інтересів. Запровадження механізмів *bug bounty* на державному рівні та створення спільних центрів аналізу загроз

(обмін інформацією про загрози) дозволяє оперативно масштабувати захисні спроможності [10]. У цьому розрізі правові механізми повинні забезпечувати надійний юридичний імунітет для фахівців, які діють в інтересах національної безпеки, та стимулювати інвестиції в українські розробки засобів захисту інформації, забезпечуючи повний технологічний цикл – від коду до кінцевого продукту – всередині країни.

Висновки. Державне регулювання інформаційної безпеки в Україні трансформувалося у складну, інтелектуально містку систему, що поєднує в собі жорсткість правових норм та гнучкість технологічних рішень. В умовах екзистенційної загрози та гібридної агресії Україна фактично стала світовим полігоном для відпрацювання новітніх стратегій захисту цифрового суверенітету. Ключовим досягненням останніх років став перехід від реактивної моделі «ліквідації наслідків» до проактивної філософії «національної інформаційної стійкості». Перспективи дальшого розвитку публічного управління у цій сфері вбачаються у трьох стратегічних напрямах. По-перше, це завершення гармонізації вітчизняного законодавства зі стандартами ЄС та НАТО, що забезпечить повну сумісність українських систем захисту з глобальною архітектурою безпеки західного світу. По-друге, це розбудова інклюзивної моделі безпеки, де кожна громада та кожен громадянин володіють достатнім рівнем медіаграмотності та кібергігієни, що робить суспільство несприйнятливим до маніпулятивних впливів. По-третє, це інституційне зміцнення координаційних центрів, що дозволить подолати відомчу розрізненість та забезпечити єдність дій у режимі реального часу.

Отже, інформаційна безпека нині є не просто галузевим завданням, а невід’ємним атрибутом сучасної української державності. Створення надійної архітектури захисту інформаційного простору – це тривалий процес, що вимагає синергії інтелектуального потенціалу науки, політичної волі влади та креативності громадянського суспільства. Тільки за умови комплексного поєднання правових гарантій, технологічних інновацій та високого рівня

суспільної свідомості Україна зможе не лише вистояти в інформаційній війні, а й стати лідером у формуванні глобальних стандартів безпеки цифрового майбутнього.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

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

2. Регламент (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних (GDPR). URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text.

3. Що таке VPN, і як ним безпечно користуватись / CSIRT NBU. 2023. URL: https://csirt.csi.cip.gov.ua/uk/posts/what-is-a-vpn-and-how-to-use-it-safely.

4. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26.08.2021 № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text.

5. Команда реагування на комп'ютерні надзвичайні події України (CERT-UA) : офіційний сайт. URL: https://cert.gov.ua.

6. Бекдор : Як хакери ламають системи. *Cyberset*. URL: https://cyberset.com.ua/vulnerabilities/backdoors.

7. Засіб криптографічного захисту інформації «Шифр-X.509» : опис продукту. *АТ «ІІТ»*. URL: https://cipher.com.ua/uk/products/x509.

8. Директива ЄС NIS2 : що це таке, для яких потреб розроблена та для чого Україна її імплементує. *Держспецзв'язку*. URL: https://cip.gov.ua/ua/news/direktiva-yes-nis2-sho-ce-take-dlya-yakikh-potreb-rozroblena-ta-dlya-chogo-ukrayina-yiyi-implementuye.

9. Artificial Intelligence Act Explorer (EU AI Act). URL: https://artificialintelligenceact.eu/ai-act-explorer.

10. Уряд легалізував Bug Bounty для державних систем. *Держспецзв'язку*. URL: https://cip.gov.ua/ua/news/uryad-legalizuvav-bug-bounty-dlya-derzhavnikh-sistem.

REFERENCES

1. Verkhovna Rada of Ukraine. (2017). Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy : Zakon Ukrainy vid 05.10.2017 № 2163-VIII [On the Basic Principles of Cybersecurity of Ukraine : Law of Ukraine dated October 5, 2017 No. 2163-VIII]. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text. [in Ukrainian]

2. European Parliament and Council of the European Union. (2016). Rehlament (YeS) 2016/679 vid 27 kvitnia 2016 roku pro zakhyst fizychnykh osib u zviazku z opratsiuvanniam personalnykh danykh i pro vilnyi rukh takykh danykh (GDPR) [Regulation (EU) 2016/679 of April 27, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR)]. URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text. [in Ukrainian]

3. CSIRT NBU. (2023). Shcho take VPN, i yak nym bezpechno korystuvatys [What is VPN and how to use it safely]. URL: https://csirt.csi.cip.gov.ua/uk/posts/what-is-a-vpn-and-how-to-use-it-safely. [in Ukrainian]

4. President of Ukraine. (2021). Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 14 travnia 2021 roku «Pro Stratehiiu kiberbezpeky Ukrainy» : Ukaz Prezydenta Ukrainy vid 26.08.2021 № 447/2021 [On the Decision of the National Security and Defense Council of Ukraine of May 14, 2021 «On the Cybersecurity Strategy of Ukraine» : Decree of the President of Ukraine dated August 26, 2021 No. 447/2021]. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text. [in Ukrainian]

5. Computer Emergency Response Team of Ukraine (CERT-UA). Ofitsiinyi sait [Official website]. URL: https://cert.gov.ua. [in Ukrainian]

6. Cyberset. Bekdor : yak khakery lamaiut systemy [Backdoor : how hackers break systems]. URL: https://cyberset.com.ua/vulnerabilities/backdoors. [in Ukrainian]

7. JSC «IIT». Zasib kryptohrafichnoho zakhystu informatsii «Shyfr-X.509» : opys produktu [Cryptographic information protection tool «Cipher-X.509» : product description]. URL: https://cipher.com.ua/uk/products/x509. [in Ukrainian]

8. State Service of Special Communications and Information Protection of Ukraine. Dyrektyva YeS NIS2 : shcho tse take, dlia yakykh potreb rozroblena ta dlia choho Ukraina yii implementuie [EU NIS2 Directive : what it is, why it was developed and why Ukraine implements it]. URL: https://cip.gov.ua/ua/news/direktiva-yes-nis2-sho-ce-take-dlya-yakikh-potreb-rozroblena-ta-dlya-chogo-ukrayina-yiyi-implementuye. [in Ukrainian]

9. Artificial Intelligence Act Explorer (EU AI Act). URL: https://artificialintelligenceact.eu/ai-act-explorer. [in English]

10. State Service of Special Communications and Information Protection of Ukraine. Uriad lehalizuvav Bug Bounty dlia derzhavnykh system [Government legalized Bug Bounty for state systems]. URL: https://cip.gov.ua/ua/news/uryad-legalizuvav-bug-bounty-dlya-derzhavnikh-sistem. [in Ukrainian]

Дата першого надходження статті до видання: 17.03.2026
Дата прийняття статті до друку після рецензування: 27.04.2026
Дата публікації (оприлюднення) статті: 29.05.2026