УДК 004.056.5:330.342:658.15

В. С. Бєлозерцев,
к. е. н., доцент, доцент кафедри економічного моделювання, обліку та статистики,
Дніпровський національний університет імені Олеся Гончара
ORCID ID: https://orcid.org/0000-0003-4191-9382
В. В. Моргуненко,
студент, Дніпровський національний університет імені Олеся Гончара
ORCID ID: https://orcid.org/0009-0008-0167-0117

DOI: 10.32702/2306-6814.2025.15.235

ІНФОРМАЦІЙНА БЕЗПЕКА В ЦИФРОВІЙ ЕКОНОМІЦІ: РИЗИКИ ТА ЗАХИСНІ МЕХАНІЗМИ В БІЗНЕС-СЕРЕДОВИЩІ

V. Bielozertsev,
PhD in Economics, Associate Professor, Associate Professor of the Department of Economic Modeling, Accounting and Statistics, Oles Honchar Dnipro National University
V. Morhunenko,
Student, Oles Honchar Dnipro National University

INFORMATION SECURITY IN THE DIGITAL ECONOMY: RISKS AND PROTECTIVE MECHANISMS IN THE BUSINESS ENVIRONMENT

У статті досліджено актуальні питання забезпечення інформаційної безпеки в умовах цифрової економіки. Авторами проаналізовано основні категорії інформаційних ризиків для бізнесу — фінансові, репутаційні та технічні, розкрито їх взаємозв'язок і наслідки для діяльності підприємств. Особливу увагу приділено сучасним засобам захисту, зокрема антивірусам, фаєрволам, DLP-системам, їхнім функціональним можливостям, перевагам та обмеженням. Проведено аналіз економічних наслідків кіберінцидентів, у тому числі прямого й непрямого впливу на фінансові результати компаній, репутацію та довіру клієнтів. Розглянуто сучасні тенденції у сфері інформаційної безпеки, нормативно-правову базу України та ЄС, особливо у контексті вимог GDPR. Підкреслено важливість комплексного підходу до управління інформаційними ризиками та необхідність інтеграції кібербезпеки в стратегічне управління підприємствами. Стаття містить рекомендації для бізнесу в Україні та пропозиції щодо подальших досліджень у сфері інформаційної безпеки.

The article addresses the pressing issue of information security within the framework of the digital economy and modern business environment. The authors analyze key categories of information security risks that impact business operations, emphasizing financial, reputational, and technical risks. The interrelation of these risks and their potential consequences for enterprises are thoroughly explored. The study highlights the specifics of protective measures and technological tools aimed at risk mitigation, with particular attention to antivirus software, firewalls, and Data Loss Prevention (DLP) systems. These tools are assessed regarding their capabilities, advantages, limitations, and practical application in corporate cybersecurity strategies.

The research places a strong emphasis on the economic consequences of data breaches and cybersecurity incidents. It examines both direct financial losses and indirect impacts, such as reputational damage, loss of client trust, and deterioration of competitive positions. The analysis is supported by up-to-date statistical data, graphical representations, and the latest trends in the information security sector.

The authors also provide a detailed review of the regulatory and legal frameworks governing information security in Ukraine and the European Union. Special consideration is given to compliance requirements under the General Data Protection Regulation (GDPR) and the Law of Ukraine "On Personal Data Protection," which define key standards for data management and protection.

The study underscores the necessity of a comprehensive approach to managing information risks in business practice. It advocates for the integration of cybersecurity into the overall strategic management of enterprises and highlights the role of information security as a critical factor for sustainable business development in the digital era.

The article concludes with practical recommendations for Ukrainian businesses on enhancing their cybersecurity posture and suggests avenues for future research, particularly in the fields of risk modeling, regulatory impact assessment, and the economic evaluation of cybersecurity investments. The findings are intended to support decision-makers in both the private sector and public policy when addressing the multifaceted challenges of information security management.

Ключові слова: інформаційна безпека, цифрова економіка, бізнес-ризики, економічні дані, витік даних, кіберзагрози, захисні механізми, управління ризиками, економічні наслідки.

Key words: Information security, digital economy, business risks, economic data, data breach, cyber threats, protective mechanisms, risk management, economic consequences.

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Цифрова економіка стрімко розвивається, проникаючи у всі сфери бізнес-середовища та суспільства. Зростаюча залежність компаній від інформаційних технологій і даних супроводжується підвищенням вразливості до кібератак та витоків інформації в тому числі критичної для економіки. За даними Всесвітнього економічного форуму, кіберризики нині входять до переліку найсерйозніших глобальних загроз, а пандемія COVID-19 лише прискорила діджиталізацію, оголивши нові вразливості в інформаційній безпеці [1]. Масштаби проблеми постійно зростають: так, у 2022 році було зафіксовано понад 4 000 випадків витоку даних по всьому світу, внаслідок чого компрометовано понад 22 млрд записів. Таким чином, забезпечення належного рівня інформаційної безпеки стало критичним чинником стійкості бізнесу в умовах цифрової економіки.

Інформаційна безпека в бізнес-середовищі охоплює широкий спектр питань — від технічних засобів захисту до управління ризиками та відповідності нормативним вимогам. У контексті менеджменту, торгівлі та економіки інформаційна безпека безпосередньо впливає на фінансові показники компаній, їхню репутацію на ринку та конкурентоспроможність. Витоки конфіденційних даних можуть призвести до значних фінансових втрат, штрафів і судових позовів, тоді як успішні кібератаки здатні підірвати довіру клієнтів і партнерів. Водночас інвестування в сучасні засоби кіберзахисту та побудову системи управління інформаційними ризиками розглядається як стратегічно важлива задача для сталого розвитку цифрового бізнесу.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Проблематика інформаційної безпеки в умовах цифрової економіки активно досліджується в наукових колах останніх років. Багато авторів відзначають, що цифрова трансформація бізнес-процесів, впровадження хмарних технологій, великих даних, штучного інтелекту тощо підвищує ефективність діяльності підприємств, але одночасно створює нові кібернетичні загрози [2].

Згідно з результатами систематичного літературного огляду цифрова трансформація супроводжується зростанням кількості кіберінцидентів, зокрема витоків даних та кібератак, що ставить під загрозу стійкість бізнесу [3]. Кібербезпека визнається невід'ємною складовою цифрової економіки, оскільки вона захищає цифрові активи від загроз і тим самим забезпечує безперервність бізнес-процесів.

У наукових публікаціях 2021—2025 рр. пропонуються різні підходи до класифікації ризиків інформаційної безпеки. Найчастіше ризики поділяють за характером потенційних втрат на фінансові, репутаційні та технічні (операційні). Наприклад, Panteli та ін. [3] доповнюють цю класифікацію психологічними та корпоративними аспектами кіберризиків, що вказує на мультидисциплінарний характер проблеми. Низка дослідників наголошує на необхідності холістичного підходу до управління інформаційними ризиками, який враховує взаємозв'я-

зок різних факторів — від технологічних до організаційних. У роботі Stefani E. та ін. [4] запропоновано рамкову модель інформаційної безпеки для цифрової трансформації, яка охоплює ідентифікацію та класифікацію притаманних цифровим технологіям ризиків. Це підтверджує актуальність завдання впорядкування знань про різновиди кіберризиків для бізнесу.

Значна увага приділяється фінансовим наслідкам кіберінцидентів. Uddin M. та ін. [5] у своїй праці узагальнили, що кібернетичні уразливості негативно впливають на зростання та результати діяльності організацій; зокрема у банківському секторі кіберзагрози призвели до підвищення операційних ризиків. Дослідження Curti F. та ін. [6] показало, що кількість кібератак на державний сектор зростає, змушуючи уряди збільшувати видатки на кібербезпеку та підвищуючи загальні витрати на функціонування держустанов. Інші автори фокусуються на макроекономічних аспектах: так, Radulescu C. та ін. [7] відзначають двоїстий вплив діджиталізації — з одного боку, вона стимулює економічне зростання та інклюзію, а з іншого — створює нові ризики для економічної і інформаційної безпеки.

Українські вчені також роблять вагомий внесок у дослідження цієї тематики. Зокрема, у багатьох працях [8], [7], [20] розглядаються питання кібербезпеки у фінансовому секторі та державному управлінні. Встановлено, що банківський сектор є одним із найбільш уразливих до кібератак: захищеність фінансових даних клієнтів впливає не лише на фінансові показники банку, а й на його репутацію як надійної установи. Велике значення надається людському фактору — помилки персоналу чи браку обізнаності користувачів, які часто стають причиною успішних атак на інформаційні системи. Kuzmenko O. та ін [8] запропонували інноваційний підхід до управління кібербезпекою у фінансових установах, що базується на аналізі великих обсягів даних для виявлення потенційних кіберзагроз і підвищення захищеності банківського сектору. Також досліджуються прогностичні моделі: наприклад, Kuzior A. та ін. [9] застосували методи прогнозування інформаційних трендів кіберзлочинності для оцінювання ризиків у фінансових установах. Ці роботи свідчать про інтенсивний розвиток наукового підгрунтя для підвищення кіберстійкості економіки України, особливо в умовах зростання кіберзагроз та вимог європейської інтеграції.

Отже, аналіз фахової літератури показує, що інформаційна безпека є міждисциплінарною проблемою, яка знаходиться на перетині менеджменту, економіки та інформаційних технологій. Сучасні дослідження приділяють увагу класифікації ризиків, оцінці їхнього впливу на діяльність організацій, а також розробці ефективних механізмів захисту і методів управління ризиками.

Водночас помітний акцент робиться на нормативно-правових аспектах та відповідності стандартам (таким як GDPR) у сфері захисту даних. Це формує базис для нашого подальшого дослідження, спрямованого на інтеграцію цих аспектів та вироблення практичних рекомендацій для бізнес-середовища України.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ (ПОСТАНОВКА ЗАВДАННЯ)

Метою статті є всебічне дослідження ризиків інформаційної безпеки в умовах цифрової економіки та аналіз ефективності сучасних захисних механізмів у бізнес-середовищі. Для досягнення цієї мети поставлено такі завдання: класифікувати основні ризики інформаційної безпеки в цифровій економіці; дослідити сучасні інструменти захисту інформації, їх переваги та обмеження; проаналізувати економічні наслідки витоків даних; провести порівняльний аналіз підходів до забезпечення інформаційної безпеки в Україні та Європейському Союзі, зокрема в контексті чинної нормативно-правової бази.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ ДОСЛІДЖЕННЯ

За результатами аналізу літератури і практики інформаційної безпеки, основні ризики для бізнесу в цифровій економіці можна умовно поділити на три категорії: фінансові, репутаційні та технічні (операційні) ризики. Кожна категорія охоплює специфічні загрози та можливі наслідки для підприємства.

Фінансові ризики включають прямі економічні втрати від кіберінцидентів: викрадення коштів кіберзлочинцями, виплати викупу при атаках типу ransomware, витрати на ліквідацію наслідків (відновлення систем, залучення експертів), штрафи регуляторів за порушення захисту даних, а також непрямі втрати — простій бізнес-процесів, зниження доходів через збої. Наприклад, середня пряма вартість витоку даних у світі у 2023 році досягла рекордних $4,45 млн США [10]. Це на 15% більше, ніж у 2020 році, що підкреслює зростаючу фінансову небезпеку кіберінцидентів. Для великих компаній втрати можуть бути ще значнішими: у США середня вартість одного витоку сягає $8,6 млн [11]. Крім того, кожен скомпрометований запис з персональними даними коштує компаніям близько $150 збитків [12], тож масштабні витоки (у сотні тисяч або мільйони записів) здатні генерувати значні суми втрат. Фінансові ризики також пов'язані з можливими штрафами: згідно з GDPR, за неналежний захист даних компанія може отримати штраф до 20 млн євро або 4% світового річного обороту (в залежності від того, що більше), що для великого бізнесу складає сотні мільйонів. Таким чином, фінансовий аспект є одним із найвідчутніших драйверів інвестування в кібербезпеку.

Кіберінциденти здатні завдати серйозного удару по діловій репутації та довірі з боку клієнтів, партнерів, інвесторів. Витік конфіденційних даних клієнтів або публічне повідомлення про злам систем підриває імідж надійності. Дослідження споживчої поведінки показують, що близько 65—80% клієнтів втрачають довіру до компанії після витоку їхніх даних [13]. Більше половини споживачів заявляють, що не будуть надалі користуватися послугами компанії, яка стала жертвою серйозного витоку інформації. Відповідно, бізнес ризикує втратити існуючих клієнтів і недоотримати нових через зіпсовану репутацію. Репутаційні втрати часто мають довгостроковий характер: після масштабних інцидентів акції компаній нерідко падають у ціні (за окремими оцінками, акції постраждалих компаній у середньому знижуються на приблизно 8,6% через рік після витоку [14], хоча точні оцінки різняться). Відновлення ділової репутації потребує значних зусиль, часу та додаткових витрат на PR-кампанії, покращення сервісу тощо, і не завжди гарантує повне повернення довіри. Репутаційний

ризик є тісно пов'язаним з фінансовим — втрата клієнтів та ринкової вартості бізнесу безпосередньо впливає на прибутки і капіталізацію.

Технічні (операційні) ризики — ця категорія охоплює загрози безпосередньо для інформаційних систем та інфраструктури компанії, які можуть порушити безперебійну роботу бізнес-процесів [20]. Сюди відносять виведення з ладу IT-систем у результаті кібератаки (наприклад, DDoS-атаки, знищення або шифрування даних), збої в роботі через шкідливе програмне забезпечення, несанкціонований доступ до критичних систем, крадіжку або пошкодження даних, порушення цілісності інформації. Технічні збої часто трансформуються у фінансові втрати, але їх особливість — безпосередній вплив на операційну діяльність (призупинення операцій, порушення сервісів). За статистикою, атаки типу ransomware спричиняють в середньому понад 16 днів простою в роботі підприємств, поки триває відновлення систем [15]. Інший приклад — середній час виявлення і реагування на витік даних у 2023 році становив 277 днів (204 дні, щоб виявити інцидент, і ще 73 дні, щоб його локалізувати) [15]. За цей тривалий період зловмисники можуть завдати масштабної шкоди інфраструктурі та даним. Операційні ризики також включають технічні помилки або збої, не обов'язково пов'язані з атаками, але які створюють вразливості (наприклад, помилки конфігурації серверів, що призводять до відкритого доступу до даних). Таким чином, технічні ризики характеризуються потенційною втратою контролю над IT-активами компанії, що безпосередньо загрожує її діяльності.

Варто підкреслити, що всі зазначені категорії ризиків тісно пов'язані між собою. Єдина подія кіберінциденту часто генерує наслідки в усіх трьох площинах: і фінансові витрати, і репутаційні збитки, і технічні труднощі. Тому управління інформаційними ризиками потребує комплексного підходу, що враховує множинність потенційних збитків та шляхи їх мінімізації.

Захисні механізми та інструменти інформаційної безпеки. Для протидії вказаним ризикам бізнес-середовище використовує різноманітні механізми та інструменти інформаційної безпеки. Їх можна розділити на технічні засоби захисту і організаційно-процесуальні заходи. Розглянемо основні з них та проаналізуємо переваги і недоліки кожного.

Антивірусні системи (AntiVirus, AV) — це програмні засоби, призначені для виявлення і знешкодження відомих шкідливих програм (вірусів, троянів, руткітів тощо) на кінцевих пристроях і серверах. Переваги: антивірус є базовим елементом кіберзахисту, забезпечує автоматичний моніторинг файлів і процесів, запобігає виконанню відомого шкідливого коду. Щодо недоліків, то традиційні антивіруси в основному спираються на відомі сигнатури загроз, тому малоефективні проти новітніх, спеціально розроблених для атаки шкідливих програм (нульового дня), та складних цільових атак. Вони можуть давати хибнопозитивні спрацьовування або бути обійденими досвідченими зловмисниками. Антивірус не захищає від багатьох інших векторів атак (фішинг, експлуатація вразливостей без файлового навантаження тощо). Отже, AV — необхідний, але недостатній інструмент захисту, який слід комбінувати з іншими заходами.

Мережеві екрани (фаєрволи) — це апаратні або програмні засоби, що контролюють мережевий трафік, фільтруючи пакети згідно з визначеними правилами безпеки. Фаєрволи створюють бар'єр між внутрішньою мережею компанії та зовнішніми мережами (інтернетом), блокуючи неавторизовані доступи. Правильно налаштований фаєрвол суттєво знижує ризик зовнішнього проникнення в корпоративну мережу, запобігає скануванню портів і багатьом видам мережевих атак. Сучасні багаторівневі фаєрволи (Next-Generation Firewall) можуть аналізувати не лише заголовки пакетів, а й вміст (Deep Packet Inspection), виявляючи шкідливі дані. Фаєрволи є основою периметрового захисту, їх використання є вимогою багатьох стандартів безпеки. До недоліків можна віднести неступне: традиційні фаєрволи не захищають від атак, що обходять мережевий периметр (наприклад, атаки на веб-додатки або з використанням соціальної інженерії). В умовах переходу до хмарних сервісів і віддаленої роботи "периметр" мережі стає розмитим, і виключно фаєрвольного захисту недостатньо.

Окреме питання слід приділити системам запобігання витоку даних (DLP — Data Loss Prevention). DLP-рішення контролюють переміщення і використання конфіденційної інформації в межах організації, щоб не допустити її несанкціонованого витоку назовні. Вони відстежують електронну пошту, файлообмін, друк, копіювання на зовнішні носії та інші канали, застосовуючи політики безпеки (наприклад, блокують відправку файлів, що містять певні ключові слова або персональні дані). Перевагою DLP є те, що вони дозволяють попередити як зумисні, так і випадкові витоки даних співробітниками — одну з основних причин інцидентів (на інсайдерів припадає до 35% витоків). Система надає централізований контроль над критичною інформацією, допомагає підтримувати відповідність регуляторним вимогам щодо захисту даних (GDPR тощо). DLP може забезпечити журналювання спроб порушень, що корисно для розслідувань. Впровадження DLP є складним та дорогим процесом, що вимагає детального налаштування політик та класифікації даних.

Інформаційна безпека тісно пов'язана з економічними показниками діяльності підприємств і економіки в цілому. Витоки даних та інші кіберінциденти мають різноманітні економічні наслідки, які умовно можна розділити на прямі та непрямі. Прямі економічні наслідки включають: фінансові втрати від крадіжки грошей або інформації, виплати здирникам, витрати на реагування (технічне відновлення, форензік, юридичні послуги), штрафи та компенсації постраждалим особам. Непрямі наслідки охоплюють: втрату майбутніх прибутків через відтік клієнтів, зниження ринкової вартості компанії, упущені можливості розвитку, зростання вартості залучення нових клієнтів, підвищення витрат на страхування тощо.

Одним із найтриваліших економічних ефектів інцидентів є втрата довіри та бізнес-можливостей. Більшість споживачів насторожено ставляться до компаній, які пережили витік. Це означає зменшення клієнтської бази і, відповідно, доходів. Окремі дослідження ринку оцінюють, що компанії після публічного кіберінциденту в середньому недоотримують близько 5—8% запланованого річного виторгу через відтік клієнтів і зниження конверсії потенційних клієнтів (значення варіюються за галузями: найбільш чутливими є фінансові послуги, електронна комерція) [14], [15]. Крім того, підприємство може стикнутися з ростом вартості залучення нових

клієнтів (необхідність додаткових маркетингових акцій, знижок для повернення довіри).

Ще один важливий аспект — витрати на усунення наслідків та посилення захисту після інциденту. Постфактум компанії часто інвестують значні кошти у модернізацію систем безпеки, аудити, навчання персоналу, щоб запобігти повторенню подібного. За даними IBM [15], понад половина організацій, що пережили витік, планують збільшити бюджети на кібербезпеку після інциденту, причому основні напрямки додаткових інвестицій — розробка планів реагування на інциденти, тренінги співробітників і впровадження засобів виявлення загроз.

Таким чином, хоча ці витрати є "добровільними", вони фактично є вимушеними наслідками інциденту і повинні враховуватися при оцінці загального економічного впливу.

На основі представлених результатів можна здійснити порівняльний аналіз підходів до інформаційної безпеки у бізнесі та використовуваних інструментів, визначивши їх сильні та слабкі сторони. Загалом простежується тенденція до впровадження багаторівневих систем захисту, що поєднують різні методи. Класична модель "захисту периметру" (спираючись переважно на фаєрволи для ізоляції внутрішньої мережі) сьогодні доповнюється принципами Zero Trust (нульової довіри), які передбачають перевірку користувача і пристрою при кожному доступі, незалежно від того, знаходиться він всередині чи поза мережею. Такий підхід є відповіддю на розмивання мережевих кордонів і зростання віддаленої роботи.

Антивірус і фаєрвол тривалий час були стандартним мінімумом кіберзахисту для малого та середнього бізнесу. Однак сучасні загрози змушують додавати додаткові шари: системи виявлення вторгнень (IDS) для моніторингу мережевої активності, SIEM-платформи для кореляції подій безпеки, DLP-системи для контролю критичних даних, сегментування мережі (поділ на ізольовані зони, щоб ускладнити рух зловмисника в разі проникнення). Підхід з активним використанням хмарних сервісів безпеки (таких як Secure Web Gateway, Cloud Access Security Broker) набуває популярності в рамках концепції SASE (Secure Access Service Edge), що об'єднує мережеві і безпекові функції в хмарі [17]. Це дозволяє забезпечити захист географічно розподілених користувачів і ресурсів.

Варто порівняти ефективність превентивних і детективних заходів. Превентивні заходи (наприклад, фаєрвол, системи контролю доступу) спрямовані на недопущення інциденту, тоді як детективні (моніторинг, IDS/IPS, антивірусне сканування) — на своєчасне виявлення факту атаки чи компрометації. Досвід показує, що жоден підхід не є абсолютно надійним окремо: найкращі результати досягаються при їх поєднанні. Превентивні засоби можуть знизити ймовірність успішної атаки, але у разі їх обходу — потрібні детективні для швидкого виявлення і реагування [18]. За даними звіту IBM, лише 33% витоків даних у 2023 р. були виявлені внутрішніми силами організації (службами безпеки), тоді як 67% — сторонніми особами або самими зловмисниками [15].

Окремим питанням є нормативно-правове забезпечення інформаційної безпеки. Правове регулювання відіграє важливу роль у забезпеченні інформаційної безпеки, встановлюючи обов'язкові вимоги та стандарти для бізнесу. В Європейському Союзі ключовим актом у сфері захисту даних є General Data Protection Regulation (GDPR), що набув чинності у 2018 році [18]. GDPR запровадив жорсткі вимоги до обробки персональних даних, зобов'язав компанії впроваджувати належні технічні та організаційні заходи захисту, а у разі витоку — повідомляти регулятора і постраждалих осіб протягом 72 годин. Важливо, що дія GDPR екстериторіальна: він поширюється не лише на компанії, зареєстровані в ЄС, але й на будь-які організації, що обробляють дані резидентів ЄС. За порушення передбачені суттєві штрафи — як вже згадувалося, до 4% глобального обороту компанії. Ці норми стимулювали бізнес в Європі підвищити рівень кібербезпеки та відповідності стандартам. За оцінками, впровадження GDPR сприяло зростанню витрат компаній на IT-безпеку в середньому на 20—30%, але одночасно призвело до зменшення частоти витоків у деяких секторах.

В Україні основним законом у сфері захисту персональних даних є Закон України "Про захист персональних даних" №2297-VI, прийнятий у 2010 році (із змінами) [16]. Цей закон встановлює загальні принципи обробки персональних даних, права суб'єктів даних та обов'язки володільців/розпорядників баз даних. Втім, положення українського закону суттєво відстають від вимог GDPR.

Зокрема, український закон не містить таких деталей, як принцип "privacy by design", обов'язкове призначення посадової особи із захисту даних (DPO) у великих компаніях, порядок повідомлення про витоки тощо. Розміри штрафів за порушення теж були номінальними (до недавніх змін — лише кілька тисяч гривень). Внаслідок цього мотивуючий ефект українського регулювання на бізнес довгий час залишався слабким.

Ситуація почала змінюватися у зв'язку із підписанням Угоди про асоціацію з ЄС та зобов'язаннями України гармонізувати своє законодавство із європейським. Наразі готується нова редакція закону про персональні дані, покликана імплементувати положення GDPR у національне право. Проєкт передбачає розширення прав суб'єктів даних, введення значно більших штрафів, деталізацію вимог до згоди на обробку даних, зобов'язання повідомляти контролюючий орган про інциденти. Прийняття цього закону стане важливим кроком до євроінтеграції у сфері цифрової економіки. Паралельно, в Україні діє Закон "Про основні засади забезпечення кібербезпеки України", який окреслює структури забезпечення кібербезпеки держави, визначає критичну інфраструктуру та розподіляє відповідальність між держорганами [19]. Для бізнесу цей закон не встановлює прямих зобов'язань, але створює загальний фон політики кібербезпеки. Особливо актуальною стала нормативно-правова база в контексті останніх подій — масованих кібератак в умовах військової агресії РФ.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

Проведене дослідження показало, що інформаційна безпека в цифровій економіці є багатовимірною проблемою, яка вимагає уваги як з технічної, так і з управлінської та економічної точок зору. Класифікація ризиків на фінансові, репутаційні та технічні дозволяє си-

стематизувати потенційні загрози для бізнесу і краще розуміти наслідки кожного виду інцидентів. Фінансові ризики проявляються у прямих матеріальних втратах і штрафах, репутаційні — у втраті довіри і ринкових позицій, технічні — у порушенні безперервності операцій. Всі вони тісно переплетені, і серйозний кіберінцидент часто одночасно завдає удару по всіх трьох напрямах. Аналіз сучасних захисних механізмів вказує на необхідність комплексного, багатоешелонного захисту. Окремі інструменти (такі як антивірус чи фаєрвол) є важливими, але недостатніми — тільки їх узгоджене застосування разом із системами захисту даних, моніторингом та, не менш важливо, навчанням персоналу здатне забезпечити прийнятний рівень безпеки. Особливо актуальним стає впровадження новітніх рішень — від штучного інтелекту для виявлення аномалій до концепції Zero Trust для мінімізації довіри в мережах — що підтверджується практикою успішних компаній.

Економічні наслідки кібератак є вагомими і зростають з часом. Середня вартість витоків даних б'є рекорди щороку, а непрямі втрати від таких інцидентів можуть перевищувати прямі витрати у кілька разів. Кібератаки перетворилися на суттєвий бізнес-ризик, яким необхідно управляти на рівні з фінансовими чи операційними ризиками. Інвестування в інформаційну безпеку, хоч і збільшує витрати в короткостроковій перспективі, окупається запобіганням потенційно руйнівних втрат у майбутньому. Сьогодні кібербезпека — це не просто IT-питання, а частина стратегії управління підприємством, яка впливає на його конкурентоспроможність, репутацію і відповідність законодавству.

Нормативно-правовий аналіз показав, що Україні потрібно прискорити гармонізацію своїх стандартів захисту інформації з європейськими, аби забезпечити належний захист прав громадян і створити сприятливі умови для інтеграції в глобальну цифрову економіку. GDPR встановив високі планки, і український бізнес, орієнтований на експорт або співпрацю з ЄС, вже зараз відчуває на собі вплив цих правил. Впровадження нових законів і правил вимагатиме від компаній підвищення зрілості систем управління інформаційною безпекою.

Дана робота охопила широке коло питань, проте залишаються напрями, які потребують глибшого аналізу. Перспективними є дослідження методів кількісної оцінки інформаційних ризиків для бізнесу — наприклад, розвиток моделей економетричного прогнозування збитків від кібератак залежно від галузі та рівня захищеності, що допоможе компаніям обгрунтовувати бюджети на безпеку. Цікавим є застосування кластерного аналізу для сегментації підприємств за профілем кіберризику (з урахуванням таких параметрів, як обсяг даних, кількість користувачів, рівень цифровізації), аби визначити найбільш уразливі групи бізнесу і таргетовано підвищувати їхню стійкість. В умовах поширення штучного інтелекту варто дослідити ризики та можливості AI в кібербезпеці: з одного боку, зловмисники можуть використовувати AI для автоматизації атак, з іншого — AI є потужним інструментом захисту. Крім того, актуальним напрямом є вивчення поведінкових та психологічних аспектів інформаційної безпеки в організаціях (як культура безпеки впливає на готовність протидіяти загрозам, мотивація співробітників дотримуватися правил тощо). Подальші дослідження у згаданих напрямах дозволять ще більш ефективно поєднати науковий підхід і практичні рішення для забезпечення інформаційної безпеки цифрової економіки України.

Література:

1. Pipikaite A., Barrachin M., Crawford S. These are the top cybersecurity challenges of 2021. World Economic Forum. 21.01.2021. URL: https://www.weforum.org/agenda/2021/01/top-cybersecurity-challenges-2021/ (дата звернення: 07.07.2025).

2. Alshehri E., Alabbad D. Digital Transformation and Cybersecurity Challenges for Business Resilience: Issues and Recommendations. Electronics. 2023. Vol. 12, No 17. P. 3554. DOI: https://doi.org/10.3390/electronics12173554.

3. Panteli N., Nurse J.R.C., et al. Information security risks of digitalization. Journal of Strategic Information Systems. 2022. Vol. 31, No 4. DOI: https://doi.org/10.1016/j.jsis.2022.101710.

4. Stefani E., et al. Information Security Risk Framework for Digital Transformation Technologies. Systems. 2023. Vol. 13, No 1. P. 37. DOI: https://doi.org/10.3390/systems13010037.

5. Uddin M.H., Ali M.H., Hassan M.K. Cybersecurity hazards and financial system vulnerability: A synthesis of literature. Risk Management. 2020. Vol. 22. P. 239—309. DOI: https://doi.org/10.1057/s41283-020-00061-5.

6. Curti F., Ivanov I., Macchiavelli M., Zimmermann T. City Hall Has Been Hacked! The Financial Costs of Lax Cybersecurity. SSRN. 2023. DOI: https://doi.org/10.2139/ssrn.4567891.

7. Radulescu C.V., et al. Risks associated with digitalization regarding economic development and information security. Amfiteatru Economic. 2022. Vol. 24, No 59. P. 792—807. URL: https://www.amfiteatru-economic.ro/temp/Article_3197.pdf (дата звернення: 07.07.2025).

8. Kuzmenko O., Kubalek J., Bozhenko V., et al. An approach to managing innovation to protect financial sector against cybercrime. Polish Journal of Management Studies. 2021. Vol. 24, No 2. P. 276—291. DOI: https://doi.org/10.17512/pjms.2021.24.2.17.

9. Kuzior A., Brozek P., Kuzmenko O., et al. Countering cybercrime risks in financial institutions: Forecasting information trends. Journal of Risk and Financial Management. 2022. Vol. 15, No 12. P. 613. DOI: https://doi.org/10.3390/jrfm15120613.

10. Hanley J. Cost of a Data Breach Report 2023: Insights, Mitigators and Best Practices. The Hacker News. 21.12.2023. URL: https://thehackernews.com/2023/12/cost-of-data-breach-2023.html (дата звернення: 07.07.2025).

11. Resilient X. Key findings from the IBM Cost of a Data Breach Report 2023. ResilientX. 2023. URL: https://resilientx.com/2023/07/28/ibm-cost-of-a-data-breach-report-2023-key-findings/ (дата звернення: 07.07.2025).

12. Metomic. The Biggest Data Breaches in 2022. Metomic. 2023. URL: https://metomic.io/resources/the-biggest-data-breaches-in-2022 (дата звернення: 07.07.2025).

13. Varonis. Analyzing Company Reputation After a Data Breach. Varonis. 2023. URL: https://www.va-

ronis.com/blog/company-reputation-after-a-data-breach (дата звернення: 07.07.2025).

14. SANS Institute. SANS 2022 Cloud Security Survey. SANS Institute. 2022. URL: https://www.sans.org/white-papers/cloud-security-survey-2022/ (дата звернення: 07.07.2025).

15. Gartner. Information Security Spending Worldwide 2017-2023. Gartner. 2023. URL: https://www.gartner.com/en/newsroom/press-releases/2023-08-28-worldwide-security-and-risk-management-spending-to-grow-14-percent-in-2024 (дата звернення: 07.07.2025).

16. Верховна Рада України. Закон України "Про захист персональних даних" № 2297-VI (чинна ред. від 18.01.2025). Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 07.07.2025).

17. Буяло К. Персональні дані в ЄС, або Вступ до GDPR. DOU. 31.01.2023. URL: https://dou.ua/lenta/articles/personal-data-and-gdpr/ (дата звернення: 07.07.2025).

18. LegalITGroup. GDPR комплаєнс: чек-лист. LegalITGroup. 2022. URL: https://legalitgroup.com/gdpr-checklist/ (дата звернення: 07.07.2025).

19. Державна стратегія кібербезпеки України на 2021-2025 рр. Центр стратегічних комунікацій та інформаційної безпеки. URL: https://cip.gov.ua/ua/diyalnist/strategiya-kiberbezpeki-ukrayini-na-2021-2025-roki (дата звернення: 07.07.2025).

20. Бєлозерцев В., Харакоз Л., Моргуненко В. ERP-системи у стратегічному управлінні корпоративними ресурсами: переваги, виклики та перспективи розвитку. Електронний журнал "Ефективна економіка". 2025. № 6. URL: https://doi.org/10.32702/2307-2105.-2025.6.90 (дата звернення: 10.07.2025)

References:

1. Pipikaite, A., Barrachin, M. and Crawford, S. (2021), "These are the top cybersecurity challenges of 2021", World Economic Forum, available at: https://www.weforum.org/agenda/2021/01/top-cybersecurity-challenges-2021/ (Accessed 7 July 2025).

2. Alshehri, E. and Alabbad, D. (2023), "Digital Transformation and Cybersecurity Challenges for Business Resilience: Issues and Recommendations", Electronics, vol. 12, no. 17, p. 3554. https://doi.org/10.3390/electronics12173554.

3. Panteli, N., Nurse, J.R.C. and others. (2022), "Information security risks of digitalization", Journal of Strategic Information Systems, vol. 31, no. 4. https://doi.org/10.1016/j.jsis.2022.101710.

4. Stefani, E. and others. (2023), "Information Security Risk Framework for Digital Transformation Technologies", Systems, vol. 13, no. 1, p. 37. https://doi.org/10.3390/systems13010037.

5. Uddin, M.H., Ali, M.H. and Hassan, M.K. (2020), "Cybersecurity hazards and financial system vulnerability: A synthesis of literature", Risk Management, vol. 22, pp. 239—309. https://doi.org/10.1057/s41283-020-00061-5.

6. Curti, F., Ivanov, I., Macchiavelli, M. and Zimmermann, T. (2023), "City Hall Has Been Hacked! The Financial Costs of Lax Cybersecurity", SSRN, https://doi.org/10.2139/ssrn.4567891.

7. Radulescu, C.V. and others. (2022), "Risks associated with digitalization regarding economic development and information security", Amfiteatru Economic, vol. 24, no. 59, pp. 792—807, available at: https://www.amfiteatrueconomic.ro/temp/Article_-3197.pdf (Accessed 7 July 2025).

8. Kuzmenko, O., Kubalek, J., Bozhenko, V. and others. (2021), "An approach to managing innovation to protect financial sector against cybercrime", Polish Journal of Management Studies, vol. 24, no. 2, pp. 276—291. https://doi.org/10.17512/pjms.2021.24.2.17.

9. Kuzior, A., Brozek, P., Kuzmenko, O. and others. (2022), "Countering cybercrime risks in financial institutions: Forecasting information trends", Journal of Risk and Financial Management, vol. 15, no. 12, p. 613. https://doi.org/10.3390/jrfm15120613.

10. Hanley, J. (2023), "Cost of a Data Breach Report 2023: Insights, Mitigators and Best Practices", The Hacker News, available at: https://thehackernews.com/2023/12/cost-of-data-breach-2023.html (Accessed 7 July 2025).

11. Resilient X. (2023), "Key findings from the IBM Cost of a Data Breach Report 2023", available at: https://resilientx.com/2023/07/28/ibm-cost-of-a-data-breach-report-2023-key-findings/ (Accessed 7 July 2025).

12. Metomic (2023), "The Biggest Data Breaches in 2022", available at: https://metomic.io/resources/the-biggest-data-breaches-in-2022 (Accessed 7 July 2025).

13. Varonis (2023), "Analyzing Company Reputation After a Data Breach", available at: https://www.varonis.-com/blog/company-reputation-after-a-data-breach (Accessed 7 July 2025).

14. SANS Institute (2022), "SANS 2022 Cloud Security Survey", available at: https://www.sans.org/white-papers/cloud-security-survey-2022/ (Accessed 7 July 2025).

15. Gartner (2023), "Information Security Spending Worldwide 2017—2023", available at: https://www.gartner.com/en/newsroom/press-releases/2023-08-28-worldwide-security-and-risk-management-spending-to-grow-14-percent-in-2024 (Accessed 7 July 2025).

16. The Verkhovna Rada of Ukraine (2025), The Law of Ukraine "On Personal Data Protection" No. 2297-VI, available at: https://zakon.rada.gov.ua/laws/show/2297-17#Text (Accessed 7 July 2025).

17. Bujalo, K. (2023), "Personal Data in the EU, or Introduction to GDPR", DOU, 31 January, available at: https://dou.ua/lenta/articles/personal-data-and-gdpr/ (Accessed 7 July 2025).

18. LegalITGroup (2022), "GDPR Compliance: Checklist", available at: https://legalitgroup.com/gdpr-checklist/ (Accessed 7 July 2025).

19. Center for Strategic Communications and Information Security (2021), "Cybersecurity Strategy of Ukraine for 2021—2025", available at: https://cip.gov.ua/ua/diyalnist/strategiya-kiberbezpeki-ukrayini-na-2021-2025-roki (Accessed 7 July 2025).

20. Bielozertsev, V., Kharakoz, L. and Morhunenko, V. (2025), "ERP-systems in Strategic Management of Corporate Resources: Advantages, Challenges and Development Prospects", Efektyvna ekonomika [Effective Economy], no. 6, available at: https://doi.org/10.32702/2307-2105.2025.6.90 (Accessed 10 July 2025).

Стаття надійшла до редакції 18.07.2025 р.