lemy i perspektyvy rozvytku pidpryiemnytstva, no. 2 (2021): 116-127.
DOI: https://doi.org/10.30977/PPB.2226-8820.2021.27.116

Mendela, I. Ya. "Planuvannia innovatsiinykh stratehii pidpryiemstvamy hotelnoho biznesu" [Planning Innovation Strategies by Hotel Businesses]. *Aktualni problemy rozvytku ekonomiky rehionu*, no. 9 (2013): 125-129.

Rumiantseva, I. B., and Mendela, I. Ya. "Hotelna industriia Ukrainy v umovakh voiennoho chasu" [Hotel Industry of Ukraine in Wartime Conditions]. *Problemy suchasnykh transformatsii*, no. 11 (2024).
DOI: https://doi.org/10.54929/2786-5738-2024-11-12-02

"Stymuliuvannia popytu: v chomu osoblyvosti ta yak zdiisniuvaty" [Demand Stimulation: What Are the Features and How to Implement It]. *Fractus*. https://fractus.com.ua/uk/blog/stimuljuvannya-popitu-v-chomu-osoblivosti-ta-yak-zdijsnjuvati/

Seheda, I. V. "Formuvannia stratehii upravlinnia hotelnym hospodarstvom rehionu" [Formation of a Regional Hotel Management Strategy]. *Modeliuvannia rehionalnoi ekonomiky*, no. 1 (2017): 151-160.

Sydoruk, S. V. "Pryntsypy terytorialnoi orhanizatsii hotelnykh posluh" [The Principles of the Territorial Organization of Hotel Services]. *Ekonomika. Upravlinnia. Innovatsii*. 2011. https://tourlib.net/statti_ukr/sydoruk.htm

"Turystychna diialnist v Ukraini u 2020 rotsi" [Tourism Activity in Ukraine in 2020]. *Derzhavna sluzhba statystyky Ukrainy*. http://ukrstat.gov.ua/

"Turystychna diialnist v Ukraini u 2021 rotsi" [Tourism Activity in Ukraine in 2021]. *Derzhavna sluzhba statystyky Ukrainy*. http://ukrstat.gov.ua/

УДК 658.012.32
JEL: D80; L86; M15
DOI: https://doi.org/10.32983/2222-4459-2025-5-481-488

КІБЕРБЕЗПЕКА ЯК КРИТИЧНИЙ ФАКТОР ЦИФРОВОЇ ТРАНСФОРМАЦІЇ БІЗНЕСУ В ПЕРІОД НЕСТАБІЛЬНОСТІ

©2025 **ВАСИЛЬЄВА М. О., ВАСИЛЬЄВ А. С.**

УДК 658.012.32
JEL: D80; L86; M15

Васильєва М. О., Васильєв А. С. Кібербезпека як критичний фактор цифрової трансформації бізнесу в період нестабільності

Мета статті полягає у всебічному дослідженні ролі кібербезпеки як критичного чинника успішної цифрової трансформації бізнесу в умовах економічної та соціальної нестабільності. У межах роботи проаналізовано основні загрози інформаційній безпеці, що виникають у процесі цифровізації, обґрунтовано необхідність інтеграції заходів кіберзахисту в стратегічне управління підприємствами, а також визначено ключові інструменти та підходи до мінімізації кіберризиків у контексті забезпечення стійкого розвитку бізнесу. У статті проведено аналіз значення кібербезпеки як критичного елемента успішної цифрової трансформації бізнесу в умовах економічної та політичної нестабільності. Розглянуто основні виклики, що виникають під час упровадження цифрових технологій, зокрема зростання кіберзагроз, які ставлять під загрозу стійкість і безперервність діяльності підприємств. Особлива увага приділена необхідності інтеграції заходів кіберзахисту в стратегічне управління компанією для забезпечення її конкурентоспроможності та довгострокового розвитку. Запропоновано комплекс практичних рекомендацій, спрямованих на підвищення рівня захищеності інформаційних систем і зміцнення бізнес-стійкості в умовах цифрової економіки. У статті описано основні типи кібератак, а також проаналізовано їх потенційні наслідки для критичних елементів інфраструктури цифрової економіки. Наведено алгоритм керування ризиками кібербезпеки. У контексті неможливості забезпечення абсолютного захисту цифрової економіки від кіберзагроз особливого значення набуває забезпечення стійкості соціотехнічних систем. Розглядаючи питання забезпечення кіберстійкості формованої цифрової економіки України, проаналізовано основні види системно-руйнівних кібератак і висвітлено заходи, спрямовані на протидію таким загрозам. У статті зроблено висновок, що досягнення незалежності та високого рівня стійкості національної інформаційної інфраструктури можливе лише за умов розвитку відповідного науково-технологічного потенціалу та підготовки нового покоління фахівців у сфері наукових і технічних дисциплін.

Ключові слова: *кібербезпека, цифрова трансформація, бізнес-моделі, нестабільність, інформаційні загрози, стратегічне управління, стійкість підприємства.*

Рис.: *1.* ***Бібл.:*** *13.*

Васильєва Марія Олександрівна *– старший викладач кафедри економіки та менеджменту, Навчально-науковий інститут «Українська інженерно-педагогічна академія» Харківського національного університету імені В. Н. Каразіна (вул. Університетська, 16, Харків, 61003, Україна)*

E-mail: *maria.vasylieva@karazin.ua*

ORCID: *https://orcid.org/0000-0001-9119-2746*

Researcher ID: *https://www.webofscience.com/wos/author/record/HPC-9596-2023*

Васильєв Антон Сергійович *– здобувач, Навчально-науковий інститут «Українська інженерно-педагогічна академія» Харківського національного університету імені В. Н. Каразіна (вул. Університетська, 16, Харків, 61003, Україна)*

E-mail: *tolst.top@gmail.com*

ORCID: *https://orcid.org/0009-0002-9605-4574*

UDC 658.012.32
JEL: D80; L86; M15

Vasylieva M. O., Vasyliev A. S. Cybersecurity as a Critical Factor in the Digital Transformation of Business in Times of Instability

The aim of the article is to comprehensively study the role of cybersecurity as a critical factor in the successful digital transformation of business in conditions of economic and social instability. The work analyzes the main threats to information security that arise in the process of digitalization, substantiates the need to integrate cyber security measures into the strategic management of enterprises, and identifies key tools and approaches to minimizing cyber risks in the context of ensuring sustainable business development. The article analyzes the importance of cybersecurity as a critical element of the successful digital transformation of business in conditions of economic and political instability. The main challenges that arise during the implementation of digital technologies are considered, in particular, the growth of cyber threats that threaten the stability and continuity of enterprise operations. Particular attention is paid to the need to integrate cyber security measures into the strategic management of a company to ensure its competitiveness and long-term development. A set of practical recommendations aimed at increasing the level of security of information systems and strengthening business resilience in the digital economy is proposed. The article describes the main types of cyberattacks, and also analyzes their potential consequences for critical elements of the digital economy infrastructure. An algorithm for managing cybersecurity risks is presented. In the context of the impossibility of ensuring absolute protection of the digital economy from cyberthreats, ensuring the resilience of socio-technical systems is of particular importance. Considering the issue of ensuring the cyber resilience of the emerging digital economy of Ukraine, the main types of system-destructive cyberattacks are analyzed and measures aimed at countering such threats are highlighted. The article concludes that achieving independence and a high level of resilience of the national information infrastructure is possible only under the conditions of developing the appropriate scientific and technological potential and training a new generation of specialists in the field of scientific and technical disciplines.

Keywords: *cybersecurity, digital transformation, business models, instability, information threats, strategic management, enterprise resilience.*
Fig.: *1.* ***Bibl.:*** *13.*

Vasylieva Mariia O. *– Senior Lecturer of the Department of Economics and Management, Educational and Scientific Institute "Ukrainian Engineering and Pedagogical Academy" of V. N. Karazin Kharkov National University (16 Universytetska Str., Kharkiv, 61003, Ukraine)*
E-mail: *maria.vasylieva@karazin.ua*
ORCID: *https://orcid.org/0000-0001-9119-2746*
Researcher ID: *https://www.webofscience.com/wos/author/record/HPC-9596-2023*
Vasyliev Anton S. *– Applicant, Educational and Scientific Institute "Ukrainian Engineering and Pedagogical Academy" of V. N. Karazin Kharkov National University (16 Universytetska Str., Kharkiv, 61003, Ukraine)*
E-mail: *tolst.top@gmail.com*
ORCID: *https://orcid.org/0009-0002-9605-4574*

Сучасний розвиток цифрової трансформації бізнесу суттєво підвищує рівень залежності підприємств від інформаційно-комунікаційних технологій, що водночас обумовлює зростання їхньої чутливості до кібернетичних загроз. У період економічної та соціальної нестабільності проблема кібербезпеки набуває особливої актуальності, оскільки будь-які порушення в інформаційних системах можуть спричинити серйозні фінансові втрати, зниження довіри споживачів, а також погіршення репутації компаній. Водночас конкурентна боротьба на ринку змушує підприємства активно впроваджувати цифрові рішення, що безпосередньо підвищує ризики кіберінцидентів. Недостатній рівень захисту інформаційних ресурсів може нівелювати потенційні переваги цифровізації та призвести до істотних стратегічних загроз для бізнесу. У цьому контексті кібербезпека виступає не просто технічною функцією, а критично важливою складовою стратегічного управління підприємствами. Таким чином, дослідження питання інтеграції кібербезпеки в процес цифрової трансформації є надзвичайно важливим для забезпечення сталого розвитку бізнесу в умовах нестабільності та невизначеності глобального середовища.

Проблематика кібербезпеки в умовах цифрової трансформації підприємств упродовж останніх років стала об'єктом пильної уваги як науковців, так і практиків. У роботах українських дослідників (зокрема, Кіндзерського Ю. В. [3], Краус К. М., Краус Н. М., Штепи О. В. [5], Лісової Р. М. [6] Мехеда А. М., Варналія З. С. [7], Піжук О. І. [9], Савченка В., Маклюка О. [10]) наголошується, що цифровізація водночас відкриває нові можливості для розвитку бізнесу та підвищує рівень кіберризиків, які можуть негативно впливати на ефективність функціонування підприємств. Питання впливу цифровізації на трансформацію бізнесу розглядаються в роботах низки науковців, серед яких Буяк Л. А. [1], Корнага О. І. [4], Піддубний Є. В. [8], Чубук Л. П., Яценко О. В., Овандер Н. Л. [11], Яковенко Я. Ю., Білик М. Ю., Олійник Є. В. [12].

Вчені акцентують, що розширення обсягів даних, які обробляються, впровадження хмарних технологій та використання Інтернету речей збільшують кількість потенційних векторів атак, що потребує створення комплексних стратегій кіберзахисту. У багатьох дослідженнях підкреслюється, що кібербезпека не повинна обмежуватися виключно сферою діяльності ІТ-підрозділів, а має розглядатися як складова стратегічного управління підприємством, інтегрована в усі бізнес-процеси. Наукові праці містять різноманітні підходи до формування політики інформаційної безпеки, методології управління кіберризиками та

моделі оцінки фінансових наслідків кіберінцидентів для підприємств.

Разом із тим, попри зростаючу кількість досліджень, залишається недостатньо висвітленим аспект інтеграції заходів кібербезпеки в процес стратегічного планування цифрової трансформації в умовах економічної та політичної нестабільності, коли посилюються ризики та невизначеність на ринку. Це вказує на необхідність подальших досліджень у напрямі розроблення комплексного підходу до кіберзахисту як важливого чинника забезпечення стійкості бізнесу в цифровій економіці.

Мета статті полягає в усебічному дослідженні ролі кібербезпеки як критичного чинника успішної цифрової трансформації бізнесу в умовах економічної та соціальної нестабільності. У межах роботи передбачається проаналізувати основні загрози інформаційній безпеці, що виникають у процесі цифровізації, обґрунтувати необхідність інтеграції заходів кіберзахисту в стратегічне управління підприємствами, а також визначити ключові інструменти та підходи до мінімізації кіберризиків у контексті забезпечення стійкого розвитку бізнесу.

Дослідження здійснювалося на основі комплексного підходу, що поєднує теоретичний аналіз, узагальнення сучасних наукових публікацій, систематизацію нормативних документів і емпіричний аналіз практичних кейсів упровадження кібербезпеки в процесі цифрової трансформації бізнесу. На першому етапі було проведено огляд і критичний аналіз наукових джерел, що стосуються взаємозв'язку цифрової трансформації та кібербезпеки, а також сучасних викликів у сфері інформаційної безпеки в умовах економічної та політичної нестабільності. Другий етап передбачав систематизацію нормативно-правових документів і стандартів, зокрема ISO/IEC 27001:2023, що регламентує вимоги та рекомендації щодо забезпечення кібербезпеки в організаціях. Було використано метод порівняльного аналізу для оцінки ефективності різних підходів до інтеграції кібербезпеки в управлінські стратегії. На завершальному етапі проведено синтез отриманих результатів і формулювання практичних рекомендацій, спрямованих на зміцнення кібербезпеки як складової стратегічного управління цифровою трансформацією бізнесу. У дослідженні застосовувалися методи дедукції, індукції, логічного узагальнення та системного підходу для забезпечення цілісного бачення досліджуваної проблеми.

Сучасна економіка дедалі сильніше інтегрується з цифровими технологіями, що трансформують усталені бізнес-моделі та відкривають нові можливості для підприємств. Проте поряд із численними перевагами цифровізація породжує й низку викликів, серед яких особливе місце займає зростання кіберризиків. В умовах нестабільності, спричиненої економічними кризами, геополітичними напруженнями та глобальними викликами, питання забезпечення інформаційної безпеки набуває критичної ваги. Поряд зі збільшенням частоти кібератак, розширенням спектра кіберзагроз і вдосконаленням методів дій зловмисники формують нові загрози для бізнесу, що потребують цілісного підходу до організації системи кіберзахисту.

Фінансові втрати та іміджеві збитки, завдані атаками на інформаційні системи компаній, здатні мати тривалі негативні наслідки. Несанкціонований доступ до конфіденційної інформації, порушення функціонування цифрових платформ і викрадення об'єктів інтелектуальної власності підривають конкурентоспроможність компаній. Особливо ризикованою є ситуація в періоди економічної турбулентності, коли підприємства змушені оптимізувати витрати, а питання кібербезпеки нерідко відходять на другий план, що може призвести до серйозних стратегічних помилок. Неналежний рівень кіберзахисту робить компанії вразливими до атак, спрямованих не лише на фінансові ресурси, а й на критично важливі бізнес-процеси.

Інтеграція кібербезпеки в стратегію цифрової трансформації є ключовою умовою забезпечення стійкого функціонування підприємств. Реалізація багаторівневої системи захисту, що охоплює моніторинг мережевої активності, застосування автоматизованих систем виявлення загроз, шифрування даних і багатофакторну аутентифікацію, сприяє зниженню рівня ризиків. Особливої уваги потребує захист хмарних сервісів, які стали невіддільною складовою цифрових екосистем компаній [9].

Ключовим елементом комплексної системи кібербезпеки залишається людський чинник, оскільки навіть найсучасніші технологічні рішення не можуть забезпечити належного рівня захисту без високої компетентності персоналу. Формування корпоративної культури інформаційної безпеки, регулярне підвищення кваліфікації працівників, а також проведення тестувань для виявлення вразливостей інформаційної інфраструктури є важливими складовими захисту підприємства. Окрім цього, необхідною умовою є розробка та впровадження планів реагування на кіберінциденти, що дозволяє мінімізувати негативні наслідки атак і забезпечити швидке відновлення роботи цифрових систем.

У сучасних умовах кібербезпека виходить за межі суто технічного аспекту, перетворюючись на стратегічний напрям розвитку компаній, що визна-

чає їхню здатність до адаптації, ефективної діяльності та збереження довіри з боку клієнтів і партнерів. Реалізація комплексних заходів кіберзахисту не лише дозволяє попереджати кіберзагрози, але й формує підґрунтя для сталого розвитку бізнесу в умовах цифрової економіки [3]. Таким чином, кібербезпека має стати невід'ємною складовою загальної стратегії розвитку підприємств, які прагнуть не лише зберегти свої конкурентні позиції, а й забезпечити довготривалий успіх у глобалізованому цифровому середовищі.

Сучасні компанії змушені функціонувати в умовах зростаючої економічної нестабільності, що зумовлена дією фінансових криз, геополітичної напруженості, технологічних змін і трансформацією споживчих пріоритетів. За таких обставин традиційні бізнес-моделі поступово втрачають свою результативність, що стимулює потребу в упровадженні більш гнучких і адаптивних управлінських підходів. Гнучкість, швидкість ухвалення управлінських рішень та інтеграція новітніх технологій виступають визначальними факторами підтримання конкурентоспроможності підприємств у динамічному ринковому середовищі.

Фінансова гнучкість підприємства також є важливою складовою його стійкості. Зокрема, застосування антикризових фінансових механізмів, залучення нетрадиційних джерел капіталу (наприклад, венчурного фінансування, краудфандингу), а також диверсифікація джерел доходів дають змогу знизити залежність від макроекономічних коливань. Інноваційні підходи до побудови бізнес-процесів, включно з використанням аутсорсингу й автоматизацією операційної діяльності, сприяють підвищенню ефективності роботи підприємства та оптимізації витрат.

Крім того, розвиток омніканальних систем продажу, які поєднують електронну комерцію, соціальні мережі та маркетплейси, забезпечує розширення каналів збуту та підтримання стабільності комерційної діяльності в умовах економічних коливань. Важливим чинником є також запровадження гнучких моделей зайнятості, таких як дистанційна робота, аутстафінг і фріланс, що дозволяє підприємствам не лише оптимізувати операційні витрати, а й підвищити мобільність і адаптивність кадрових ресурсів.

Для забезпечення довготривалої життєздатності підприємства необхідно впроваджувати інструменти, що підвищують його стійкість до зовнішніх загроз. Одним із таких інструментів виступає диверсифікація продуктового портфеля, яка передбачає розширення номенклатури товарів і послуг з метою зменшення ризиків, пов'язаних із коливаннями споживчого попиту [1].

Адаптація бізнес-моделі до динамічних умов ринкового середовища виступає визначальним чинником забезпечення стійкого розвитку підприємства в довгостроковій перспективі. Застосування цифрових технологій, фінансової адаптивності, інноваційних управлінських практик та ефективних механізмів управління ризиками сприяє зміцненню конкурентних позицій організацій. Реалізація стратегій гнучкого менеджменту забезпечує своєчасне реагування підприємства на зміни зовнішнього середовища, що стає ключовою передумовою його успішної діяльності в умовах ринкової нестабільності [8].

Кіберзагрози мають складну багаторівневу природу, охоплюючи як технічні загрози (атаки на IT-інфраструктуру, витоки конфіденційної інформації, поширення шкідливих програм), так і загрози, пов'язані з людським фактором (фішингові атаки, соціальна інженерія, порушення політик безпеки через недбалість працівників). Ефективне управління кібербезпекою має здійснюватися шляхом інтеграції її інструментарію в загальну стратегію розвитку підприємства. Основними елементами такої інтеграції є: формування політик інформаційної безпеки, впровадження багаторівневих систем захисту, проведення постійного моніторингу та аудиту інформаційної інфраструктури, систематичне підвищення кваліфікації співробітників, а також розроблення та реалізація планів реагування на кіберінциденти.

Крім впровадження технічних засобів захисту, важливою складовою забезпечення кібербезпеки є формування корпоративної культури інформаційної безпеки. Вона передбачає систематичне підвищення обізнаності працівників щодо потенційних кіберзагроз, розвиток навичок безпечної взаємодії з інформаційними системами, а також формування відповідального підходу до захисту даних на всіх рівнях управління підприємством.

Цифрова трансформація впродовж останніх п'яти років є одним із найпотужніших трендів розвитку бізнесу, тенденція зберігається і на перспективу. У сучасних публікаціях і під час обговорень на IT-форумах акцент часто робиться на організаційних проблемах та обмеженнях, що виникають через використання застарілих технологій, що справді актуально для багатьох компаній. Проте більшість експертів з інформаційної безпеки вважають, що саме питання безпеки є основними бар'єрами на шляху впровадження цифрової трансформації [12].

Керівники підрозділів інформаційної безпеки надають пріоритетну увагу двом основним джерелам ризику: зовнішнім загрозам і внутрішнім уразливостям. Більшість експертів у сфері інформацій-

ної безпеки оцінюють зростання поліморфних атак і загроз, що постійно змінюються з метою уникнення виявлення, як «доволі серйозну» або навіть «критично серйозну» проблему [5]. Обидва ці фактори потенційно сприятимуть зростанню кіберризиків у міру ускладнення поверхні атак, що супроводжує процес цифрової трансформації в організаціях.

З огляду на критичність зазначених загроз, доцільно надати детальне пояснення їхньої природи. Поліморфізм як метод кібернападу полягає в динамічному формуванні коду шкідливого програмного забезпечення безпосередньо під час його виконання. Водночас сама процедура генерації цього коду також зазнає змін під час кожного нового зараження, що ускладнює виявлення. Часто для цього використовують техніку модифікації коду шляхом додавання інструкцій, що не змінюють логіку виконання програми. Постійні модифікації шкідливого коду унеможливлюють створення універсальної сигнатури для виявлення конкретного зразка шкідливого ПЗ. У відповідь на це фахівці з кібербезпеки активно застосовують такі методи протидії, як евристичний аналіз із використанням технологій штучного інтелекту, а також емуляцію, що дозволяють ефективніше виявляти поліморфні загрози навіть за умов їхньої постійної видозміни [5].

Ще однією серйозною проблемою, з якою стикаються сучасні підприємства, є обмежена видимість усіх зон і процесів ІКТ-систем для фахівців підрозділів кібербезпеки, що обумовлено дедалі більшою складністю обчислювальної інфраструктури, притаманної цифровій трансформації [4]. Зазначене питання часто є наслідком наявності застарілих, неінтегрованих у корпоративну мережу організації багатофункціональних систем і програмних продуктів, що раніше використовувалися, зокрема, в оборонній промисловості.

Для ефективного забезпечення безпеки складних, високо розподілених ІТ-середовищ, які охоплюють віддалені офіси, корпоративні центри обробки даних (ЦОД) і гібридні хмарні рішення, служби безпеки мають забезпечувати максимальну видимість інфраструктури. Це є критично необхідною умовою для своєчасного виявлення аномальної діяльності та оперативної нейтралізації потенційних загроз [7].

Цифрова трансформація водночас посилила фокус на захисті конфіденційності даних і підвищила вимоги до її забезпечення. З розвитком більш витончених і руйнівних кібератак регуляторні органи запроваджують дедалі суворіші нормативно-правові вимоги та керівні принципи щодо захисту персональної ідентифікаційної інформації. Як наслідок, організаціям необхідно постійно дотримуватись вимог комплаєнсу (відповідності внутрішнім і зовнішнім стандартам і нормам, англ. *compliance*) і впроваджувати кращі практики, сертифіковані продукти та професійно підготовлених спеціалістів, щоб гарантувати належний рівень управління ризиками [10].

Варто зазначити, що навіть до початку цифрової трансформації системи інформаційної безпеки підприємств, як правило, складалися з кількох розрізнених сховищ даних, локальних сервісів і були розгорнуті на різних хмарних платформах із використанням неоднорідних інструментів захисту [6].

Стратегія цифрової трансформації (ЦТ) здатна призвести до формування ще більш складного середовища, яке характеризується зростанням кількості хмарних сервісів, центрів обробки даних (ЦОД) і швидким поширенням пристроїв Інтернету речей (IoT), значна частина яких спочатку не розроблялася з урахуванням вимог кібербезпеки.

Особливий акцент необхідно зробити на управлінні інцидентами інформаційної безпеки на об'єктах критичної інформаційної інфраструктури (КІІ). Ці інциденти можуть включати як цілеспрямовані атаки (англ. – *advanced persistent threat, APT*), так і техногенні катастрофи, фізичне викрадення активів, а також інші загрози. Зі зростанням складності кібератак відповідно ускладнюється й інфраструктура кібербезпеки, що вимагає впровадження більш розвинених засобів захисту.

Незважаючи на прогрес у сфері кіберзахисту, уразливості, що можуть бути усунуті шляхом оновлення програмного забезпечення чи встановлення патчів, залишаються потенційно небезпечними для частини організацій. Хоча майже всі компанії заявляють про підтримання «певного рівня актуальності» оновлень, лише третина повідомляє про те, що їхні системи є «надзвичайно актуальними» з точки зору виправлення вразливостей. Водночас стрімкий прогрес у сфері інтелектуальних систем управління кібербезпекою, зокрема із застосуванням штучного інтелекту, дає підстави сподіватися на поступове зниження цієї вразливості в найближчій перспективі [3].

Управління ризиками у сфері кібербезпеки ґрунтується на положеннях міжнародного стандарту ISO/IEC 27001:2023, який акцентує увагу на специфіці захисту в умовах цифрової трансформації. Зокрема, рекомендації для кінцевих користувачів формують систему поведінкових норм, установлену постачальниками послуг. Вони охоплюють усвідомлення ключових положень політики кібербезпеки застосунків та контенту, розуміння ризиків, що виникають у цифровому середовищі, дотримання принципів захисту персональних даних,

управління власною інформаційною безпекою, а також обов'язок повідомляти відповідні органи про підозрілі дії чи інциденти [13].

У контексті забезпечення кібербезпеки ключовим пріоритетом виступає налагодження ефективної координації між різними учасниками, що формують кіберпростір, оскільки ізольовані дії окремих організацій не здатні забезпечити належного рівня захисту від кіберзагроз. Алгоритм управління ризиками кібербезпеки складається з послідовних етапів (*рис. 1*), кожен з яких має чітко визначені завдання та логіку переходу. Процес управління ризиками передбачає встановлення контексту, оцінювання ризику, обробку ризику, прийняття рішення, а також постійне інформування та моніторинг.

- *аналіз ризику,* який охоплює збирання та систематизацію даних про можливі загрози, вразливості та потенційні наслідки;
- *ідентифікація ризику,* під час якої виявляються джерела ризику, події, що можуть його спричинити, і наслідки для інформаційної безпеки;
- *кількісна оцінка ризику,* що передбачає оцінювання ймовірностей настання ризиків та їхнього впливу на діяльність організації.

На етапі прийнятті рішення щодо результатів оцінювання ризику здійснюється аналіз отриманих результатів. Якщо оцінений рівень ризику є прийнятним, ризик може бути прийнятий без додаткових заходів. Якщо рівень ризику перевищує допустимі межі, необхідно перейти до етапу обробки ризику.

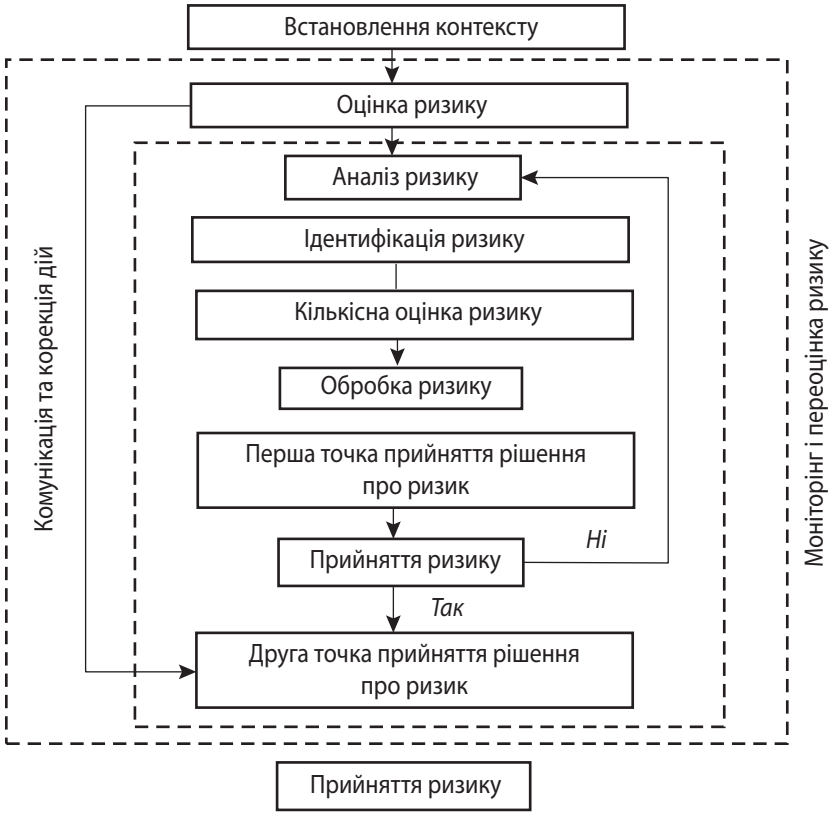

Рис. 1. Алгоритм керування ризиками кібербезпеки

Джерело: сформовано авторами на основі інформаційних джерел [1–14].

На першому етапі формується загальна основа для подальшої роботи з ризиком. Це включає визначення зовнішніх і внутрішніх факторів, що впливають на діяльність організації, ідентифікацію зацікавлених сторін, а також установлення критеріїв прийнятності ризику.

Оцінювання ризику здійснюється шляхом поєднання трьох взаємопов'язаних процесів:

Обробка ризику включає вибір і впровадження заходів для зниження рівня ризику до прийнятного рівня. Це може бути досягнуто шляхом усунення джерел ризику, зменшення ймовірності або наслідків реалізації ризику, передання ризику третім сторонам чи ухвалення залишкового ризику.

Після впровадження заходів обробки проводиться повторна оцінка. Якщо результати є задо-

вільними, ризик приймається. Якщо ні – процес повертається до етапу оцінювання ризику для повторного аналізу й корекції заходів.

Фінальний етап передбачає офіційне погодження на залишковий рівень ризику, який організація готова прийняти відповідно до встановлених критеріїв.

Протягом усього процесу управління ризиками забезпечується постійна комунікація між усіма зацікавленими сторонами для обміну інформацією, координації дій та прийняття рішень.

Управління ризиками є безперервним процесом, що потребує постійного моніторингу та регулярної переоцінки рівня ризику, ефективності заходів і змін у зовнішньому та внутрішньому середовищі.

Цей алгоритм є циклічним і передбачає можливість багаторазового повернення до попередніх етапів для корекції рішень, що забезпечує його гнучкість та адаптивність до змін у сфері кібербезпеки.

Керівні настанови для організацій пропонують комплексний підхід до управління кібербезпекою, що передбачає впровадження та сертифікацію системи управління інформаційною безпекою, створення та використання безпечних ІКТ-продуктів, які пройшли відповідну оцінку, а також проведення тестування, моніторингу мереж і оперативного реагування на інциденти. Важливими аспектами є забезпечення технічної підтримки, постійне оновлення знань про новітні розробки у сфері кібербезпеки, підвищення рівня обізнаності користувачів, контроль дотримання політик безпеки, а також розробка архітектури кіберзахисту, що гарантує прозорість ІТ-інфраструктури й забезпечує централізоване управління. Крім того, особлива увага приділяється формуванню стратегії, яка інтегрує процеси автоматизації робочих процедур і забезпечує обмін аналітичною інформацією про загрози як усередині, так і за межами організації. Що стосується власне забезпечення кібербезпеки, то як пріоритет виокремлено координацію взаємодії між організаціями, що формують кіберпростір, самостійні дії яких не забезпечують ефективного захисту від кіберзагроз.

ВИСНОВКИ

Результати проведеного дослідження свідчать про те, що кібербезпека є визначальним фактором успішної цифрової трансформації бізнесу, особливо в умовах економічної та політичної нестабільності. Забезпечення ефективного захисту інформаційних систем розглядається не лише як завдання технічного характеру, а як комплексна управлінська функція, що потребує інтеграції в загальну стратегію розвитку підприємства. Стрімкий розвиток цифрових технологій супроводжується збільшенням кількості та складності кіберзагроз, що обумовлює необхідність впровадження багаторівневих систем захисту, формування культури інформаційної безпеки на корпоративному рівні, регулярного підвищення кваліфікації співробітників, а також розробки антикризових планів реагування на кіберінциденти. В умовах нестабільного зовнішнього середовища саме комплексний підхід до кібербезпеки дозволяє мінімізувати ризики порушення безперервності бізнес-процесів, забезпечити фінансову стійкість підприємства та підвищити його конкурентні позиції.

Перспективним напрямом подальших досліджень є створення адаптивних моделей кіберзахисту, здатних ефективно функціонувати за умов високої невизначеності та швидких змін у цифровій інфраструктурі. ■

БІБЛІОГРАФІЯ

1. Буяк Л. А. Методи та моделі впливу цифровізації на трансформацію бізнесу. *Підприємництво і торгівля*. 2023. № 39. С. 25–34. DOI: https://doi.org/10.32782/2522-1256-2023-39-03
2. Гринько Т. В., Гвініашвілі Т. З., Калиберда М. С. Стратегічне управління підприємством в умовах цифрової економіки. *Економіка та суспільство*. 2023. Вип. 50. DOI: https://doi.org/10.32782/2524-0072/2023-50-71
3. Кіндзерський Ю. В. Кібербезпека і становлення цифрової економіки: проблеми взаємозв'язку. *Економічний вісник Національного гірничого університету*. 2020. № 3. С. 18–26. DOI: https://doi.org/10.33271/ebdut/71.018
4. Корнага О. І. Характеристика цифрової трансформації економіки. *Economic Synergy*. 2024. Вип. 1. С. 189–199. DOI: https://doi.org/10.53920/ES-2024-1-14
5. Краус К. М., Краус Н. М., Штепа О. В. Цифрова трансформація кібербезпеки на мікрорівні в умовах воєнного стану. *Innovation and Sustainability*. 2022. № 3. С. 26–37. DOI: https://doi.org/10.31649/ins.2022.3.26.37
6. Лісова Р. М. Вплив діджиталізації на бізнес-моделі: етапи та інструменти цифрової трансформації. *Науковий вісник Ужгородського національного університету. Серія «Міжнародні економічні відносини та світове господарство»*. 2019. Вип. 24. Ч. 2. С. 114–118. URL: http://www.visnyk-econom.uzhnu.uz.ua/archive/24_2_2019ua/24.pdf
7. Мехед А. М., Варналій З. С. Фінансова безпека підприємств в умовах цифрової економіки. *Вісник Університету банківської справи*. 2021. № 3. С. 55–61. DOI: https://doi.org/10.18371/2221-755x3(42)2021253524

8. Піддубний Є. В. Вплив цифрової трансформації української економіки та бізнес-моделі підприємств. *Наукові праці Міжрегіональної Академії управління персоналом. Серія «Економічні науки»*. 2023. Вип. 5. С. 45–50. DOI: https://doi.org/10.32689/2523-4536/72-7
9. Піжук О. І. Кібербезпека як фактор прискорення цифрової трансформації економіки України. *Інтернаука. Серія «Економічні науки»*. 2020. № 10. С. 67–73. DOI: https://doi.org/10.25313/2520-2294-2020-10-6409
10. Савченко В., Маклюк О. Кібербезпека як фактор ефективності функціонування закладів вищої освіти. *Економіка та суспільство*. 2024. Вип. 60. DOI: https://doi.org/10.32782/2524-0072/2024-60-24
11. Чубук Л. П., Яценко О. В., Овандер Н. Л. Вплив цифрової економіки на зміну моделей бізнесу та фінансового управління: інституціоналізація цифрових трансформацій. *Економіка. Менеджмент. Бізнес*. 2024. № 1. С. 58–64. DOI: https://doi.org/10.31673/2415-8089.2024.010008
12. Яковенко Я. Ю., Білик М. Ю., Олійник Є. В. Цифрова трансформація бізнес-структур: стратегічні орієнтири в епоху інновацій та технологічних змін. *Економічний простір*. 2024. № 190. С. 355–360. DOI: https://doi.org 10.32782/2224-6282/190-63
13. ДСТУ ISO/IEC 27001:2023. Інформаційні технології. Методи та засоби забезпечення безпеки. Системи управління інформаційною безпекою. Вимоги. Київ : ДП «УкрНДНЦ», 2023.

REFERENCES

Buiak, L. A. "Metody ta modeli vplyvu tsyfrovizatsii na transformatsiiu biznesu" [Methods and Models of the Influence of Digitalization on Business Transformation]. *Pidpryiemnytstvo i torhivlia*, no. 39 (2023): 25-34. DOI: https://doi.org/10.32782/2522-1256-2023-39-03

Chubuk, L. P., Yatsenko, O. V., and Ovander, N. L. "Vplyv tsyfrovoi ekonomiky na zminu modelei biznesu ta finansovoho upravlinnia: instytutsionalizatsiia tsyfrovykh transformatsii" [Impact of Digital Economy on Business Models and Financial Management: Institutionalization of Digital Transformations]. *Ekonomika. Menedzhment. Biznes*, no. 1 (2024): 58-64. DOI: https://doi.org/10.31673/2415-8089.2024.010008

DSTU ISO/IEC 27001:2023. Informatsiini tekhnolohii. Metody ta zasoby zabezpechennia bezpeky. Systemy upravlinnia informatsiinoiu bezpekoiu. Vymohy [DSTU ISO/IEC 27001:2023. Information Technology. Methods and Means of Ensuring Security. Information Security Management Systems. Requirements]. Kyiv: DP «UkrNDNTs», 2023.

Hrynko, T. V., Hviniashvili, T. Z., and Kaliberda, M. S. "Stratehichne upravlinnia pidpryiemstvom v umovakh tsyfrovoi ekonomiky" [Strategic Management of the Enterprise in the Conditions of the Digital Economy]. *Ekonomika ta suspilstvo*, no. 50 (2023). DOI: https://doi.org/10.32782/2524-0072/2023-50-71

Kindzerskyi, Yu. V. "Kiberbezpeka i stanovlennia tsyfrovoi ekonomiky: problemy vzaiemozviazku" [Cybersecurity and Becoming of the Digital Economy: Problems of Interconnection]. *Ekonomichnyi visnyk Natsionalnoho hirnychoho universytetu*, no. 3 (2020): 18-26. DOI: https://doi.org/10.33271/ebdut/71.018

Kornaha, O. I. "Kharakterystyka tsyfrovoi transformatsii ekonomiky" [Characteristics of Digital Transformation of Economy]. *Economic Synergy*, no. 1 (2024): 189-199. DOI: https://doi.org/10.53920/ES-2024-1-14

Kraus, K. M., Kraus, N. M., and Shtepa, O. V. "Tsyfrova transformatsiia kiberbezpeky na mikrorivni v umovakh voiennoho stanu" [Digital Transformation of Cyber Security at the Micro-Level under Martial Status]. *Innovation and Sustainability*, no. 3 (2022): 26-37. DOI: https://doi.org/10.31649/ins.2022.3.26.37

Lisova, R. M. "Vplyv didzhytalizatsii na biznes-modeli: etapy ta instrumenty tsyfrovoi transformatsii" [The Impact of Digitalization on Business Models: Stages and Tools of Digital Transformation]. *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Seriia «Mizhnarodni ekonomichni vidnosyny ta svitove hospodarstvo»*. 2019. http://www.visnyk-econom.uzhnu.uz.ua/archive/24_2_2019ua/24.pdf

Mekhed, A. M., and Varnalii, Z. S. "Finansova bezpeka pidpryiemstv v umovakh tsyfrovoi ekonomiky" [Financial Security of Enterprises in the Digital Economy]. *Visnyk Universytetu bankivskoi spravy*, no. 3 (2021): 55-61. DOI: https://doi.org/10.18371/2221-755x3(42)2021253524

Piddubnyi, Ye. V. "Vplyv tsyfrovoi transformatsii ukrainskoi ekonomiky ta biznes-modeli pidpryiemstv" [The Impact of Digital Transformation of the Ukrainian Economy on Business Models of Enterprises]. *Naukovi pratsi Mizhrehionalnoi Akademii upravlinnia personalom. Seriia «Ekonomichni nauky»*, no. 5 (2023): 45-50. DOI: https://doi.org/10.32689/2523-4536/72-7

Pizhuk, O. I. "Kiberbezpeka yak faktor pryskorennia tsyfrovoi transformatsii ekonomiky Ukrainy" [Cybersecurity as an Acceleration Factor of the Digital Transformation of Ukraine's Economy]. *Internauka. Seriia «Ekonomichni nauky»*, no. 10 (2020): 67-73. DOI: https://doi.org/10.25313/2520-2294-2020-10-6409

Savchenko, V., and Makliuk, O. "Kiberbezpeka yak faktor efektyvnosti funktsionuvannia zakladiv vyshchoi osvity" [Cyber Security as a Factor of the Efficiency of the Functioning of Higher Education's Institutions]. *Ekonomika ta suspilstvo*, no. 60 (2024). DOI: https://doi.org/10.32782/2524-0072/2024-60-24

Yakovenko, Ya. Yu., Bilyk, M. Yu., and Oliinyk, Ye. V. "Tsyfrova transformatsiia biznes-struktur: stratehichni oriientyry v epokhu innovatsii ta tekhnolohichnykh zmin" [Digital Transformation of Business Structures: Strategic Guidelines in the Era of Innovation and Technological Changes]. *Ekonomichnyi prostir*, no. 190 (2024): 355-360. DOI: https://doi.org 10.32782/2224-6282/190-63

Науковий керівник – Крутова А. С.,
доктор економічних наук, професор кафедри економіки та менеджменту Навчально-наукового інституту «Українська інженерно-педагогічна академія» Харківського національного університету ім. В. Н. Каразіна