УДК 351:327+35.071

Остап'як Василь Іванович
доктор політичних наук, доцент,
професор кафедри публічного управління та адміністрування
Івано-Франківський національний технічний університет нафти і газу
Ostapiak Vasyl
Doctor of Political Science, Associate Professor,
Professor of the Department of Public Administration and Management
Ivano-Frankivsk National Technical University of Oil and Gas
ORCID: 0000-0001-9374-1956

DOI: 10.25313/2617-572X-2026-3-68-20

КІБЕРБЕЗПЕКА ТА ЦИФРОВЕ ВРЯДУВАННЯ В ДІЯЛЬНОСТІ ОРГАНІВ МІСЦЕВОГО САМОВРЯДУВАННЯ

CYBERSECURITY AND DIGITAL GOVERNANCE IN THE ACTIVITIES OF LOCAL GOVERNMENTS

Анотація. *Вступ. У статті розглянуто трансформацію кібербезпеки з вузькотехнічної категорії у фундаментальний стратегічний чинник стійкості органів місцевого самоврядування (ОМС). В умовах повномасштабної війни та інтенсифікації кібератак на муніципальну інфраструктуру, забезпечення захищеності місцевих інформаційних ресурсів стає критичною умовою збереження довіри мешканців та безперервності надання публічних послуг.*

Метою статті є теоретичне обґрунтування концептуального поля кібербезпеки в системі муніципального управління, аналіз нормативно-правового забезпечення цифрового врядування на місцевому рівні та розроблення комплексної моделі управління кіберризиками в територіальних громадах.

Матеріали та методи. Дослідження ґрунтується на аналізі нормативно-правових актів України, стратегічних документів у сфері цифровізації, звітів CERT-UA та аналітичних матеріалів CCDCOE НАТО. Застосовано методи системного аналізу, етимологічного та семантичного розбору понять, а також метод моделювання для розроблення алгоритмів кіберзахисту ОМС.

Результати. Визначено чотирикомпонентне понятійне поле (кібербезпека, інформаційна безпека, електронне урядування, цифрове врядування), що складає основу сучасного муніципального менеджменту. Доведено, що цифровізація ОМС має двоїстий характер, вимагаючи впровадження кібербезпеки як інституційного «фільтра». Проаналізовано вплив воєнного стану на цифрову стійкість громад та виокремлено ключові вразливості: фінансові обмеження, кадровий дефіцит та технологічний борг. Запропоновано чотирикомпонентну модель управління ризиками (нормативно-інституційний, організаційний, технічний та кадровий блоки), яка передбачає інтеграцію принципів security by design у муніципальні процеси та впровадження ролі CDTO/CISO на місцевому рівні.

Перспективи. Подальші дослідження доцільно спрямувати на вивчення механізмів міжмуніципального співробітництва у сфері кіберзахисту (спільні SIEM-системи), розроблення моделей фінансової підтримки (субвенцій) для зміцнення кіберстійкості громад та імплементацію вимог Директиви NIS2 у діяльність ОМС.

Ключові слова: *публічне управління, місцеве самоврядування, цифрове врядування, кібербезпека, територіальна громада, кіберстійкість, електронні послуги, воєнний стан, модель CIA, цифрова трансформація.*

Summary. *Introduction. The article examines the transformation of cybersecurity from a narrowly technical category into a fundamental strategic factor in the resilience of local governments (LGs). In the context of a full-scale war and the intensification of cyberattacks on municipal infrastructure, ensuring the security of local information resources becomes a critical condition for maintaining the trust of residents and the continuity of public services.*

The purpose of the article is to theoretically substantiate the conceptual field of cybersecurity in the municipal government system, analyze the regulatory and legal support for digital governance at the local level, and develop a comprehensive model for managing cyber risks in territorial communities.

Materials and methods. The study is based on the analysis of regulatory and legal acts of Ukraine, strategic documents in the field of digitalization, CERT-UA reports, and analytical materials of NATO CCDCOE. The methods of system analysis, etymological and semantic analysis of concepts, as well as the modeling method for developing algorithms for cyber protection of local governments were applied.

Results. A four-component conceptual field was defined (cybersecurity, information security, e-governance, digital governance), which forms the basis of modern municipal management. It is proven that the digitalization of local governments has a dual nature, requiring the implementation of cybersecurity as an institutional "filter". The impact of martial law on the digital resilience of communities was analyzed and key vulnerabilities were identified: financial constraints, personnel shortage and technological debt. A four-component risk management model (normative-institutional, organizational, technical and personnel blocks) was proposed, which involves the integration of security by design principles into municipal processes and the implementation of the role of CDTO/CISO at the local level.

Prospects. Further research should be directed at studying mechanisms for intermunicipal cooperation in the field of cyber defense (joint SIEM systems), developing models of financial support (subsidies) to strengthen the cyber resilience of communities, and implementing the requirements of the NIS2 Directive in the activities of local governments.

Key words: *public administration, local government, digital governance, cybersecurity, territorial community, cyber resilience, electronic services, martial law, CIA model, digital transformation.*

Постановка проблеми. Трансформація публічного управління в Україні в умовах розбудови цифрового суспільства супроводжується інтенсивним впровадженням інструментів цифрового врядування на рівні територіальних громад. Органи місцевого самоврядування (ОМС) дедалі ширше використовують електронні реєстри, хмарні сервіси та платформи взаємодії з громадянами, що суттєво підвищує оперативність прийняття рішень та доступність адміністративних послуг. Водночас розширення муніципальної цифрової інфраструктури неминуче призводить до зростання залежності життєдіяльності громад від стабільності та надійності інформаційно-комунікаційних систем. В умовах воєнного стану, коли кібератаки стають інструментом гібридної агресії та спрямовані на дестабілізацію систем життєзабезпечення, питання кібербезпеки ОМС переходить із площини суто технічного супроводу до сфери стратегічної національної безпеки. За відсутності належного рівня захисту цифрові інструменти можуть стати джерелом критичних управлінських ризиків, що зумовлює необхідність наукового переосмислення кібербезпеки як інтегрального компонента цифрового врядування на місцевому рівні.

Аналіз останніх досліджень і публікацій. Теоретичні та прикладні аспекти кібербезпеки у публічному секторі перебувають у центрі уваги багатьох науковців. Етимологія та еволюція поняття «кібербезпека» від праць Н. Вінера до сучасних словникових визначень проаналізовані в лінгвістичних та академічних студіях [1; 2]. У працях І. Крикавської [3] та А. Вовка [4] ґрунтовно досліджено нормативне забезпечення цифровізації та сучасні проблеми управління кібербезпекою в Україні, зокрема акцентовано на кумулятивному руйнівному ефекті вразливостей муніципальних систем для держави. Правову основу цього процесу формує пакет законів щодо основ кібербезпеки, захисту інформації в системах, персональних даних та електронних довірчих послуг [5; 6; 7; 8]. Інституційна архітектура управління цифровим розвитком та координація суб'єктів кіберзахисту, включаючи роль Мінцифри та НКЦК, розкривається через аналіз урядових постанов та спеціальних законодавчих норм [9; 10]. Міжнародний досвід та інструменти оцінювання цифрової зрілості представлені у звітах CCDCOE НАТО та показниках Індексу цифрової трансформації регіонів [11]. Практичні виклики, пов'язані зі зростанням кількості кіберінцидентів та атаками на державні органи в умовах війни, зафіксовані в аналітиці CERT-UA та профільних медіа [12; 13]. Потенційний масштаб збитків від компрометації муніципальних мереж підтверджується міжнародними кейсами Атланти та Балтимора [14; 15]. Разом із тим, попри значний масив напрацювань, питання формування цілісної управлінської моделі кіберзахисту територіальних громад в умовах кризового функціонування потребує подальшої деталізації.

Метою статті є теоретичне обґрунтування концептуального поля кібербезпеки в системі муніципального управління, аналіз нормативно-правового та інституційного забезпечення цифрового врядування на рівні органів місцевого самоврядування, а також розроблення комплексної чотирикомпонентної моделі управління кіберризиками для зміцнення цифрової стійкості територіальних громад.

Виклад основного матеріалу. Поняття кібербезпеки, що сформувалося на базі дискурсу інформатичних і кібернетичних наук середини XX століття, сьогодні набуває особливого стратегічного значення саме в контексті діяльності органів місцевого самоврядування. Основою для сучасних термінів виступила кібернетика — міждисциплінарна наука про системи керування, започаткована наприкінці 1940-х років у працях Норберта Вінера. Сам термін

«cybernetics», що походить від грецького «керманич», семантично пов'язаний з управлінням і контролем, що ідеально відображає сутність владних повноважень на місцях. Етимологічний розвиток цього поняття, детально описаний у лінгвістичних дослідженнях [1], вказує на еволюцію від загального управління системами до концепції всеосяжного захисту муніципальних цифрових інфраструктур.

Словник Merriam-Webster фіксує перший відомий вжиток англійського слова «cybersecurity» у 1989 році в значенні захисту цифрових систем [2], що нині є критичною базовою вимогою для функціонування будь-якої територіальної громади. У прикладному вимірі муніципальну кібербезпеку доцільно характеризувати як сукупність цілеспрямованих безпекових заходів, орієнтованих на забезпечення захищеності комп'ютерних мереж рад, локальних баз даних та комунальних інформаційних систем. Концептуалізація безпеки традиційно здійснюється через модель CIA-тріади: конфіденційність (захист персональних даних мешканців громади), цілісність (недоторканність місцевих реєстрів і рішень виконавчих комітетів) та доступність (безперебійна робота муніципальних електронних сервісів). Ця модель слугує фундаментальною основою для розроблення місцевих політик кібербезпеки та стратегій захисту критичної цифрової інфраструктури громад.

У дослідженні І. Крикавської [3] аналізується семантичний зміст термінів «digitalization», «cybersecurity» та «e-government» із доведенням того, що цифровізація місцевого публічного управління має двоїстий характер. З одного боку, вона створює безпрецедентні можливості для підвищення якості муніципальних послуг та прозорості місцевих бюджетів, а з іншого — неминуче породжує потребу в значно жорсткіших вимогах до захисту конфіденційної інформації громадян. Авторка наголошує, що кібербезпека у місцевому публічному секторі фактично набуває статусу ключового інституційного «фільтра», через який мають проходити абсолютно всі цифрові трансформації на рівні територіальних громад.

Понятійне поле, релевантне аналізу кібербезпеки у цифровому врядуванні органів місцевого самоврядування, охоплює чотири взаємопов'язані категорії, які слід розглядати в єдиному комплексі. Першою категорією є безпосередньо кібербезпека як система інженерних та управлінських заходів і політик захисту муніципальної цифрової інфраструктури та даних у публічному секторі громади. Другою виступає інформаційна безпека як значно ширша нормативна рамка, що регламентує режими доступу, зберігання й обробки місцевої інформації, зокрема документації рад поза межами кіберпростору. Третьою категорією є електронне урядування, що являє собою інструментальні форми застосування ІКТ у діяльності органів місцевого самоврядування для підвищення підзвітності влади та оптимізації адміністративних послуг через ЦНАП. Четвертою категорією визнається цифрове врядування як всеосяжна сучасна модель організації управлінських процесів у громадах, що включає інструменти місцевої електронної демократії, цифрову участь мешканців, просторову аналітику та інші концепції рівня «Smart City».

У працях А. Вовка кібербезпека описується як стрижневий напрям модернізації публічного управління, що нерозривно пов'язує центральні органи влади, сектор безпеки й оборони та органи місцевого самоврядування [4]. Автор особливо акцентує на тому, що вразливість муніципальних інформаційних систем здатна мати кумулятивний руйнівний ефект для загальнодержавної безпеки. Це пояснюється тим, що компрометація баз даних місцевих рад часто призводить до масового витоку персональної інформації громадян, несанкціонованого втручання в системи життєзабезпечення населених пунктів та загального порушення стійкості управління на базовому рівні.

Нормативна основа кібербезпеки у сфері муніципального управління формується на перетині інформаційного, адміністративного права та загальнонаціональної політики цифрової трансформації. Базовим актом виступає Закон України «Про основні засади забезпечення кібербезпеки України» [5], у якому органи місцевого самоврядування прямо й недвозначно віднесені до суб'єктів забезпечення кібербезпеки поряд із державними структурами.

Таблиця 1

Основні категорії цифрового середовища територіальних громад

Категорія	Сутність та характер заходів	Об'єкт та фокус діяльності
Кібербезпека	Система інженерних та управлінських заходів, технічні політики захисту.	Муніципальна цифрова інфраструктура, мережі рад та дані в публічному секторі громади.
Інформаційна безпека	Широка нормативна рамка, що регламентує режими доступу та обробки даних.	Місцева інформація в цілому, включаючи документацію рад поза межами кіберпростору.
Електронне урядування	Інструментальні форми застосування ІКТ (інформаційно-комунікаційних технологій).	Оптимізація адміністративних послуг через ЦНАП, підвищення підзвітності влади.
Цифрове врядування	Всеосяжна модель організації управлінських процесів та взаємодії.	Електронна демократія, цифрова участь мешканців, просторова аналітика та концепція «Smart City».

Джерело: авторська розробка

Відповідно до закону, посадові особи місцевого самоврядування несуть відповідальність за захищеність життєво важливих інтересів своєї громади в кіберпросторі, що вимагає імплементації цих норм у регламенти рад та посадові інструкції службовців.

Функціонування інформаційно-комунікаційних систем органів місцевого самоврядування додатково регулюється масивом актів, до якого належать закони України «Про захист інформації в інформаційно-телекомунікаційних системах» [6], «Про захист персональних даних» [7] та «Про електронну ідентифікацію та електронні довірчі послуги» [8]. Разом із підзаконними актами Уряду ці документи встановлюють жорсткі вимоги до кіберзахисту комунальних об'єктів критичної інфраструктури. У межах цього нормативного поля ОМС зобов'язані організовувати надійний захист власних апаратних комплексів, локальних електронних реєстрів (зокрема реєстрів територіальних громад), муніципальних вебпорталів та каналів комунікації.

Розвиток місцевого цифрового врядування базується на комплексі загальнодержавних стратегічних рішень. Стратегія розвитку інформаційного суспільства в Україні визначила довгострокові орієнтири для впровадження електронного урядування та цифрової партисипації на місцевому рівні. Подальші секторальні документи, такі як Стратегія цифрової трансформації соціальної сфери та Стратегія у сфері управління державними фінансами, сформували прямі вимоги до місцевих рад щодо забезпечення кіберзахисту інформаційних ресурсів під час цифровізації соціальних послуг населенню та електронного управління місцевими бюджетами.

Процес інституціоналізації цифрового врядування в Україні отримав системний характер із заснуванням Міністерства цифрової трансформації на підставі постанови КМУ № 856, що закріпило за відомством роль ключового суб'єкта формування політики електронного урядування та цифрового розвитку [9]. Для органів місцевого самоврядування (ОМС) це рішення визначило чіткий вектор цифровізації муніципальних сервісів. Водночас Закон України «Про основні засади забезпечення кібербезпеки України» включив ОМС до переліку суб'єктів національної системи кібербезпеки, поклавши на них відповідальність за захист місцевих інформаційних ресурсів. У цій архітектурі стратегічну координацію здійснює НКЦК при РНБО, тоді як Держспецзв'язку та Мінцифра виконують регуляторні та методичні функції у сфері захисту даних [10].

Аналітичні звіти НАТО (CCDCOE) підтверджують формування потужної державної інфраструктури, що включає CERT-UA та Національний центр резервування даних. Така технологічна база створює необхідний «фон безпеки» для територіальних громад, які інтегрують свої локальні системи з державними реєстрами. Протягом останнього десятиліття цифрові технології трансформували модель діяльності ОМС: впровадження онлайн-кабінетів мешканців, геоінформаційних систем та автоматизованих реєстрів змінило логіку комунікації влади й громади. Перехід до дистанційних управлінських процедур підвищує прозорість, проте вимагає від муніципалітетів нових підходів до забезпечення безперервності надання послуг і захисту персональних даних у разі кіберінцидентів.

Центральне місце у цифровій екосистемі громад посідає вебпортал «Дія», навколо якого консолідуються сервіси соціального захисту («Соціальна громада», «єДопомога») та інструменти електронної демократії (петиції, громадські бюджети). Навіть у гірських та віддалених районах ОМС впроваджують цифрові черги до ЦНАП та мобільні застосунки для оперативного зв'язку з населенням. Рівень цієї трансформації відображає Індекс цифрової трансформації регіонів, де станом на 2023 рік середній показник по країні становив 0,632, хоча лідери (Дніпропетровська, Львівська області) вже наближаються до 0,9, демонструючи високу цифрову зрілість локальних органів влади [11]. Повномасштабна війна критично актуалізувала питання стійкості цих систем. Постійні атаки на енергомережі та зв'язок безпосередньо загрожують доступності електронних послуг у громадах. Досвід 2022 року, коли дефейсинг урядових сайтів тимчасово обмежив роботу сервісів «Дії», став сигналом для ОМС щодо необхідності зміцнення власних цифрових контурів [12]. Статистика свідчить про зростання кіберзагроз: у 2023 році CERT-UA зафіксувала 2543 інциденти (ріст на 15,9%), де значна частка атак була спрямована саме на місцеві органи влади [13]. Міжнародні приклади, як-от атаки на Атланту (2018) та Балтимор (2019), де блокування муніципальних систем призвело до збитків у мільйони доларів і переходу на паперовий документообіг, демонструють потенційний масштаб загрози для українських міст [14; 15].

Висновки і перспективи подальших досліджень. Проведене дослідження дозволяє констатувати, що цифровізація діяльності органів місцевого самоврядування в Україні остаточно перейшла з етапу фрагментарного впровадження окремих ІТ-рішень до фази системної інституційної трансформації муніципального управління. Узагальнення теоретичних засад та аналіз практичного досвіду свідчать, що кібербезпека перестала бути виключно технічною категорією, набувши статусу фундаментальної умови життєздатності територіальних громад в умовах глобальних гібридних загроз та повномасштабної збройної агресії. Сформована в Україні нормативно-правова база, що спирається на профільне законодавство про кібербезпеку та діяльність Міністерства цифрової трансформації, створює необхідний контур для розбудови цифрового врядування, проте вона вимагає подальшої адаптації до специфічних ресурсних можливостей місцевого рівня. Головним висновком роботи є доведення необхідності переходу до комплексної ризик-орієнтованої моделі управління, яка інтегрує принципи захищеності на всіх

етапах життєвого циклу муніципальних сервісів. Запропонована чотирикомпонентна структура, що охоплює нормативно-інституційний, організаційний, технічний та соціально-кадровий блоки, дозволяє громадам еволюційно нарощувати рівень своєї кіберстійності залежно від їхньої цифрової зрілості. Особливої ваги набуває посилення ролі CDTO у структурі місцевих рад та систематичне підвищення рівня кібергігієни персоналу, оскільки людський фактор залишається найбільш критичним вектором потенційних атак. Перспективи подальших наукових розвідок у цьому напрямі вбачаються у детальному вивченні механізмів міжмуніципального співробітництва для створення спільних центрів кіберзахисту, що дозволить оптимізувати видатки місцевих бюджетів та забезпечити фаховий моніторинг загроз. Актуальним залишається розроблення прикладного інструментарію для оцінювання ризиків у системах управління комунальною інфраструктурою, а також дослідження безпекових аспектів застосування штучного інтелекту в муніципальній аналітиці. Окремого вивчення потребує процес імплементації положень Директиви NIS2 у вітчизняне законодавство, що сприятиме гармонізації українських практик із європейськими стандартами. Подальші дослідження мають також фокусуватися на розробленні ефективних фінансових моделей підтримки кіберстійкості громад через механізми цільових державних субвенцій, що забезпечить сталість цифрових трансформацій та безпеку мешканців у довгостроковій перспективі.

ДОДАТКОВА ІНФОРМАЦІЯ

ФІНАНСУВАННЯ: Автори не отримували фінансування для цього дослідження.
ЗАЯВА ПРО ДОСТУПНІСТЬ ДАНИХ: Не застосовується.
КОНФЛІКТ ІНТЕРЕСІВ: Автори заявляють про відсутність конфлікту інтересів.

Література

1. Where does the word cyber come from?.URL: https://blog.oup.com/2015/03/cyber-word-origins/ (дата звернення: 07.02.2026).

2. Definition of CYBERSECURITY. *Merriam-Webster: America's Most Trusted Dictionary*. URL: https://www.merriam-webster.com/dictionary/cybersecurity (дата звернення: 06.02.2026).

3. Kryvakska I. Regulatory and institutional support of digitalization and cybersecurity of the public administration system in the EU. *Вісник Національного університету «Львівська політехніка». Серія: Юридичні науки.* 2023. № 1 (37). С. 148–154

4. Вовк А. Сучасні проблеми публічного управління забезпеченням кібербезпеки в Україні. *Публічне управління: концепції, парадигма, розвиток, удосконалення*. 2024. № 8. С. 28–35.

5. Про основні засади забезпечення кібербезпеки України. *Офіційний вебпортал парламенту України*.URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 02.02.2026).

6. Про захист інформації в інформаційно-комунікаційних системах. *Офіційний вебпортал парламенту України*. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text (дата звернення: 28.02.2026).

7. Про захист персональних даних. *Офіційний вебпортал парламенту України*. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 28.02.2026).

8. Про електронну ідентифікацію та електронні довірчі послуги. *Офіційний вебпортал парламенту України*. URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text (дата звернення: 22.02.2026).

9. Питання Міністерства цифрової трансформації. *Офіційний вебпортал парламенту України*. URL: https://zakon.rada.gov.ua/laws/show/856-2019-п#Text (дата звернення: 25.02.2026).

10. Про основні засади забезпечення кібербезпеки України. *Офіційний вебпортал парламенту України*. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 07.02.2026).

11. National Cybersecurity Governance: UKRAINE. URL: https://ccdcoe.org/uploads/2024/08/NationalCybersecurityGovernance_Ukraine_Davydiuk_Potii_2024.pdf (дата звернення: 06.02.2026).

12. Економічна правда. Кількість кібератак у 2023 році зросла на 16% — Держспецзв'язку. *Економічна правда*. URL: https://epravda.com.ua/news/2024/01/31/709355/ (дата звернення: 03.02.2026).

13. Від кібератаки 14 січня постраждали 22 державних органи, — Держспецзв'язку. *Урядовий портал*. URL: https://www.kmu.gov.ua/news/vid-kiberataki-14-sichnya-postrazhdali-22-derzhavnih-organi-derzhspeczvyazku (дата звернення: 28.02.2026).

14. Atlanta Ransomware Case Study. c*Free Antivirus i VPN*. URL: https://www.avast.ua/business/resources/atlanta-ransomware#mac (дата звернення: 03.02.2026).

15. The Baltimore Ransomware Attack: A Look Back. *N2W Software*. URL: https://n2ws.com/blog/aws-disaster-recovery/baltimore-ransomware-attack (дата звернення: 03.02.2026).

References

1. Oxford University Press. (2015). *Where does the word cyber come from?* [Where does the word cyber come from?]. Retrieved from https://blog.oup.com/2015/03/cyber-word-origins/

2. Merriam-Webster. (n.d.). *Definition of cybersecurity* [Definition of cybersecurity]. Retrieved from https://www.merriam-webster.com/dictionary/cybersecurity

3. Kryvakska, I. (2023). Rehuliatorne ta instytutsiine zabezpechennia tsyfrovizatsii ta kiberbezpeky systemy publichnoho upravlinnia v YeS [Regulatory and institutional support of digitalization and cybersecurity of the public administration system in the EU]. *Visnyk Natsionalnoho universytetu "Lvivska politekhnika". Seriia: Yurydychni nauky*, 1 (37), 148–154. [in Ukrainian].

4. Vovk, A. (2024). Suchasni problemy publichnoho upravlinnia zabezpechenniam kiberbezpeky v Ukraini [Modern problems of public administration in ensuring cybersecurity in Ukraine]. *Publichne upravlinnia: kontseptsii, paradyhma, rozvytok, udoskonalennia*, 8, 28–35. [in Ukrainian].

5. Verkhovna Rada of Ukraine. (n.d.). Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy [On the basic principles of ensuring cybersecurity of Ukraine]. Retrieved from https://zakon.rada.gov.ua/laws/show/2163-19#Text [in Ukrainian].

6. Verkhovna Rada of Ukraine. (n.d.). Pro zakhyst informatsii v informatsiino-komunikatsiinykh systemakh [On the protection of information in information and communication systems]. Retrieved from https://zakon.rada.gov.ua/laws/show/80/94-вр#Text [in Ukrainian].

7. Verkhovna Rada of Ukraine. (n.d.). Pro zakhyst personalnykh danykh [On personal data protection]. Retrieved from https://zakon.rada.gov.ua/laws/show/2297-17#Text [in Ukrainian].

8. Verkhovna Rada of Ukraine. (n.d.). Pro elektronnu identyfikatsiiu ta elektronni dovirchi posluhy [On electronic identification and electronic trust services]. Retrieved from https://zakon.rada.gov.ua/laws/show/2155-19#Text [in Ukrainian].

9. Cabinet of Ministers of Ukraine. (2019). Pytannia Ministerstva tsyfrovoi transformatsii [Issues of the Ministry of Digital Transformation]. Retrieved from https://zakon.rada.gov.ua/laws/show/856-2019-п#Text [in Ukrainian].

10. Verkhovna Rada of Ukraine. (n.d.). Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy [On the basic principles of ensuring cybersecurity of Ukraine]. Retrieved from https://zakon.rada.gov.ua/laws/show/2163-19#Text [in Ukrainian].

11. National Cybersecurity Governance: UKRAINE. Retrieved from https://ccdcoe.org/uploads/2024/08/NationalCybersecurityGovernance_Ukraine_Davydiuk_Potii_2024.pdf

12. Ekonomichna pravda. (2024). Kilkist kiberatak u 2023 rotsi zrosla na 16% — Derzhspetszviazku [The number of cyberattacks increased by 16% in 2023 — State Service of Special Communications]. Retrieved from https://epravda.com.ua/news/2024/01/31/709355/ [in Ukrainian].

13. Uriadovyi portal. (2022). Vid kiberataky 14 sichnia postrazhdaly 22 derzhavnykh orhany — Derzhspetszviazku [22 state authorities affected by the cyberattack of January 14 — State Service of Special Communications]. Retrieved from https://www.kmu.gov.ua/news/vid-kiberataki-14-sichnya-postrazhdali-22-derzhavnih-organi-derzhspeczvyazku [in Ukrainian].

14. Avast. (n.d.). *Atlanta ransomware case study* [Atlanta ransomware case study]. Retrieved from https://www.avast.ua/business/resources/atlanta-ransomware#mac

15. N2W Software. (n.d.). *The Baltimore ransomware attack: A look back* [The Baltimore ransomware attack: A look back]. Retrieved from https://n2ws.com/blog/aws-disaster-recovery/baltimore-ransomware-attack

Дата першого надходження статті до видання: 02.03.2026
Дата прийняття статті до друку після рецензування: 28.03.2026
Дата публікації: 31.03.2026