Отримано: 28 квітня 2026 р.

Прорецензовано: 10 травня 2026 р.

Прийнято до друку: 18 травня 2026 р.

email: kuchkovaov@gmail.com

ORCID-ідентифікатор: https://orcid.org/0000-0002-9249-0216

email: y.c.bilousov@gmail.com

ORCID-ідентифікатор: https://orcid.org/0009-0009-0557-3717

DOI: http://doi.org/10.25264/2311-5149-2026-41(69)-123-128

Кучкова О. В., Білоусов Я. С. Стратегічне управління безпекою бізнес-систем у цифрову епоху. *Наукові записки Національного університету «Острозька академія» : серія «Економіка».* Острог : Вид-во НаУОА, червень 2026. № 41(69). С. 123–128.

УДК: 005.21:658.012.8:004

JEL-класифікація: L21, M21, O33

Кучкова Ольга Вікторівна,
кандидатка економічних наук, доцентка кафедри маркетингу та логістики,
завідувачка кафедри маркетингу та логістики
Українського державного університету науки і технологій

Білоусов Ярослав Сергійович,
аспірант кафедри маркетингу та логістики
Українського державного університету науки і технологій

СТРАТЕГІЧНЕ УПРАВЛІННЯ БЕЗПЕКОЮ БІЗНЕС-СИСТЕМ У ЦИФРОВУ ЕПОХУ

У статті досліджено теоретико-методологічні засади формування ефективної стратегії управління безпекою бізнес-систем в умовах цифрової трансформації. Обґрунтовано, що сучасні бізнес-системи функціонують як відкриті соціотехнічні системи, інтегровані з хмарними технологіями, штучним інтелектом, Big Data та IoT, що суттєво розширює спектр ризиків і загроз їх функціонуванню. Доведено необхідність переходу від традиційних підходів інформаційної безпеки до комплексного управління економічною безпекою підприємства, яке охоплює фінансову стійкість, захист активів, репутацію та конкурентоспроможність.

Визначено, що теоретичною основою формування стратегії є системний, ризик-орієнтований та інтегративний підходи, які поєднують класичні положення теорії систем і економічної безпеки з сучасними міжнародними стандартами та фреймворками, зокрема NIST Cybersecurity Framework 2.0 та ISO/IEC 27001:2022. Акцентовано увагу на зростанні ролі концепції Zero Trust як ключового принципу забезпечення безпеки в умовах розмитих цифрових кордонів організацій.

Окрему увагу приділено українському досвіду цифровізації, який демонструє високий рівень впровадження принципів Security by Design у державному та приватному секторах. Показано, що ефективна стратегія управління безпекою бізнес-систем виступає не лише засобом захисту, а й важливим фактором підвищення довіри стейкхолдерів і забезпечення стійкого розвитку підприємства.

Ключові слова: *ефективність управління, стратегічне управління, економічна безпека, бізнес-система, цифрова трансформація, управління розвитком.*

Olha Kuchkova,
PhD in Economics, Associate Professor,
Head of the Department of Marketing and Logistics,
Ukrainian State University of Science and Technology

Yaroslav Bilousov,
PhD student at the Department of Marketing and Logistics,
Ukrainian State University of Science and Technology

STRATEGIC MANAGEMENT OF BUSINESS SYSTEM SECURITY IN THE DIGITAL ERA

This article examines the theoretical and methodological foundations of forming an effective security management strategy for business systems under digital transformation. Modern business systems function as open socio-technical systems integrated with cloud technologies, artificial intelligence, Big Data, and IoT, significantly expanding operational risks and threats. The study substantiates a necessary transition from traditional information security toward comprehensive enterprise economic security, encompassing financial stability, asset protection, reputation, and competitiveness.

The theoretical basis for strategy formulation includes systemic, risk-oriented, and integrative approaches, combining classical systems theory and economic security with international frameworks, particularly the NIST Cybersecurity Framework 2.0 and ISO/IEC 27001:2022. Additionally, the study emphasizes the growing role of the Zero Trust model as a fundamental principle for securing blurred organizational digital boundaries.

The strategic methodology involves a stepwise process: system diagnosis, risk identification, target security modeling, action programming with defined KPIs, implementation, monitoring, and adaptive adjustment. The paper demonstrates

the feasibility of leveraging modern tools, including AI technologies, big data analytics, real-time monitoring systems, and principles of adaptive security and resilience.

Particular attention is paid to the Ukrainian digitalization experience, demonstrating high implementation levels of «Security by Design» principles across public and private sectors. Ultimately, an effective security management strategy serves not only as a protective mechanism but also as a critical determinant for increasing stakeholder trust and ensuring sustainable enterprise development.

Keywords: *management efficiency, strategic management, economic security, business system, digital transformation, development management.*

Постановка проблеми. Сучасний етап розвитку глобальної економіки характеризується тотальною цифровізацією, що докорінно змінює архітектуру побудови та функціонування бізнес-систем. Перехід до цифрових моделей управління відкриває перед підприємствами безпрецедентні можливості для зростання, проте одночасно генерує нові типи викликів та загроз. У цих умовах традиційні підходи до забезпечення стабільності стають недостатніми, що зумовлює необхідність переосмислення парадигми безпеки.

Стратегічне управління безпекою бізнес-систем у цифрову епоху вже не може обмежуватися лише захистом ресурсів або протидією окремим ризикам. Воно трансформується у комплексний процес підтримки динамічної стійкості підприємства. Ключовим завданням стає створення такої системи управління розвитком, яка б інтегрувала цифрові технології у фундамент соціально-економічної безпеки, забезпечуючи адаптивність бізнесу до непередбачуваних змін зовнішнього середовища.

Аналіз останніх досліджень та публікацій. Проблематика управління безпекою бізнес-систем в умовах цифрової трансформації активно досліджується у сучасній науковій літературі, що зумовлено стрімким розвитком цифрових технологій та зростанням кіберзагроз. Останні дослідження демонструють перехід від фрагментарних підходів до забезпечення інформаційної безпеки до комплексних, інтегрованих моделей управління ризиками на рівні всієї організації.

Теоретичний підґрунтя стратегічного управління бізнес-процесами закладено в межах процесного підходу та реінжинірингу. Фундаментальний внесок у переосмислення процесів як базису для зростання результативності бізнесу зробили М. Гаммер та Дж. Чампі [1]. Системний розвиток методології BPM та її поєднання з управлінськими рішеннями детально проаналізовано Т. Девенпортом [2]. Роль процесів у створенні конкурентних переваг і ланцюгів цінності обґрунтував М. Портер [3], тоді як інструментарій узгодження стратегічних пріоритетів із показниками ефективності розробили Р. Каплан та Д. Нортон [4]. Сучасний контекст управління, зумовлений цифровою трансформацією та еволюцією бізнес-моделей, представлений у працях Г. Віала [5], Е. Бріньольфссона та А. Макафі [6].

Мета і завдання дослідження. Мета дослідження полягає в обґрунтуванні теоретико-методологічних засад та розробці практичних рекомендацій щодо формування ефективної стратегії управління безпекою бізнес-систем в умовах цифрової трансформації.

Для досягнення поставленої мети визначено такі завдання дослідження**:**

– проаналізувати сучасні підходи до управління безпекою бізнес-систем у контексті цифрової трансформації та визначити їх еволюцію;

– узагальнити теоретичні основи формування безпеки бізнес-систем на засадах системного, ризик-орієнтованого та інтегративного підходів;

– провести порівняльний аналіз сучасних фреймворків і стандартів управління безпекою (NIST CSF 2.0, ISO/IEC 27001:2022, Zero Trust Architecture) та визначити їх переваги й обмеження;

– обґрунтувати методологію формування стратегії управління безпекою бізнес-систем із урахуванням принципів адаптивності та resilience;

– узагальнити сучасний український та міжнародний досвід забезпечення безпеки бізнес-систем і визначити напрями його адаптації.

Реалізація зазначених завдань дозволяє сформувати комплексне бачення побудови ефективної, адаптивної та стійкої системи управління безпекою бізнесу в умовах цифрової економіки.

Виклад основного матеріалу. Цифрова трансформація кардинально змінює архітектуру бізнес-систем, переводячи їх у гібридне цифрове середовище, де фізичні процеси інтегруються з хмарними технологіями, штучним інтелектом, Big Data та IoT [12; 14]. Бізнес-системи при цьому стають складними відкритими соціотехнічними системами, які постійно зазнають нових загроз: кібератаки, витоки даних, порушення конфіденційності, залежність від постачальників хмарних сервісів та регуляторних ризиків [19; 16].

Управління безпекою бізнес-систем у цьому контексті виходить за межі традиційної інформаційної безпеки й охоплює економічну безпеку підприємства (фінансову стійкість, збереження активів, репутацію та конкурентоспроможність). Формування ефективної стратегії вимагає чітких теоретико-методологічних засад, які забезпечують системність, адаптивність і орієнтацію на бізнес-результати [17].

Теоретичною основою є системний підхід (Л. фон Берталанфі, загальна теорія систем), згідно з яким бізнес-систему розглядають як сукупність взаємопов'язаних елементів (людські ресурси, процеси, технології, дані), де безпека є емерджентною властивістю всієї системи, а не лише її IT-складової [7]

S. Kraus та ін. у своїх наукових роботах підкреслюють, що цифрова трансформація створює нові можливості, але водночас генерує системні ризики, які вимагають інтеграції безпеки в бізнес-стратегію вже на етапі стратегічного планування [8].

Ключовим сучасним принципом є політика нульової довіри – жоден суб'єкт (користувач, пристрій, додаток) не вважається довіреним за замовчуванням. Це відповідає реаліям цифрового середовища, де кордони організації розмиті [10, 15].

Реалізація такого безкомпромісного захисту потребує не просто точкових рішень, а комплексної методології формування стратегії, що базується на інтегративному підході.

Методологія формування стратегії базується на інтегративному підході, що поєднує стратегічний менеджмент, ризик-орієнтоване управління та цифрові технології [17].

Основними методологічними елементами можна відокремити:

1. Ризик-орієнтований підхід (NIST Cybersecurity Framework 2.0 та ISO/IEC 27001:2022). NIST CSF пропонує шість функцій (Govern, Identify, Protect, Detect, Respond, Recover), які дозволяють оцінювати поточний стан безпеки та будувати roadmap розвитку. ISO 27001 забезпечує формалізацію через систему управління інформаційною безпекою (ISMS) з обов'язковою сертифікацією. Обидва фреймворки є комплементарними й активно застосовуються в умовах цифрової трансформації [9, 11].

2. Стратегічний менеджмент безпеки – стратегія безпеки повинна бути частиною загальної бізнес-стратегії (alignment). Використовуються такі інструменти, як PESTLE з цифровим SWOT-аналізом, матриця ризиків з урахуванням цифрових загроз та моделі зрілості кібербезпеки (CMMI, Cybersecurity Maturity Model) [17].

3. Сучасний інструментарій реалізації стратегії охоплює аналіз даних та штучний інтелект для високоточного прогнозування загроз, використання хмарних технологій із вбудованими протоколами захисту, а також впровадження систем автоматизованого тестування і моніторингу в режимі реального часу для забезпечення безперервної стійкості цифрового середовища [14].

4. Принцип адаптивності та resilience – стратегія має бути гнучкою, з можливістю швидкого реагування на нові загрози (agile security management) [16].

Процес формування ефективної стратегії управління безпекою розпочинається з глибокої діагностики, яка передбачає всебічну оцінку поточного стану бізнес-системи та ідентифікацію критичних цифрових ризиків. На основі отриманих даних здійснюється цільове моделювання, де визначається бажаний рівень захищеності, що має бути повністю узгоджений зі стратегічними цілями організації.

Наступним кроком є безпосередня розробка комплексної програми дій, яка базується на чітких показниках ефективності (KPI), таких як мінімізація кількості інцидентів, скорочення часу на відновлення систем та забезпечення високого рівня відповідності стандартам (compliance). Етап впровадження та моніторингу забезпечує не лише технічну інтеграцію рішень, а й їхнє вкорінення в організаційну культуру через механізми регулярного аудиту. Завершує цей цикл етап корекції, що гарантує постійне оновлення стратегії відповідно до динамічних змін у технологіях та нормативному регулюванні.

Такий підхід забезпечує не лише захист, а й створення конкурентної переваги через підвищення довіри стейкхолдерів і стійкості бізнесу.

Теоретико-методологічні засади формування ефективної стратегії управління безпекою бізнес-систем ґрунтуються на системному, ризик-орієнтованому та інтегративному підходах, що поєднують класичні теорії економічної безпеки з сучасними фреймворками NIST CSF та ISO 27001, доповненими принципами Zero Trust та цифровими технологіями. Лише за таких умов стратегія стає не витратною статтею, а драйвером стійкого розвитку підприємства в умовах цифрової трансформації.

У сучасних умовах цифрової трансформації підходи до захисту бізнес-систем пройшли шлях від статичних бар'єрів до динамічних інтелектуальних систем. Історично першою була традиційна (периметрова) модель безпеки, відома як принцип «замок і рів». Її основна логіка базувалася на створенні жорсткого кордону навколо внутрішньої мережі організації: все, що всередині – апріорі вважалося довіреним, а все ззовні – ворожим. Однак із розвитком хмарних технологій та віддаленої роботи цей підхід втратив ефективність, оскільки «периметр» як такий перестав існувати, а внутрішні загрози стали не менш небезпечними за зовнішні.

Як відповідь на складність нових викликів з'явився NIST Cybersecurity Framework (версія 2.0), який пропонує гнучкий, ризико-орієнтований підхід. На відміну від жорстких інструкцій, цей фреймворк зосереджений на бізнес-результатах і допомагає керівництву приймати рішення через шість ключових функцій:

управління, ідентифікація, захист, виявлення, реагування та відновлення. Це робить його ідеальним інструментом для великих корпорацій, що прагнуть інтегрувати кібербезпеку в загальну бізнес-стратегію.

Паралельно з цим, міжнародний стандарт ISO/IEC 27001:2022 залишається «золотим стандартом» системного управління. Його оновлена версія враховує сучасні реалії цифровізації, зміщуючи акцент на інформаційну безпеку, кібербезпеку та захист конфіденційності. На відміну від технічних моделей, ISO – це передусім про процеси, аудит та чітку відповідність вимогам, що є критично важливим для компаній, які працюють на глобальних ринках і потребують офіційного підтвердження своєї надійності.

Вершиною сучасної архітектури безпеки стала модель Zero Trust Architecture (ZTA), що базується на рекомендаціях NIST SP 800-207. Вона повністю відкидає застарілу ідею «довіреної мережі» і впроваджує принцип «ніколи не довіряй, завжди перевіряй». У цій моделі кожен суб'єкт, пристрій чи додаток проходить сувору автентифікацію перед кожним сеансом доступу до ресурсів, незалежно від свого місцезнаходження. Такий підхід забезпечує максимальну стійкість систем у розмитому цифровому середовищі, роблячи безпеку невід'ємною частиною будь-якої транзакції чи процесу.

Вибір між цими стратегіями сьогодні не є взаємовиключним – найуспішніші організації інтегрують системність ISO, гнучкість NIST та сувору логіку Zero Trust для побудови по-справжньому життєздатної бізнес-системи.

Таблиця 1

Порівняння стратегій управління безпекою бізнес-систем в умовах цифрової трансформації

Критерій	Традиційна (периметрова) модель	NIST CSF 2.0	ISO/IEC 27001:2022	Zero Trust Architecture
Основний принцип	«Довіряй всьому всередині периметра»	Гнучке risk-based управління (6 функцій: Govern, Identify, Protect, Detect, Respond, Recover)	Створення та підтримка ISMS (системи управління інформаційною безпекою)	«Never trust, always verify» – постійна перевірка
Фокус	Захист периметра (firewall, VPN)	Комплексне управління ризиками кібербезпеки	Політики, процедури, контроль та сертифікація	Ідентифікація, мікросегментація, безперервна верифікація доступу
Сертифікація / Аудит	Ні (внутрішній контроль)	Ні (добровільна самооцінка зрілості)	Так (зовнішній аудит, 3-річний сертифікат)	Ні (філософія + архітектура, можна інтегрувати)
Гнучкість та адаптивність	Низька (погано працює в хмарі та гібридному середовищі)	Висока (підходить для будь-якого розміру бізнесу)	Середня (вимагає оновлення політик)	Висока (ідеально для cloud, remote, IoT)
Ресурси для впровадження	Середні	Низькі–середні (фазовий підхід)	Високі (документація, аудит)	Високі (спеціалізовані навички, інструменти)
Підходність для цифрової трансформації	Низька (застаріла для сучасних загроз)	Висока (добре масштабується)	Висока (для компаній, які потребують довіри партнерів)	Найвища (створена саме для цифрового світу)
Переваги	Простота на початковому етапі	Гнучкість, безкоштовні рекомендації, швидке впровадження	Міжнародне визнання, підвищення довіри клієнтів	Мінімізація латерального руху атак, стійкість до insider threats
Недоліки	Вразливість після прориву периметра, слабка видимість всередині	Відсутність сертифікації	Дорого та ресурсоємно, менш технічний	Складність впровадження, потребує зрілої інфраструктури
Найкраще підходить для	Невеликих компаній з простою інфраструктурою	Компаній на етапі цифрової трансформації, критичної інфраструктури	Міжнародних компаній, які потребують compliance та сертифікації	Гібридних і хмарних середовищ, підприємств з високими ризиками
Приклади впровадження	Класичні корпоративні мережі до 2015–2020 рр.	Багато американських та глобальних компаній (критична інфраструктура)	Компанії, що працюють з ЄС, GDPR, міжнародними партнерами	Cimpress, сучасні tech-компанії, державні структури США

Джерело: узагальнено авторами.

Сучасний український досвід цифровізації демонструє унікальне поєднання державних інновацій та гнучкості приватного сектору. Еталоном такого підходу є портал «Дія» та державні цифрові сервіси, де безпека є не додатковою функцією, а фундаментом, закладеним у платформу за принципом Security by Design [18]. В умовах постійних кіберзагроз держава активно застосовує штучний інтелект для моніторингу систем, що дозволяє автоматично виявляти аномалії, протидіяти складним фішинговим атакам, захищати інфраструктуру від масованих DDoS-запитів та блокувати поширення дезінформації. Завдяки

цьому мільйони щоденних звернень громадян обробляються з високим рівнем конфіденційності, що робить українську цифрову екосистему однією з найбільш захищених у світі.

Паралельно з державним сектором, український бізнес (від e-commerce до сервісних компаній) також суттєво трансформував свої підходи до захисту. Сьогодні компанії не просто встановлюють антивіруси, а проводять регулярні стрес-тести та penetration testing для пошуку вразливостей. Обов'язковим стандартом стало впровадження багатофакторної автентифікації (MFA) та ізоляція IoT-пристроїв з регулярним оновленням прошивок. Особлива увага приділяється людському фактору: після хвилі фішингових атак бізнес перейшов до системного навчання співробітників у поєднанні з використанням інтелектуальних інструментів класу SIEM та UEBA для аналізу поведінки користувачів. Провідні IT-компанії, такі як WEZOM, допомагають підприємцям будувати архітектуру безпеки «з нуля», інтегруючи захисні механізми безпосередньо у код майбутніх цифрових продуктів [19].

Окремим критично важливим напрямком є енергетичний сектор та об'єкти критичної інфраструктури. Тут захист зміщується у площину моніторингу промислових систем управління (OT), де штучний інтелект у реальному часі аналізує стан мереж на предмет відхилень від норми. Такий підхід повністю відповідає принципам міжнародного фреймворку NIST CSF, забезпечуючи повний цикл життєстійкості системи: від ідентифікації активів і захисту периметра до миттєвого виявлення, реагування та швидкого відновлення після можливих інцидентів. Це створює надійний щит для найважливіших галузей економіки, перетворюючи кібербезпеку на невід'ємну частину національної стійкості.

Вибір оптимальної стратегії управління безпекою не є універсальним рішенням, а залежить від масштабів організації, її технологічної зрілості та бізнес-цілей. Щоб побудувати життєздатну систему захисту, варто дотримуватися наступних стратегічних орієнтирів.

Якщо організація лише розпочинає свій шлях цифрової трансформації, найбільш раціональним кроком буде використання NIST CSF 2.0. Цей фреймворк слугує гнучким і фінансово доступним фундаментом, який дозволяє швидко оцінити ризики та вибудувати базові процеси захисту без надмірних бюрократичних витрат.

Для компаній, що виходять на міжнародні ринки або прагнуть суттєво підвищити рівень довіри з боку клієнтів та партнерів, пріоритетом має стати впровадження ISO 27001. Отримання офіційного сертифіката не лише впорядковує внутрішню систему управління інформаційною безпекою, а й стає потужною конкурентною перевагою під час тендерів та укладання міжнародних контрактів.

У випадках, коли бізнес-процеси вже глибоко інтегровані у хмарне або гібридне середовище, критично важливим є перехід до моделі Zero Trust. Це найефективніший підхід станом на 2026 р., оскільки він забезпечує безперервну верифікацію кожного доступу та надійно захищає дані в умовах розмитого цифрового периметра.

Проте для досягнення максимальної стійкості найбільш оптимальним є комбінований підхід. Він передбачає використання NIST CSF як фундаменту для управління ризиками, впровадження ISO 27001 для створення формальної та визнаної системи менеджменту, а також поступову інтеграцію технічних елементів Zero Trust у саму архітектуру цифрової платформи. Саме такий синтез дозволяє поєднати управлінську чіткість, міжнародні стандарти та передовий технічний захист.

Таким чином, в умовах цифрової трансформації традиційна модель вже не забезпечує достатнього рівня захисту. Найефективніші стратегії – це ризико-орієнтовані та адаптивні (NIST + Zero Trust), а ISO 27001 додає формальну дисципліну та зовнішнє підтвердження.

Висновки. Традиційна периметрова модель «замок і рів» остаточно втратила актуальність. На зміну їй прийшла концепція Zero Trust (нульової довіри), яка відповідає реаліям розмитих кордонів цифрової організації та гібридних середовищ, де кожен суб'єкт потребує безперервної верифікації.

Найбільшу ефективність демонструє інтегративний підхід. Використання гнучкості NIST CSF 2.0 для оперативного управління ризиками, системності ISO/IEC 27001 для формалізації процесів та архітектурних принципів Zero Trust дозволяє побудувати емерджентну систему захисту, здатну не лише протидіяти загрозам, а й забезпечувати розвиток бізнесу.

Штучний інтелект, аналіз Big Data та автоматизований моніторинг у реальному часі перетворюють безпеку з реактивної («відповідь на інцидент») на предиктивну («прогнозування та запобігання»). Це підтверджується успішним українським досвідом (зокрема, порталу «Дія» та енергетичного сектору), де принцип Security by Design став ключовим для національної стійкості.

Ефективна стратегія безпеки сьогодні – це не витратна стаття бюджету, а конкурентна перевага. Вона інтегрується в організаційну культуру, базується на чітких KPI та забезпечує довіру стейкхолдерів, що є критичним для капіталізації бізнесу в цифрову епоху.

Література:

1. Hammer, M., & Champy, J. (1993). *Reengineering the Corporation: A Manifesto for Business Revolution*. HarperBusiness, 271.

2. Davenport, T. H. (1993). *Process Innovation: Reengineering work through information technology*. Harvard Business School Press.

3. Porter, M. E. (1985). *Competitive Advantage: Creating and Sustaining Superior Performance*. Free Press.

4. Kaplan, R. S., & Norton, D. P. (1996). *The Balanced Scorecard: Translating Strategy into Action*. Harvard Business School Press.

5. Vial, G. (2019). Understanding digital transformation: A review and a research agenda. *The Journal of Strategic Information Systems*, *28*(2), 118–144. doi.org

6. Brynjolfsson, E., & McAfee, A. (2014). *The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies*. W. W. Norton & Company.

7. von Bertalanffy, L. (1968). *General System Theory: Foundations, Development, Applications*. George Braziller.

8. Kraus, S., Jones, P., Kailer, N., Weinmann, A., Chaparro-Banegas, N., & Roig-Tierno, N. (2021). Digital transformation and entrepreneurship: A systematic literature review. *Journal of Business Research*, 123, 1–15. https://doi.org/10.1177/21582440211047576

9. National Institute of Standards and Technology. (2024). *NIST Cybersecurity Framework (CSF) 2.0*. U.S. Department of Commerce.

10. National Institute of Standards and Technology. (2020). *Zero Trust Architecture* (NIST Special Publication 800-207). U.S. Department of Commerce.

11. International Organization for Standardization. (2022). *Information Security, Cybersecurity and Privacy Protection – Information Security Management Systems – Requirements* (ISO/IEC Standard No. 27001:2022).

12. Mell, P., & Grance, T. (2011). *The NIST Definition of Cloud Computing* (NIST Special Publication 800-145). National Institute of Standards and Technology.

13. Stallings, W. (2018). *Effective Cybersecurity: A Guide to Using Best Practices and Standards*. Addison-Wesley.

14. Kim, D., & Solomon, M. (2021). *Fundamentals of Information Systems Security* (4th ed.). Jones & Bartlett Learning.

15. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero Trust Architecture* (NIST Special Publication 800-207). National Institute of Standards and Technology. doi.org

16. European Union Agency for Cybersecurity (ENISA). (2022). *Cybersecurity and Resilience of Smart Systems*. ENISA.

17. Gartner. (2023). *Top Security and Risk Management Trends*. Gartner Research.

18. Міністерство цифрової трансформації України. (2023). Українські практики цифровізації: портал Дія. <https://thedigital.gov.ua/>. (2026, квітень, 27).

Ministerstvo tsyfrovoyi transformatsiyi Ukrayiny [Ministry of Digital Transformation of Ukraine]. (2023). *Ukrainski praktyky tsyfrovizatsii: portal Diia* [Ukrainian digitalization practices: Diia portal].. <https://thedigital.gov.ua/>. (2026, April, 27). [in Ukrainian].

19. WEZOM. (2024). *Cybersecurity solutions and digital transformation practices*. <https://wezom.com.ua/ua>. (2026, April, 27).