УДК 35.07:004.056:355.02

**Гончарук Юрій Володимирович**
*здобувач освітньо-наукової програми доктора*
*філософії за спеціальністю «Публічне управління та адміністрування»*
*кафедри публічного управління та адміністрування*
*Національного лісотехнічного університету України*
**Honcharuk Yurii**
*Postgraduate Student of the educational and scientific program of*
*Doctor of Philosophy in the specialty «Public Administration and Management»*
*Department of Public Administration and Management of*
*Ukrainian National Forestry University*
ORCID: 0009-0000-0314-1579

DOI: 10.25313/2617-572X-2026-2-11927

# ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В ПУБЛІЧНОМУ УПРАВЛІННІ: ВИКЛИКИ ТА ЗАГРОЗИ ВОЄННОГО ЧАСУ

# CYBERSECURITY PROVISION IN PUBLIC ADMINISTRATION: WARTIME CHALLENGES AND THREATS

***Анотація.*** *Вступ. Стаття присвячена дослідженню проблеми забезпечення кібербезпеки органів публічного управління в умовах повномасштабної агресії Росії. Успішне функціонування державних інституцій, захист національної безпеки та суспільної довіри залежать від рівня їхньої кіберстійкості. Ефективне реагування на кіберінциденти – це складний процес, що вимагає серйозного планування, ресурсів та формування безпечного віртуального середовища. У сучасну цифрову епоху публічне управління стикається з дедалі витонченішими кіберзлочинами, включаючи DDoS-атаки, експлуатацію відомих вразливостей (CVE), шкідливе програмне забезпечення та фішингові кампанії, які є серйозною загрозою. Актуальність дослідження посилюється зростанням кількості та складності кібератак, спрямованих проти органів державного управління, критичної інфраструктури та підприємств, важливих для функціонування економіки України, починаюся з 2022 року. Особливу увагу приділено появі нових типів загроз, таких як атаки на ланцюги постачання програмного забезпечення та «петлеві атаки» («Loop DoS Attack»), що впливають на традиційні методи захисту.*

*Мета. Метою статті є дослідження проблем, які виникають у сфері публічного управління, пов'язаних з кібербезпекою, в умовах повномасштабного вторгнення Росії, здійснення аналізу ефективності роботи системи виявлення вразливостей та реагування на кіберінциденти, а також визначення шляхів підвищення кіберстійкості та вдосконалення механізмів захисту.*

*Матеріали і методи. Дослідження ґрунтується на аналізі законодавчих та нормативно-правових актів України та Європейського Союзу, з особливим акцентом на діяльність Агентства Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA), що є важливим для адаптації національного законодавства. Використовувалися наукові праці вітчизняних та зарубіжних учених, а також емпіричні дані – статистичні звіти Державної служби спеціального зв'язку та захисту інформації України (Держспецзв'язку) кіберінцидентів. В процесі роботи застосовувалися методи теоретичного узагальнення, групування, порівняльного аналізу (зокрема, оцінка позиції України в Національному індексі кібербезпеки (NCSI)), а також метод систематизації для розробки системи оцінки ризиків та ідентифікаторів кіберзагроз.*

*Результати. Проведений аналіз засвідчив, що кібербезпека набуває першочергового значення в системі національної безпеки в контексті публічного управління. Статистичні дані Держспецзв'язку чітко демонструють прогресуючий тренд на зростання кількості кіберінцидентів, що свідчить про постійне розширення кібервійни. Основними цілями атак залишаються органи влади, критична інфраструктура та підприємства, важливі для функціонування економіки України.*

*У статті систематизовано основні види кіберзагроз та визначено їхні ідентифікатори (мережеві, файлові, системні, поведінкові, експлуатації вразливостей), які вимагають високої кваліфікації фахівців. Також виявлено низку системних проблем: недостатня інтеграція сучасних систем захисту; брак кваліфікованих фахівців з кібербезпеки; а також нехтування кіберризиками з боку вищого керівництва, яке має нести відповідальність за кіберзахист. Підкреслено, що для зниження ризиків необхідне збільшення інвестицій у кіберзахист.*

*Перспективи. Необхідність підвищення рівня кіберстійкості безпосередньо залежить від формування міцної культури кібербезпеки. Подальші дослідження мають бути спрямовані на розробку конкретних методологічних підходів до впровадження міжнародних стандартів кібербезпеки та кращих практик (ISO 27001, SOC2, NIST CSF) при проведенні аудиту та огляду стану кіберзахисту в органах публічного управління України. Реалізація цих заходів є критичною для побудови ефективних планів вдосконалення кіберзахисту.*

***Ключові слова:*** *публічне управління, кібербезпека, кіберінцидент, кібератака, Держспецзв'язок, критична інфраструктура, Національний індекс кібербезпеки (NCSI), інформаційна безпека, оцінка ризиків.*

***Summary.*** *Introduction. The article is devoted to researching the critical issue of ensuring cybersecurity in public administration bodies under the conditions of Russia's full-scale aggression. The successful functioning of state institutions, the protection of national security, and public trust depend on the level of their cyber resilience. Effective response to cyber incidents is a complex process that requires serious planning, resources, and the formation of a secure virtual environment. In the modern digital era, public administration faces increasingly sophisticated cybercrimes, including DDoS attacks, exploitation of known vulnerabilities (CVE), malware, and phishing campaigns, which pose a serious threat. The relevance of the research is amplified by the growing number and complexity of cyberattacks, targeting public administration bodies, critical infrastructure, and enterprises vital for the functioning of Ukraine's economy, starting from 2022. Special attention is given to the emergence of new types of threats, such as supply chain attacks and "Loop DoS Attacks", which impact traditional protection methods.*

*Objective. The objective of the article is to study the problems arising in the sphere of public administration related to cybersecurity under the conditions of Russia's full-scale invasion, to analyze the effectiveness of the system for vulnerability detection and cyber incident response, and to determine ways to enhance cyber resilience and improve protection mechanisms.*

*Materials and Methods. The research is based on the analysis of legislative and regulatory acts of Ukraine and the European Union, with a particular focus on the activities of the European Union Agency for Cybersecurity (ENISA), which is important for adapting national legislation. Scientific works of both domestic and foreign scholars were utilized, as well as empirical data from the statistical reports of the State Service of Special Communications and Information Protection of Ukraine (SSSCIP) regarding cyber incidents. The methods of theoretical generalization, grouping, comparative analysis (specifically, assessing Ukraine's position in the National Cyber Security Index (NCSI)), and the method of systematization for developing a risk assessment system and cyber threat indicators were applied during the work.*

*Results. The conducted analysis has shown that cybersecurity is gaining paramount importance in the national security system within the context of public administration. SSSCIP statistical data clearly demonstrate a progressing trend towards an increase in the number of cyber incidents, indicating the constant expansion of cyber warfare. The main targets of attacks remain government bodies, critical infrastructure, and enterprises essential for the functioning of Ukraine's economy. The article systematizes the main types of cyber threats and defines their indicators (network, file, system, behavioral, and vulnerability exploitation), which require high specialist qualification. A number of systemic problems were also identified: insufficient integration of modern protection systems; a shortage of qualified cybersecurity specialists; and the neglect of cyber risks by senior management, who should bear responsibility for cyber defense. It is emphasized that increasing investment in cyber defense is necessary to mitigate risks.*

*Prospects. The necessity of increasing the level of cyber resilience directly depends on the formation of a strong cybersecurity culture. Further research should be aimed at developing specific methodological approaches for the implementation of international cybersecurity standards and best practices (ISO 27001, SOC2, NIST CSF) when conducting audits and reviewing the state of cyber protection in Ukrainian public administration bodies. The implementation of these measures is critical for building effective plans to improve cyber defense.*

***Key words:*** *public administration, cybersecurity, cyber incident, cyber-attack, SSSCIP, critical infrastructure, National Cyber Security Index (NCSI), information security, risk assessment.*

**Постановка проблеми.** Ефективне реагування на кіберінциденти — це складний процес створення успішного потенціалу реагування та вимагає значного планування й ресурсів. Це допомагає органам публічного управління адекватно та вчасно реагувати на такі інциденти, а також ефективному та результативному управлінні ними.

Захист інформаційної незалежності, забезпечення ефективного функціонування системи обміну даних є актуальним завданням органів публічного управління у сфері кібербезпеки.

Органи публічного управління зобов'язані надійно захищати свої активи та операції, включаючи IT-інфраструктуру та інформацію.

У сучасну цифрову епоху публічне управління стикається з дедалі серйознішими викликами у сфері кібербезпеки. Кіберзлочини проти державних установ набувають все більш витончених форм і стають сер-

йозною загрозою для національної безпеки, суспільної довіри та ефективності державного управління.

У державних установ дедалі частіше виникають проблеми, пов'язані з різноманітними видами кібератак. Це відбувається при наданні електронних послуг, блокуванні роботи державних органів, фішингових атаках електронною поштою та соціальними мережами, порушенні конфіденційності даних, блокуванні роботи або руйнуванні стратегічно важливих для держави підприємств.

**Аналіз останніх досліджень і публікацій.** Наукові дослідження свідчать, що найбільш поширеними формами кіберзлочинів у сфері публічного управління є: несанкціонований доступ до інформаційних систем, атаки типу DDoS (Distributed Denial of Service — розподілена відмова в обслуговуванні), шкідливе програмне забезпечення (malware), фішинг, маніпуляції з даними та крадіжка персональних даних громадян.

Державні інституції є вразливими до цілеспрямованих атак. У публікаціях міжнародних організацій, таких як OECD та ENISA, підкреслюється потреба у зміцненні кібергігієни, підвищенні обізнаності працівників публічного управління, а також у створенні централізованих стратегій кіберзахисту.

Вагомий внесок у розробку теоретичних основ та методологічних підходів до проблеми кібербезпеки зробили провідні вчені. Так Метью Едвардс та Емма Вільямс у дослідженні «Характеристика кіберзлочинів: ревю» [1] роблять огляд характеристик та мотивації правопорушників, які беруть участь у кіберзалежних злочинах. Марія Бада і Джейсон Р. С. [2] звертають увагу на психологічний вплив кібератак. Крім того, в літературі розглядається питання взаємодії державних установ із приватним сектором у контексті обміну даними про загрози та співпраці у розробці захисних технологій. Джулія Наполітано вказує на важливість формування культури кібербезпеки як елемента публічного управління [3]. Вона акцентує увагу на тому, що керівники органів публічного управління нехтують кіберризиками, а також існує постійна невизначеність щодо того, хто несе відповідальність за кібербезпеку в організації (в ідеалі відповідальність мають нести керівники вищої ланки) [3].

Українські дослідники такі як Кулешов М. [4] акцентують увагу на недостатній інтеграції сучасних систем кіберзахисту в органах публічного управління, відсутності достатньо ефективного реагування на інциденти, а також брак висококваліфікованих фахівців з кібербезпеки. Ковальова А. разом зі співавторами [5] розглядають особливості розслідування та відповідальності за кіберзлочини у збройному конфлікті. Колесніков А, Зяйлик М. [6] аналізують передумови та методи боротьби з кіберзлочинністю в Україні. Зокрема, у їхніх працях підкреслюється потреба адаптації українського законодавства до вимог ЄС у сфері кіберзлочинності.

Разом з тим необхідність підвищення рівня кібербезпеки в органах публічного управління в умовах повномасштабного вторгнення потребує подальшого дослідження.

**Формулювання цілей статті (постановка завдання)**. Метою статті є дослідження проблем, які виникають у сфері публічного управління, пов'язаних з кібербезпекою, в умовах повномасштабного вторгнення. Для досягнення поставленої мети було визначено такі завдання:

- здійснити аналіз теоретичних основ та методологічних підходів до проблеми кібербезпеки та її місця в системі органів публічного управління;
- розглянути ідентифікатори кіберзагроз щодо забезпечення кібербезпеки;
- визначити підходи до організації та проведення огляду стану кіберзахисту;
- проаналізувати ефективність роботи системи виявлення вразливостей та реагування на кіберінциденти та кібератаки протягом 2022–2024 років.

**Виклад основного матеріалу.** Питання кібербезпеки є важливим як для країн Євросоюзу, так і України. У ЄС у 2004 році було створено Агентство Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA), яке надає практичні рекомендації та інструменти для державного та приватного секторів в країнах-членах ЄС. Діяльність агентства включає сприяння розробці національних стратегій і співробітництву між командами з реагування на надзвичайні ситуації та розбудови потенціалу. ENISA допомагає розробляти політику та законодавство ЄС з питань інформаційної безпеки.

Протягом 2022–2024 роки відбулося суттєве збільшення кількості кібератак та їхньої складності в Україні. Найбільше постраждали державний сектор, фінансова сфера та енергетика. Основними напрямками дій зловмисників є DDoS-атаки й атаки на критичну інфраструктуру, експлуатація відомих вразливостей інформаційних систем (CVE), фішингові кампанії тощо. Економічні втрати через кібератаки є значними і включають витрати на відновлення, та втрату репутації організацій.

Із появою штучного інтелекту використовують нові типи атак на ланцюги постачання програмного забезпечення, «петлеві атаки» («Loop DoS Attack») на 7-му рівні тощо. Все це впливає на традиційні методи захисту інформації. «Петлеву атаку» складно зупинити, навіть, після введення тригеру, вона націлена на протоколи прикладного рівня. Така атака об'єднує дві мережеві служби і створює великі обсяги трафіку, що призводить до відмови обслуговування залучених систем.

Сучасний розвиток цифрових технологій, відносно низька вартість обчислювальної потужності, доступність даних (Big Data) забезпечують інноваційні продукти та технології в публічному управлінні.

Зростання кібератак характеризуються все новими загрозами, тому органам публічного управління потрібно збільшувати свої інвестиції для зниження

ризиків. В таблиці 1 представлено систему оцінку ризиків кібербезпеки.

Дуже важливим є розвиток високої культури кібербезпеки на рівні держави, адже органи державного управління та бізнес можуть по-різному бачити ризики кібербезпеки. Деякі організації взагалі можуть ними нехтувати. Головними інструментами держави тут є нормативно-правові вимоги щодо мінімального рівня захисту від кіберзагроз та призначення наглядових органів, відповідальних за моніторинг дотримання цих вимог та допомогу організаціям з їх впровадження.

Саме такий підхід працює в країнах ЄС, де головним наглядовим органом є вищезгадана ENISA. Ця агенція розробляє політику в сфері кібербезпеки, створює детальні стандарти та рекомендації щодо впровадження вимог, встановлених законодавством ЄС в цій сфері. Окрім цього, вона здійснює моніторинг та розслідування великих кіберінцидентів та допомагає розробити спільну стратегію відповіді на найбільш поширені кібератаки.

Слід розуміти, що не зважаючи на те, що Європейський Союз намагається побудувати єдиний підхід до управління кібербезпекою, рівень захищеності конкретних країн-членів ЄС є дуже різним та залежить від ряду факторів (рівень розвитку технологічної інфраструктури, фінансових можливостей, впливу бізнесу тощо).

Для вимірювання готовності країн до запобігання кіберзагрозам та управління кіберінцидентами варто розглядати Національний індекс кібербезпеки, який налічує різні показники, що стосуються заходів з розробки політики кібербезпеки, аналізу кіберзагроз, боротьби з кіберзлочинністю та безпеки цифрових послуг.

Національний індекс кібербезпеки (National Cyber Security Index, NCSI) — це показник, який оцінює рівень кібербезпеки країни, вимірюючи її здатність визначати, протистояти та розвиватися у сфері кіберзагроз. Індекс був розроблений Естонською академією електронного управління (e-Governance Academy, eGA). Україна займала 24 місце у 2024 році з показником 75,32, випереджаючи деякі європейські країни, але поступаючись лідерам рейтингу, таким як Греція, Бельгія та Литва. [8]. У 2024 році до лідерів за рейтингом входять: Естонія, Литва, Великобританія, Фінляндія, Ізраїль.

Індекс оцінює спроможність держави у трьох основних сферах:

- Кібербезпека політик і стратегій (наявність національної стратегії, законодавства тощо).
- Оперативна спроможність (компетентні органи, центри реагування на кіберінциденти, кібернавчання тощо).
- Захист цифрових послуг й інфраструктури (захист електронного уряду, критичної інфраструктури, конфіденційності тощо).

Індекс базується на 46 показниках, згрупованих у 12 категорій. Кожна країна отримує кількісну оцінку від 0 до 100 балів. Слід зазначити, що

*Таблиця 1*

**Система оцінки ризиків кібербезпеки**

| Компонентні рамкові заходи управління кібербезпекою | Деталі |
|---|---|
| Схильність до ризику (Risk Appetite) | Це рівень ризику, який організація готова прийняти, щоб досягти своїх цілей. Іншими словами, це визначення, які саме загрози та їх потенційний вплив є прийнятними. |
| Політика інформаційної безпеки (Information Security Policy) | Це набір правил, стандартів і процедур, які регулюють поведінку співробітників та використання інформаційних технологій в організації. Політика встановлює, як саме потрібно захищати інформацію та системи. Вона може включати такі аспекти, як правила використання паролів, доступ до даних, використання особистих пристроїв на роботі (BYOD) тощо. |
| Оцінка та моніторинг ризиків (Risk Assessment and Monitoring) | Це систематичний процес виявлення, аналізу та оцінки кіберзагроз, а також їхнього потенційного впливу на діяльність органів публічного управління. Оцінка ризиків допомагає зрозуміти, де знаходяться найвразливіші місця в системі. Моніторинг ризиків — це постійний процес відстеження цих загроз, оскільки ландшафт загроз постійно змінюється. |
| Навчання з інформаційної безпеки (Information Security Training) | Цей компонент передбачає навчання співробітників основним принципам кібербезпеки. Більшість кібератак починається з людської помилки — наприклад, переходу за фішинговим посиланням або використання слабких паролів. Регулярне навчання допомагає підвищити обізнаність персоналу і перетворити їх на першу лінію захисту. Навчання може включати тренінги, симуляції фішингових атак, семінари тощо. |
| Перевірка партнерів (Third-Party Partner Audits) | Багато організацій та установ залежать від послуг зовнішніх партнерів, таких як хмарні провайдери, постачальники програмного забезпечення або консалтингові фірми. Якщо інформаційні системи партнера скомпрометовані, це може призвести до витоку даних і в самій організації чи установі. Тому важливо регулярно перевіряти, чи дотримуються партнери належних стандартів кібербезпеки. Це може бути здійснено через аудити, оцінку ризиків або запит на надання відповідних незалежних сертифікатів безпеки або звітів, підготовлених зовнішніми аудиторами. |

*Джерело:* складено за даними [7]

*Таблиця 2*

**Характеристика ідентифікаторів кіберзагроз**

| Індикатори | Характеристика ідентифікаторів кіберзагроз |
|---|---|
| Мережеві | • Підозрілі IP-адреси (джерела атак, командні сервери ботнетів).<br>• Доменні імена, URL-адреси, що використовуються для фішингу чи C&C (Command and Control).<br>• Аномальний мережевий трафік. |
| Файлові | • Хеші для виявлення відомих шкідливих програм.<br>• Незвичайні або невідомі виконувані файли.<br>• Модифікації системних файлів або служб. |
| Системні | • Наявність нових чи невідомих процесів у системі.<br>• Неавторизовані зміни у реєстрі.<br>• Ознаки руткітів чи бекдорів. |
| Поведінкові | • Аномальні дії користувачів.<br>• Різке зростання кількості користувачів з привілейованими правами доступу.<br>• Підозріла активність електронної пошти, комп'ютерних програм та пристроїв. |
| Експлуатації вразливостей | • Використання відомих вразливостей.<br>• Виклики до нестандартних API.<br>• Активність сканування портів або пошуку вразливих служб. |

*Джерело:* складено автором самостійно

дані оновлюються періодично на основі публічних джерел, зокрема законодавства, звітів та офіційної інформації урядів.

Важливим аспектом кібербезпеки є визначення індикаторів кіберзагроз — ознак, які свідчать про можливу або вже реалізовану атаку в інформаційній системі. Вони допомагають виявляти, ідентифікувати та реагувати на шкідливу активність. Ідентифікатори бувають мережеві, файлові, системні, поведінкові та експлуатації вразливостей.

Всі ці індикатори є доволі технічними, й вимагають наявності відповідної кваліфікації та знань. В системі публічного управління в Україні основним суб'єктом забезпечення кібербезпеки є Державна служба спеціального зв'язку та захисту інформації України (Держспецзв'язку). Саме ця служба надає кваліфікована підтримку з питань кібербезпеки, відповідає за захист державних інформаційних ресурсів та критичної інфраструктури, а також координує моніторинг, попередження та реагування на інциденти кібербезпеки.

Окремим завданням Держспецзв'язку є ведення моніторингу та статистики кіберінцидентів. Як видно з рис. 1, прослідковується чіткий тренд на зростання кількості кіберінцидентів, зареєстрованих їхніми фахівцями.

Протягом першого півріччя 2025 року фахівці Держспецзв'язку опрацювали 3018 кіберінцидентів. Це на 17% більше, ніж у попередньому півріччі (тоді було опрацьовано 2575) [9], і становить 70% від усієї кількості кіберінцидентів, зареєстрованих в 2024 році.

Основними цілями ворога є об'єкти, де циркулює найбільше інформації, яку можна використати

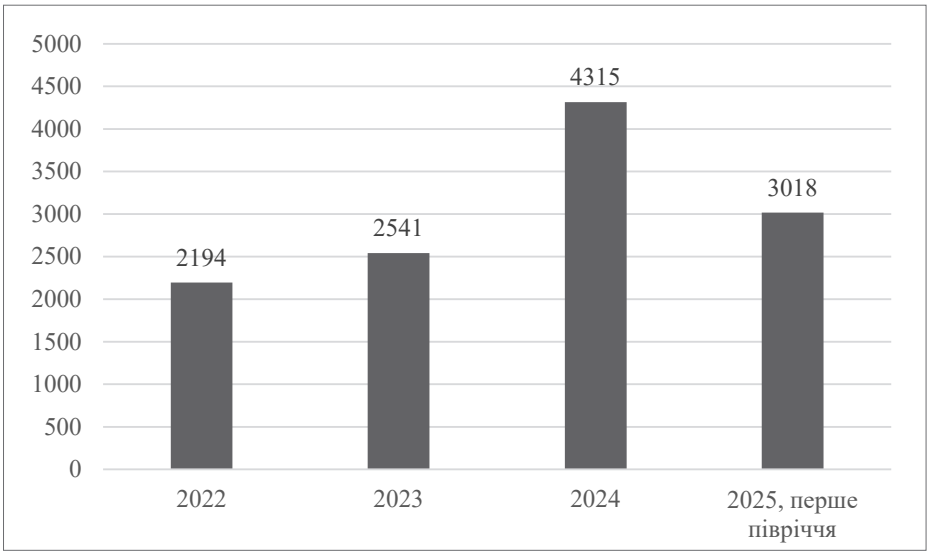


Рис. 1. Кількість зареєстрованих кіберінцидентів в Україні за 2022–2025 рр.

*Джерело:* складено за даними [9]

у воєнних діях, а також ті, де надаються сервіси, зупинка яких матиме значний вплив на безпеку та добробут цивільного населення [9]:

- місцеві органи влади,
- уряд та урядові організації,
- сектор безпеки та оборони,
- енергетичний сектор,
- комерційні організації, важливі для економіки України,
- телекомунікації тощо [10].

Вказана вище інформація свідчить, що кібервійна проти України постійно прогресує, а українські фахівці зобов'язані безперервно вдосконалювати власні навички, методи та інструменти захисту та активно протидіяти існуючим загрозам.

Враховуючи ці реалії, нагальною потребою є аналіз існуючих підходів до організації та проведення огляду стану кіберзахисту. Існуючі вимоги на загальнодержавному рівні можуть бути не завжди актуальними й не враховувати сучасних тенденцій в сфері кіберзагроз.

В зв'язку з цим, важливо розглядати кращі міжнародні практики та стандарти в цій сфері, зокрема стандарти ISO 27001, SOC2, NIST CSF тощо. Вони вже відпрацьовані роками та є загальновизнаними в світі. ISO 27001 більш поширений в європейських країнах, SOC2 та NIST CSF — В США.

Першою перевагою є те, що вони можуть застосовуватися в будь-яких сферах: в органах публічного управління, громадських організаціях, навчальних закладах, приватних підприємствах тощо. А другою — вони встановлюють вимоги до побудови процесів, пов'язаних з інформаційною та кібербезпекою, Це не глибокі технічні стандарти, які описують вимоги до антивірусів чи іншого програмного забезпечення. Вони, якраз, фокусуються на побудові єдиної системи всередині організації, фундаментом для якої є регулярний перегляд та оцінка ризиків. Окрім цього, наявність процесів, побудованих за будь-яким з цих стандартів, слугуватиме підтвердженням певного рівня надійності системи інформаційної та кібербезпеки для контрагентів та партнерів. Спираючись, на світовий досвід, легше визначити реальні вразливості.

**Висновки та перспективи подальших досліджень.** Проведений аналіз свідчить, що кібербезпека набуває все більшого значення в системі національної безпеки та публічному управлінні. Її значимість ще більше посилилася в умовах повномасштабного вторгнення Росії. Статистика, яку веде Держцпецзв'язку, чітко демонструє тренд на зростання кількості кіберінцидентів. Основними цілями кібератак є державні органи, уряд, об'єкти критичної інфраструктури та підприємства, які є важливими для функціонування економіки України.

Незважаючи на прогрес, який підтверджується позицією України в Національному індексі кібербезпеки (NCSI), виявлено низку системних проблем:

- недостатня інтеграція сучасних систем захисту;
- брак кваліфікованих фахівців;
- нехтуванням кіберризиками з боку керівництва.

Необхідність підвищення рівня кіберстійкості безпосередньо залежить від формування міцної культури кібербезпеки, де відповідальність має лежати на вищому керівництві, а персонал має регулярно проходити відповідне навчання.

Ключовим суб'єктом у сфері кібербезпеки є Держспецзв'язку, який повинен ефективно реагувати на загрози. Але окрім нього кожен суб'єкт публічного управління, критичної інфраструктури та бізнесу повинен розвивати свою власну систему кіберзахисту в умовах постійного зростання кіберзагроз.

Для подальшого зміцнення кіберзахисту в системі публічного управління України необхідно брати до уваги застосування кращих світових практик та стандартів (ISO 27001, SOC2, NIST CSF тощо) при побудові систем інформаційної та кібербезпеки. Реалізація цих заходів є першим кроком для визначення поточного рівня кібербезпеки та побудови ефективних планів її вдосконалення, що є особливо важливим в умовах війни.

***ДОДАТКОВА ІНФОРМАЦІЯ***

**ВНЕСОК АВТОРІВ:** Усі автори зробили внесок порівну.
**ФІНАНСУВАННЯ:** Автори не отримували фінансування для цього дослідження.
**ЗАЯВА ПРО ДОСТУПНІСТЬ ДАНИХ:** Не застосовується.
**КОНФЛІКТ ІНТЕРЕСІВ:** Автори заявляють про відсутність конфлікту інтересів.

**Література**

1. Edwards M., Williams E., Peersman C., Rashid A. Characterising Cybercriminals: A Review. *arXiv.org.* 2022. URL: https://arxiv.org/pdf/2202.07419 (дата звернення: 02.12.2025).

2. Bada M., Benson L. E., McAlaney J. R. C. The Social and Psychological Impact of Cyber Attacks. *Emerging Cyber Threats and Cognitive Vulnerabilities.* Academic Press, 2019/20.

3. Napolitano G. A literature review on the role of cybersecurity in changing management accounting, auditing and governance. *Monash University.* URL: https://www.monash.edu/__data/assets/pdf_file/0006/3118902/ (дата звернення: 02.12.2025).

4. Кулешов М. В. Сутність та зміст розслідування кіберінцидентів та кібератак підрозділами служби безпеки України. *Інформація і право*. 2019. № 2(29). С. 115–122.

5. Ковальова А., Яковлева А., Чорна А. Кримінальна відповідальність за кіберзлочини, вчинені в умовах воєнного стану. В кн.: Матеріали конференцій МЦНД: [зб. тез доп.]. (19.04.2024; Кропивницький, Україна). С. 63–64.

6. Колесніков А., Зяйлик М. Економіко-правові засади розвитку кіберзлочинності та методів боротьби з нею. *Актуальні проблеми правознавства.* 2017. Вип. 1(9). С. 26–29.

7. Cyber Security Auditing, Assurance, and Awareness Through CSAM and CATRAM. Stati Uniti: IGI Global, 2020. С. 135–137. URL: https://dokumen.pub/qdownload/cyber-security-auditing-assurance-and-awareness-through-csam-and-catram-9781799856092-1799856097.html (дата звернення: 02.12.2025).

8. Україна на 24 місці в рейтингу з кібербезпеки. *AIN.UA.* 2024. 16 черв. URL: https://ain.ua/2024/06/16/ukrayina-na-24-misczi-v-rejtyngu-z-kiberbezpeky/ (дата звернення: 02.12.2025).

9. Інтенсивність фішингових атак зросла, але люди стали більш обізнаними в питаннях кібергігієни: аналітичний звіт CERT-UA. *Держспецзв'язку.* URL: https://cip.gov.ua/ua/news/intensivnist-fishingovikh-atak-zrosla-ale-lyudi-stali-bilsh-obiznanimi-v-pitannyakh-kibergigiyeni-analitichnii-zvit-cert-ua (дата звернення: 02.12.2025).

10. У 2024 році кількість кібератак на Україну зросла на 70%: [інформаційне повідомлення]. *Інститут масової інформації (IMI).* URL: https://imi.org.ua/news/u-2024-rotsi-kilkist-kiberatak-na-ukrayinu-zrosla-na-70-i65931 (дата звернення: 02.12.2025).

**References**

1. Edwards, M., Williams, E., Peersman, C., & Rashid, A. (2022). Characterising Cybercriminals: A Review. *arXiv.org.* URL: https://arxiv.org/pdf/2202.07419

2. Bada, M., Benson, L. E., & McAlaney, J. R. C. (2019/20). The Social and Psychological Impact of Cyber Attacks. *Emerging Cyber Threats and Cognitive Vulnerabilities*. Academic Press.

3. Napolitano, G. A literature review on the role of cybersecurity in changing management accounting, auditing and governance. *Monash University.* URL: https://www.monash.edu/__data/assets/pdf_file/0006/3118902/

4. Kuleshov, M. V. (2019). Sutnist ta zmist rozsliduvannia kiberintsyndentiv ta kiberatak pidrozdilamy sluzhby bezpeky Ukrainy. *Informatsiia i pravo,* No. 2(29), pp. 115–122 [in Ukrainian].

5. Kovaliova, A., Yakovlieva, A., & Chorna, A. (2024). Kryminalna vidpovidalnist za kiberzlochyny, vchyneni v umovakh voiennoho stanu: Materialy konferentsii MTsND. Kropyvnytskyi, Ukraine, pp. 63–64 [in Ukrainian].

6. Kolisnikov, A., & Ziailyk, M. (2017). Ekonomiko-pravovi zasady rozvytku kiberzlochynnosti ta metodiv borotby z neiu. *Aktualni problemy pravoznavstva,* Vol. 1(9), pp. 26–29 [in Ukrainian].

7. Cyber Security Auditing, Assurance, and Awareness Through CSAM and CATRAM (2020). Stati Uniti: IGI Global, pp. 135–137. URL: https://dokumen.pub/qdownload/cyber-security-auditing-assurance-and-awareness-through-csam-and-catram-9781799856092–1799856097.html

8. Ukraina na 24 mistsi v reitynhu z kiberbezpeky. (2024). *AIN.UA.* URL: https://ain.ua/2024/06/16/ukrayina-na-24-misczi-v-rejtyngu-z-kiberbezpeky/ [in Ukrainian].

9. Intensyvnist fishynhovykh atak zrosla, ale liudy staly bilsh obiznanymy v pytanniakh kiberhihiieny: analitychnyi zvit CERT-UA. *Derzhspetszviazku.* URL: https://cip.gov.ua/ua/news/intensivnist-fishingovikh-atak-zrosla-ale-lyudi-stali-bilsh-obiznanimi-v-pitannyakh-kibergigiyeni-analitichnii-zvit-cert-ua [in Ukrainian].

10. U 2024 rotsi kilkist kiberatak na Ukrainu zrosla na 70%. *Instytut masovoi informatsii (IMI).* URL: https://imi.org.ua/news/u-2024-rotsi-kilkist-kiberatak-na-ukrayinu-zrosla-na-70-i65931 [in Ukrainian].

*Дата першого надходження статті до видання: 08.01.2026*
*Дата прийняття статті до друку після рецензування: 08.02.2026*
*Дата публікації: 28.02.2026*