УДК 004.02+006/.8 doi.org/10.33298/2226-8553.2025.1.42.28

***Богом'я В. І., Черемісіна Л. О., Ярмолатій А. В., Галунько В.В.***

# ЕФЕКТИВНА ОРГАНІЗАЦІЯ СИСТЕМИ СТАНДАРТІВ ТА ПРАВОВИХ НОРМ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

*Сучасне суспільство активно використовує цифрові технології в різних сферах життя: економіці, охороні здоров'я, освіті, державному управлінні тощо. Це створює нові можливості, але в той же час відкриває шлях для появи кіберзагроз. Все це відповідно призводить до величезних економічних втрат від кібератак. Так збитки, завдані кібератаками, щороку сягають мільярдів доларів. Захист інформації є важливим елементом економічної стабільності та національної безпеки держави. Таким чином, актуальність статті обумовлена необхідністю протистояти сучасним кіберзагрозам, забезпечити безпеку інформації, дотримуватися законодавчих вимог та адаптуватися до швидких змін у цифровому світі. Відомо, що міжнародні стандарти часто розробляються з урахуванням глобальних практик, але їх застосування може бути ускладнене через локальні особливості. Загальні виклики у впровадженні стандартів і правових норм вже визначені фахівцями, але не наведена характеристика проблем у забезпеченні кібербезпеки та які рекомендації необхідно зробити для удосконалення системи стандартів та правових норм.*

*Тому метою статті є аналіз існуючих систем стандартів та правових норм у сфері інформаційної безпеки для розуміння їхньої ефективності, актуальності та можливостей удосконалення для розроблення відповідних рекомендацій. За результатами аналізу можна зазначити, що міжнародні стандарти, такі як ISO/IEC 27001 та ISO/IEC 27002, забезпечують фундаментальні принципи для створення систем управління інформаційною безпекою, сприяючи уніфікації підходів та управлінню ризиками. Разом з тим, динамічний розвиток кіберзагроз вимагає регулярного оновлення нормативно-правової бази для ефективної протидії новим викликам. Також спостерігається важливість комплексного підходу до забезпечення інформаційної безпеки. Це дозволить створити ефективну організацію системи стандартів та правових норм інформаційної безпеки, а тому створити безпечне інформаційне середовище, яке сприятиме стабільному розвитку суспільства, бізнесу та держави в умовах цифрової трансформації.*

***Ключові слова:*** *інформаційна безпека, кібербезпека, кіберзагроза, міжнародні стандарти, національні стандарти, правові норми, ефективність, система*

**Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями.** Сучасне цифрове суспільство характеризується швидким розвитком цифрових технологій. Сучасне суспільство активно використовує цифрові технології в різних сферах життя: економіці, охороні здоров'я, освіті, державному управлінні тощо. Це створює нові можливості, але в той же час відкриває шлях для появи кіберзагроз [1,6].

Наразі спостерігається швидке зростання кількості та складності кіберзлочинів, коли атаки на інформаційні системи, витік даних, фішинг, шкідливе програмне забезпечення та інші форми кіберзлочинності становлять серйозну загрозу для компаній, урядів та приватних осіб.

Все це відповідно призводить до величезних економічних втрат від кібератак. Так збитки, завдані кібератаками, щороку сягають мільярдів доларів. Захист інформації є важливим елементом економічної стабільності та національної безпеки держави.

Ще одним аспектом ситуації є те, що у світі зростає обсяг персональної інформації, що зберігається та передається в цифровій формі. Забезпечення конфіденційності є важливим аспектом захисту прав людини, тому захист персональних даних є дуже важливим [2,7].

Також присутні міжнародні та геополітичні загрози, коли кіберпростір стає ареною міждержавного протистояння, а кіберзброя – новим інструментом у геополітиці.

Національні та міжнародні правові норми вимагають впровадження заходів безпеки, що зобов'язує організації дотримуватися стандартів і законодавчих вимог, тому виникає необхідність дотримання відповідного законодавства [3,4].

Таким чином, актуальність статті обумовлена необхідністю протистояти сучасним кіберзагрозам, забезпечити безпеку інформації, дотримуватися законодавчих вимог та адаптуватися до швидких змін у цифровому світі.

**Аналіз останніх досліджень і публікацій.** Правові норми у сфері кібербезпеки визначені у міжнародному законодавстві Загальної декларацією прав людини (ст. 12 про конфіденційність) та Будапештської конвенцією про кіберзлочинність [5,6].

Правові норми у сфері кібербезпеки визначені у Національному законодавстві Законом України "Про основні засади забезпечення кібербезпеки України" та Європейськими директивами, наприклад, GDPR.

Низький рівень обізнаності про стандарти наведено у [7, 8].

Труднощі адаптації міжнародних норм до національних реалій наведено у [9, 10], коли міжнародні стандарти часто розробляються з урахуванням глобальних практик, але їх застосування може бути ускладнене через локальні особливості.

Загальні виклики у впровадженні стандартів і правових норм визначені у [9, 10], але не наведена характеристика проблем у забезпеченні кібербезпеки та які рекомендації необхідно зробити для удосконалення системи стандартів та правових норм.

**Метою статті є** аналіз існуючих систем стандартів та правових норм у сфері інформаційної безпеки для розуміння їхньої ефективності, актуальності та можливостей удосконалення для розроблення відповідних рекомендацій.

Для досягнення цієї мети необхідно вирішити такі завдання:

1. Провести огляд міжнародних та національних стандартів кібербезпеки (наприклад, ISO/IEC 27001, NIST, GDPR).
2. Провести дослідження правового регулювання кібербезпеки на рівні національного та міжнародного законодавства.
3. Провести аналіз основних викликів у впровадженні стандартів та норм.
4. Розробити рекомендації щодо вдосконалення системи стандартів і правових норм у сфері інформаційної безпеки.

**Виклад основного матеріалу дослідження.** Коротко розглянемо теоретичні основи інформаційної безпеки, а саме наддамо поняття інформаційної безпеки та кібербезпеки, визначимо основні загрози інформаційній безпеці та характеризуємо роль стандартів і правових норм у забезпеченні кібербезпеки.

**Інформаційна безпека** – це стан захищеності інформаційних ресурсів та процесів їхньої обробки, який забезпечує конфіденційність, цілісність та доступність інформації.

Основними цілями інформаційної безпеки є конфіденційність – захист інформації від несанкціонованого доступу; цілісність – забезпечення коректності та захист від несанкціонованих змін та доступність – гарантування доступу до інформації у необхідний час.

Що стосується поняття «кібернетична безпека», то кібербезпека – це сукупність заходів, спрямованих на захист систем, мереж, програмного забезпечення та даних від кіберзагроз, таких як хакерські атаки, шкідливі програми, фішинг тощо. Кібербезпека є складовою інформаційної безпеки, орієнтованою переважно на цифрове середовище.

Які основні загрози інформаційній безпеці існують та визначені фахівцями в цієї галузі:

– кіберзлочини: хакерські атаки (наприклад, DDoS-атаки), викрадення персональних або корпоративних даних, фішинг (обман користувачів для отримання їхніх даних).

– шкідливе програмне забезпечення: віруси, трояни, програми-здирники (ransomware), бекдори (backdoor) для несанкціонованого доступу до систем.

– інсайдерські загрози: дії співробітників, що можуть ненавмисно або навмисно створити загрози для інформаційної безпеки.

– порушення конфіденційності: незаконний доступ до персональних даних, витік корпоративної інформації.

– соціальна інженерія: маніпулювання людьми для отримання доступу до конфіденційної інформації.

– технічні збої: аварії в обладнанні, втрати даних через несправності систем.

Для визначення ролі стандартів і правових норм у забезпеченні кібербезпеки розглянемо такі стандарти кібербезпеки, як міжнародні стандарти (ISO/IEC 27001, NIST Cybersecurity Framework), що забезпечують уніфікацію вимог до безпеки інформації, визначення процедур для оцінки ризиків і реагування на інциденти, підвищення рівня довіри між партнерами та клієнтами. Також національні стандарти, що допомагають враховувати локальні особливості та специфіку законодавства [10,11].

Системи стандартів у сфері інформаційної безпеки організована наступним чином. Існують міжнародні стандарти в сфері інформаційної безпеки.

ISO/IEC 27001 (Система управління інформаційною безпекою). Цей стандарт є міжнародно визнаною моделлю для створення, впровадження, моніторингу та вдосконалення системи управління інформаційною безпекою (СУІБ). Основні характеристики стандарту: забезпечення захисту інформації шляхом управління ризиками; визначає вимоги до впровадження політики інформаційної безпеки, управління ризиками, моніторингу, аудиту та вдосконалення безпеки; ідентифікація активів та оцінка ризиків; впровадження контролю доступу, криптографії, управління інцидентами та безперервності бізнесу; дозволяє організаціям отримати офіційне підтвердження відповідності вимогам стандарту.

ISO/IEC 27002 (Керівні принципи забезпечення безпеки). Цей стандарт є доповненням до ISO/IEC 27001 і надає практичні рекомендації для впровадження заходів безпеки. Основним характеристиками є: допомогти організаціям впроваджувати відповідні заходи захисту на основі аналізу ризиків; охоплює 14 основних доменів, серед яких: управління активами, безпека персоналу, управління доступом, криптографія, фізична безпека, захист операцій тощо; вибір конкретних заходів безпеки залежно від бізнес-цілей і ризиків; адаптація політик безпеки до потреб організації.

Існують також інші міжнародні релевантні стандарти, наприклад:

– ISO/IEC 27005 – Управління ризиками інформаційної безпеки, який забезпечує методологічну основу для ідентифікації, оцінки та управління ризиками.

– ISO/IEC 22301 – Управління безперервністю бізнесу, який регламентує підготовку організацій до кризових ситуацій.

– NIST Cybersecurity Framework (США). Включає 5 основних функцій: ідентифікація, захист, виявлення, реагування, відновлення. Служить національною основою для управління кіберризиками.

До національних стандартів можна віднести ДСТУ в Україні. Наприклад, ДСТУ ISO/IEC 27001:2015 – національна адаптація міжнародного стандарту для українських організацій, що законодавчо підтримує впровадження СУІБ в державному та приватному секторах.

Також, необхідно визначити NIST (США). Це Національний інститут стандартів і технологій США розробляє рекомендації та стандарти кібербезпеки, наприклад, NIST SP 800-53 (Контроль безпеки та конфіденційності) та зосереджується на інтеграції безпеки в технологічну інфраструктуру [10, 12].

Іншими прикладами можуть бути у Німеччині BSI IT-Grundschutz; у ЄС: ENISA (Європейське агентство з кібербезпеки).

Вплив стандартів на управління ризиками та організацію безпеки здійснюється через систематизацію процесів, коли стандарти надають структурований підхід до управління ризиками, а також визначають етапи: ідентифікація активів, оцінка ризиків, вибір заходів захисту [10, 11].

Також вплив стандартів на управління ризиками та організацію безпеки здійснюється через підвищення ефективності управління, коли впровадження стандартів сприяє уніфікації політик

безпеки, що знижує імовірність помилок та забезпечується інтеграція безпеки в усі бізнес-процеси. Це надає можливість [12,13]:

– зменшення ризиків, коли відповідність стандартам допомагає мінімізувати кіберзагрози шляхом впровадження надійних технічних і організаційних заходів;

o підвищення довіри, коли організації, які дотримуються міжнародних стандартів, викликають більше довіри у клієнтів і партнерів;

o підготовка до інцидентів, коли стандарти регламентують процеси управління інцидентами, забезпечення безперервності бізнесу та швидкого відновлення після атак;

o відповідність законодавству, коли дотримання стандартів часто є обов'язковою умовою для виконання правових вимог, таких як GDPR.

Таким чином, стандарти та національні регуляції відіграють важливу роль у формуванні ефективної системи інформаційної безпеки, сприяючи зменшенню ризиків і підвищенню стійкості організацій до кіберзагроз.

За результатами аналізу [1-7, 11] можна визначити характеристики проблем у сфері впровадження стандартів і правових норм.

По-перше, це низький рівень обізнаності про стандарти, що обумовлено відсутністю інформаційної кампанії щодо важливості стандартів кібербезпеки, недостатнім рівнем підготовки фахівців у сфері інформаційної безпеки та складністю технічних термінів і процедур, викладених у стандартах.

Наслідками цього низького рівня обізнаності є те, що підприємства та організації не впроваджують належні заходи безпеки та присутний ризик неналежного реагування на кіберінциденти [11].

По-друге це труднощі адаптації міжнародних норм до національних реалій, що обумовлено різницею в юридичних системах та економічних умовах різних країн, високою вартістю адаптації стандартів для малих і середніх підприємств та відсутністю відповідних ресурсів та інфраструктури для впровадження.

Наслідками цього є повільне впровадження міжнародних стандартів у національне законодавство та невідповідність вимогам глобального ринку.

По-третє, це динаміка кіберзагроз та потреба в оновленні законодавства, що обумовлено постійним розвитком нових типів кіберзагроз (наприклад, шкідливе ПЗ, атаки на IoT), технологічними інноваціями (штучний інтелект, блокчейн, квантові обчислення), які змінюють середовище загроз та застаріле або недостатньо деталізоване законодавство у багатьох країнах.

Наслідками динаміка кіберзагроз є недостатня підготовленість національних систем безпеки до сучасних викликів та відставання від потреб цифрового суспільства [11,12].

**Рекомендації.** Враховуючі вищенаведене доцільно надати рекомендації щодо вдосконалення систем стандартів і правових норм, як розробка нових стандартів, що відповідають сучасним викликам, посилення міжнародного співробітництва у сфері кібербезпеки, розроблення освітніх ініціатив для підвищення рівня компетенцій у сфері кібербезпеки.

Що стосується розроблення нових стандартів, що відповідають сучасним викликам, це – інтеграція вимог до захисту новітніх технологій (IoT, штучний інтелект (AI), хмарних обчислень); розробка стандартів, що враховують галузеві особливості (медицина, фінанси, енергетика), спрощення та адаптація стандартів для різних масштабів бізнесу (малий і середній бізнес).

Це наддасте змогу отримати збільшення охоплення стандартами різних типів організацій та підвищення готовності до нових типів загроз.

Що стосується посилення міжнародного співробітництва у сфері кібербезпеки, це – створення глобальних платформ для обміну досвідом та інформацією про кіберзагрози, розробка універсальних стандартів, які будуть взаємно прийнятими різними країнами, підтримка країн, що розвиваються, у впровадженні кібербезпеки.

Це наддасте змогу отримати такий очікуваний ефект, як зменшення розриву між країнами у рівні кіберзахисту та підвищення ефективності міжнародної координації у боротьбі з кіберзлочинністю.

Що стосується освітніх ініціатив для підвищення рівня компетенцій у сфері кібербезпеки, це – впровадження освітніх програм з кібербезпеки у школах та університетах, підвищення кваліфікації існуючих фахівців через тренінги та сертифікації, організація національних і міжнародних конференцій, хакатонів, семінарів.

Це наддасте змогу отримати такий очікуваний ефект, як формування кадрів, здатних ефективно впроваджувати сучасні стандарти та підвищення загального рівня кібергігієни серед населення.

Реалізація зазначених рекомендацій дозволить створити більш гнучку, адаптивну та ефективну систему кібербезпеки, яка відповідатиме сучасним викликам цифрового світу, забезпечуючи захист держави, бізнесу та громадян.

**Висновки з дослідження**

1. Підводячи підсумки аналізу систем стандартів і правових норм, можна зазначити, що міжнародні стандарти, такі як ISO/IEC 27001 та ISO/IEC 27002, забезпечують фундаментальні принципи для створення систем управління інформаційною безпекою, сприяючи уніфікації підходів та управлінню ризиками.

Але спостерігаються труднощі впровадження національних норм, тому адаптація міжнародних стандартів до національних реалій потребує врахування економічних, юридичних та технологічних особливостей кожної країни. Це уповільнює процес інтеграції сучасних заходів безпеки.

Разом з тим, динамічний розвиток кіберзагроз вимагає регулярного оновлення нормативно-правової бази для ефективної протидії новим викликам.

2. Також спостерігається важливість комплексного підходу до забезпечення інформаційної безпеки. Це по-перше системність, коли забезпечення інформаційної безпеки повинно включати як технічні, так і організаційні заходи. При цьому важливо забезпечити інтеграцію стандартів, правових норм та управлінських рішень.

По-друге, це освіта та обізнаність, коли необхідно підвищувати рівень знань та компетенцій як серед фахівців, так і серед широкого загалу, щоб запобігати основним кіберзагрозам.

По-третє, це міжнародне співробітництво, коли глобальний характер кіберзагроз потребує координації зусиль на міждержавному рівні, включаючи обмін інформацією та кращими практиками.

По-четверте, це інновації, коли для протидії новим викликам у сфері кібербезпеки важливо постійно розробляти та впроваджувати сучасні технології, які відповідають актуальним загрозам.

Це дозволить створити ефективну організацію системи стандартів та правових норм інформаційної безпеки, а тому створити безпечне інформаційне середовище, яке сприятиме стабільному розвитку суспільства, бізнесу та держави в умовах цифрової трансформації.

## ЛІТЕРАТУРА

1. ДСТУ ISO/IEC 27000:2018. Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою (ISO/IEC 27000:2016, IDT).
2. ДСТУ ISO/IEC 27002:2018 Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки (ISO/IEC 27002:2013; Cor 1:2014, IDT).
3. IEEE 802.11-2020 – стандарт безпеки бездротових локальних мереж, контроль доступу (MAC) та функції фізичного рівня (PHY).
4. Впровадження засобів захисту інформації для споживачів та постачальників хмарних послуг на основі стандарту ISO/IEC 27017.
5. Стандарт безпеки даних платіжних карт PCI DSS. Стандарт FINRA для забезпечення захисту даних користувачів при здійсненні фінансових операцій.

6. Інформаційна безпека держави: навч. посіб. для студ. спец. 6.170103 «Управління інформаційною безпекою», 125 «Кібербезпека»/ В.І. Гур'єв, Д.Б. Мехед, Ю.М. Ткач, І.В. Фірсова. Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2021. 166 с. : іл.
7. Tupkalo V., Zaplotynskyi B. Fundamentals of information security management system engineering of modern process-oriented enterprises: monograph. Kyiv: KUIPL, 2024. 81 p., https://www.lap-publishing.com
8. Tupkalo V.M., Bogomya V.I., Iarmolatii A.V. Information security management system: problem aspects of implementation. Сучасні аспекти модернізації науки: стан, проблеми, тенденції розвитку: матеріали XXXVIII Міжнародної науково-практичної конференції / за ред. І.В. Жукової, Є.О. Романенка. м. Брно (Чехія): ГО «ВАДНД», 07 листопада 2023 р. С.276-280.
9. Корченко О.Г. Аудит та управління інцидентами інформаційної безпеки // О.Г. Корченко, С.О. Гнатюк, С.В. Казмірчук, В.М. Панченко, С.В. Мельник. Київ: Центр навч.-наук. та наук.-пр. видань НА СБ України, 2020. 193 с.
10. Юдін О.І. Захист інформації в мережах передачі даних // О.І. Юдін, О.Г. Корченко, Г.Ф. Конахович Київ: Вид-во ТОВ «НВП» Інтерсервіс», 2021. 716 с.
11. Юдін О.К. Інформаційна безпека. Нормативно-правове забезпечення: підручник / О.К.Юдін. Київ : НАУ, 2021. 639 с.
12. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. О. Хорошко, В.Б. Толубко, С.В. Толюпа]; за заг. ред. д-ра техн. наук, професора В.Б. Толубка. Київ: ДУТ, 2021, 288 с.
13. Богом'я В.І., Кочегаров В.С. Кібербезпека в хмарних сервісах за допомогою застосування криптографічних методів. Водний транспорт. 2022. Вип.1(35). С.25–32.

***Bohomia V. I., Cheremisina L. O., Yarmolatii A. V., Galynko V.V.***

**EFFECTIVE ORGANIZATION OF THE SYSTEM OF STANDARDS AND LEGAL NORMS OF INFORMATION SECURITY**

Modern society actively employs digital technologies in various areas of life: the economy, healthcare, education, public administration, and more. This creates new opportunities but simultaneously opens pathways for the emergence of cyber threats.

*All this leads to significant economic losses caused by cyberattacks. The damage inflicted by cyberattacks amounts to billions of dollars annually. Information protection is a crucial element of a state's economic stability and national security.*

*Thus, the relevance of this article is driven by the need to counter contemporary cyber threats, ensure information security, comply with legislative requirements, and adapt to rapid changes in the digital world.*

*It is known that international standards are often developed with consideration of global practices, but their application can be complicated by local specifics. General challenges in implementing standards and legal norms have already been identified by experts, but the specific issues in ensuring cybersecurity and the recommendations needed to improve the system of standards and legal norms have not been fully characterized.*

*The aim of this article is to analyze the existing systems of standards and legal norms in the field of information security to understand their effectiveness, relevance, and potential for improvement, and to develop appropriate recommendations.*

*Based on the analysis, it can be noted that international standards, such as ISO/IEC 27001 and ISO/IEC 27002, provide fundamental principles for creating information security management systems, contributing to the unification of approaches and risk management.*

*At the same time, the dynamic evolution of cyber threats requires the regular updating of the regulatory framework to effectively address new challenges.*

*Moreover, the importance of a comprehensive approach to ensuring information security has been observed. This will enable the creation of an effective organization of the system of standards and legal norms of information security, fostering a secure information environment that supports the stable development of society, business, and the state in the context of digital transformation.*

***Keywords:*** *information security, cybersecurity, cyber threat, international standards, national standards, legal norms, effectiveness, system*