https://doi.org/10.31891/2307-5740-2025-342-3(1)-14
УДК 658.012.8

СОРОКІВСЬКА Олена
Тернопільський національний технічний університет імені Івана Пулюя
https://orcid.org/0000-0001-8549-2910
e-mail: sorokivska_o@tntu.edu.ua
КУЖДА Тетяна
Тернопільський національний технічний університет імені Івана Пулюя
https://orcid.org/0000-0002-5962-0795
e-mail: kuzhda_t@tntu.edu.ua
КІНАЛЬ Назар
Тернопільський національний технічний університет імені Івана Пулюя
https://orcid.org/0009-0003-7980-2101
e-mail: nazarkinal@ukr.net

ЦИФРОВІ РИЗИКИ ТА ІНФОРМАЦІЙНА БЕЗПЕКА КОРПОРАТИВНОГО СЕКТОРУ

Стаття присвячена дослідженню цифрових ризиків та інформаційної безпеки корпоративного сектору, особливо в умовах воєнного часу. Акцент зроблено на аналізі сучасних загроз, які виникають у зв'язку з кіберзлочинністю, витоком конфіденційної інформації та порушенням функціонування інформаційних систем підприємств. Розглянуто тенденції зростання кількості кібератак та їх наслідки для бізнесу, включаючи фінансові втрати, репутаційні ризики та компрометацію даних.

У статті систематизовано сучасні методи та підходи до захисту інформаційної інфраструктури компаній, зокрема впровадження багаторівневої автентифікації, концепції Zero Trust, шифрування даних, а також моніторингу даркнету для запобігання витоку корпоративної інформації. Особливу увагу приділено аналізу європейського досвіду у сфері кібербезпеки, порівнянню рівня впровадження ІКТ-захисту серед підприємств ЄС та України.

На основі проведеного дослідження розроблено модель організації та управління корпоративною інформаційною безпекою, що включає п'ять ключових компонентів: організаційну структуру, технологічні рішення, управління ризиками, захист корпоративних даних та аудит безпеки. Запропонована модель спрямована на мінімізацію кіберзагроз та забезпечення стійкого розвитку бізнесу в умовах цифрової трансформації. Результати дослідження можуть бути використані керівниками підприємств, IT-спеціалістами та фахівцями з інформаційної безпеки для розробки ефективних стратегій захисту корпоративних інформаційних систем.

Ключові слова: цифрові ризики, інформаційна безпека, кіберзагрози, корпоративний сектор, кіберстійкість, кіберризики, захист даних, управління кібербезпекою.

SOROKIVSKA Olena, KUZHDA Tetiana, KINAL Nazar
Ternopil Ivan Puluj National Technical University

DIGITAL RISKS AND INFORMATION SECURITY OF THE CORPORATE SECTOR

The article explores current issues of digital risks and information security in the corporate sector amid increasing cyber threats. The authors analyze the specifics of modern threats faced by companies, including risks of unauthorized access, data breaches, DDoS attacks, phishing campaigns, and malware. Special attention is given to the analysis of cybersecurity in wartime conditions, where companies become targets for hostile hacker groups aiming to destabilize the economy and undermine trust in businesses. The study presents the dynamics of the growing number of cyberattacks during 2022–2024, identifies the key business sectors most vulnerable to threats, and examines their impact on enterprises. A separate section is devoted to analyzing European experience in corporate cybersecurity, comparing the level of implementation of information security measures among EU and Ukrainian enterprises. The research has shown that despite the high level of awareness among Ukrainian companies regarding cybersecurity, the documentation of security policies and their regular review remain insufficient, increasing the likelihood of successful attacks. Based on the obtained results, a model for organizing and managing corporate information security has been developed. This model consists of five key components: organizational structure, technological solutions, risk management, corporate data protection, and control & audit. The proposed model aims to minimize cyber threats, enhance the resilience of the corporate environment, and strengthen trust among clients and partners. It can be utilized by company executives, IT specialists, and information security professionals to develop effective strategies for protecting corporate information systems in the context of digital transformation and increasing cyber threats.

Keywords: digital risks, information security, cyber threats, corporate sector, cyber resilience, cyber risks, data protection, cybersecurity management.

Стаття надійшла до редакції / Received 01.04.2025
Прийнята до друку / Accepted 28.04.2025

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

Дослідження та удосконалення інформаційної безпеки сучасних корпорацій є критично важливим, особливо в період війни, коли загрози кібербезпеці зростають експоненційно. В умовах військових конфліктів компанії стають мішенями для хакерських атак, кібершпигунства та інформаційних диверсій, що може призвести до витоку конфіденційних даних, фінансових втрат і підриву довіри до бізнесу. Ефективний захист

інформаційних систем забезпечує стабільність функціонування компаній, запобігає саботажу критично важливих процесів і сприяє економічній безпеці країни.

У воєнний час особливо зростає роль інформаційної зброї, коли ворог використовує кібератаки для дестабілізації економіки, маніпуляції громадською думкою та підриву стратегічних галузей. Корпорації, що володіють важливими технологіями та ресурсами, повинні постійно вдосконалювати механізми захисту, впроваджувати новітні методи шифрування, багаторівневу автентифікацію та системи моніторингу кіберзагроз.

І саме цифровізація відіграє ключову роль у вирішенні проблеми інформаційної безпеки сучасних корпорацій. Вона дозволяє впроваджувати передові технології кіберзахисту, автоматизувати процеси моніторингу та оперативного реагування на загрози. Сучасні цифрові рішення, зокрема штучний інтелект і машинне навчання, допомагають аналізувати величезні масиви даних у режимі реального часу, виявляти аномалії та запобігати атакам ще до того, як вони завдадуть шкоди. Хмарні технології забезпечують безпечне зберігання та резервне копіювання даних, що мінімізує ризики втрати інформації внаслідок кібератак чи фізичних пошкоджень інфраструктури. Використання багаторівневої автентифікації та біометричних методів ідентифікації значно підвищує рівень захисту доступу до корпоративних систем. Саме тому дослідження питання підвищення рівня інформаційної безпеки корпоративного розвитку в умовах цифрових змін є сьогодні важливим та актуальним.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Аналіз українських та зарубіжних публікацій на тему інформаційної безпеки в умовах цифрових змін виявляє декілька ключових аспектів. У монографії В. І. Чубаєвського розглянуто сутність та детермінанти управління корпоративною інформаційною безпекою підприємств в умовах глобальних викликів. Автор здійснює компаративний аналіз еволюції та структури корпоративного інформаційного простору, досліджує трансформацію видів економічної ефективності діяльності підприємств під впливом цифровізації та пропонує концепцію формування корпоративної інформаційної безпеки [1, с. 115].

У статті О. О. Ляховича та І. О. Оплачко досліджується сутність економічної безпеки в умовах цифровізації, визначаються особливості забезпечення економічної безпеки з урахуванням транспарентності підприємств. Науковці систематизують цифрові загрози економічній безпеці та формують таксономію транспарентності підприємств, пропонуючи концепт діяльності, що враховує межі транспарентності для нейтралізації загроз економічній безпеці [2, с. 103].

І. М. Доронін аналізує питання державного планування в сфері цифрової економіки та розвитку суспільства, досліджуючи правові проблеми, що виникають у цій сфері. Дослідник звертає увагу на неповне врахування питань забезпечення національної безпеки при державному плануванні цифрового розвитку, підкреслюючи необхідність інтеграції аспектів інформаційної безпеки в стратегії цифровізації [3, с. 32].

У статті Валіулліної розглядаються теоретико-методологічні основи інформаційної безпеки корпоративної економіки в умовах глобалізаційних процесів. Автор аналізує вплив інформаційних технологій на корпоративну економіку та підкреслює важливість визначення ефективних шляхів забезпечення інформаційної безпеки для підвищення конкурентоспроможності на світовому ринку [4, с. 34].

Таким чином, вітчизняні дослідження акцентують увагу на необхідності адаптації до нових викликів, пов'язаних з цифровими загрозами, та розробці комплексних підходів до захисту інформаційних ресурсів для забезпечення стійкого розвитку та конкурентоспроможності підприємств.

Аналіз зарубіжних публікацій свідчить про окремі важливі тренди у сфері забезпечення інформаційної безпеки сучасних корпорацій. У статті [5] досліджується взаємозв'язок між сертифікацією інформаційної безпеки (ISO 27001) та фінансовими показниками компаній. Результати показують, що наявність сертифікації позитивно корелює з фінансовими показниками, причому цей вплив зростає з часом. Також зазначається, що приховування інформації про сертифікацію може негативно впливати на ефективність підприємства.

Інше дослідження, [6] присвячено розробленню системи управління інформаційною безпекою, узгодженої зі стандартом NTC-ISO/IEC 27001:2013. Ця модель дозволяє організаціям впроваджувати необхідні види контролю, процедури та політики для збереження цілісності, конфіденційності та доступності інформаційних активів, що є критично важливим в умовах цифровізації.

У науковій праці [7] автори розглядають питання оцінки рентабельності інвестицій у технології кібербезпеки для мережевих критичних інфраструктур. Науковці підкреслюють важливість стратегічного підходу до інвестування в кібербезпеку, оскільки це безпосередньо впливає на стійкість та ефективність корпоративного розвитку в цифровому середовищі.

Таким чином, зарубіжні дослідження зосереджуються на впровадженні стандартів інформаційної безпеки, таких як ISO 27001, для покращення фінансових показників та забезпечення стійкого корпоративного розвитку в умовах цифровізації. Вони також акцентують на необхідності стратегічного планування інвестицій у кібербезпеку та розробці моделей управління інформаційною безпекою, що відповідають міжнародним стандартам.

ВИДІЛЕННЯ НЕВИРІШЕНИХ РАНІШЕ ЧАСТИН ЗАГАЛЬНОЇ ПРОБЛЕМИ, КОТРИМ ПРИСВЯЧУЄТЬСЯ СТАТТЯ

Аналіз останніх досліджень та публікацій у сфері цифрових ризиків та інформаційної безпеки корпоративного сектору свідчить про те, що значна увага приділяється загальним питанням кібербезпеки, впровадженню міжнародних стандартів ISO 27001 та NIST CSF, а також оцінці фінансових наслідків кібератак. Однак, залишається низка невирішених аспектів, які потребують подальшого дослідження. Зокрема, відсутні комплексні дослідження, які б аналізували специфіку інформаційної безпеки корпоративного сектору в умовах воєнного часу, коли кіберзагрози не лише спричиняють фінансові втрати, а й можуть бути інструментом інформаційної війни та економічної дестабілізації. Також недостатньо досліджено питання адаптації сучасних підходів до кіберзахисту в умовах обмежених ресурсів для впровадження комплексних рішень безпеки, характерних для великих корпорацій. Окрім цього, мало уваги приділяється розробці методологій оцінки ефективності заходів кібербезпеки, які б дозволяли підприємствам кількісно вимірювати рівень загроз та оцінювати доцільність інвестицій у захист інформації.

Таким чином, дана стаття спрямована на заповнення виявлених прогалин шляхом розробки моделі організації та управління корпоративною інформаційною безпекою, що враховує сучасні виклики, зокрема в умовах воєнного часу, обмежених ресурсів та активного розвитку цифрових технологій.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ

Метою статті є дослідження цифрових ризиків та інформаційної безпеки корпоративного сектору, зокрема в умовах зростаючих кіберзагроз, воєнного конфлікту та активної цифровізації бізнесу. Робота спрямована на виявлення основних тенденцій у сфері кібербезпеки, оцінку рівня загроз, а також розробку ефективної моделі захисту корпоративної інформаційної інфраструктури.

Основні завдання дослідження:

- провести аналіз цифрових ризиків та кіберзагроз, що впливають на корпоративний сектор, зокрема в умовах воєнного часу;
- визначити основні виклики інформаційної безпеки для підприємств, що працюють у середовищі з високою загрозою хакерських атак, шпигунства та інформаційних диверсій;
- дослідити рівень упровадження інформаційної безпеки в корпоративному секторі України порівняно з країнами ЄС;
- розробити модель організації та управління інформаційною безпекою підприємств, що включає ключові компоненти: організаційну структуру, технологічні рішення, управління ризиками, захист корпоративних даних та контроль/аудит.
- сформувати пропозиції щодо подальшого вдосконалення політики безпеки корпоративних інформаційних систем.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Розвиток цифрових технологій значно прискорює корпоративний розвиток, створюючи нові можливості для підвищення ефективності бізнес-процесів, зростання продуктивності та розширення ринків. Автоматизація рутинних операцій, використання штучного інтелекту та аналітики великих даних дозволяють компаніям швидше приймати обґрунтовані рішення та оптимізувати ресурси. Хмарні технології та платформи для віддаленої співпраці дають можливість підприємствам працювати гнучкіше, масштабувати свою діяльність без значних витрат на інфраструктуру та залучати таланти з усього світу. Інтернет речей (IoT) допомагає оптимізувати виробничі процеси, знижуючи витрати на обслуговування та підвищуючи безпеку операцій.

Цифрові маркетингові інструменти дозволяють компаніям краще аналізувати поведінку споживачів, персоналізувати пропозиції та підвищувати рівень клієнтської лояльності. Розвиток фінансових технологій (FinTech) сприяє спрощенню фінансових операцій, прискоренню платежів та впровадженню безпечних цифрових транзакцій. Завдяки цифровізації компанії можуть швидко адаптуватися до змін у зовнішньому середовищі, забезпечуючи конкурентні переваги та стабільний розвиток навіть у кризові періоди. У той же час війна змусила бізнес швидше адаптувати нові підходи до інформаційної безпеки, роблячи її не просто технічним аспектом, а стратегічним пріоритетом. Виокремимо основні тренди посилення інформаційної безпеки у контексті зростання кіберзагроз (табл. 1).

Аналіз тенденцій у сфері кібербезпеки демонструє перехід від пасивного захисту до активного управління ризиками та адаптації до нових загроз. Основний акцент робиться на кіберстійкість, що передбачає не лише запобігання атакам, а й швидке відновлення після інцидентів. Важливим аспектом є розширення багатофакторної автентифікації (MFA) та концепції Zero Trust, які мінімізують ризики несанкціонованого доступу.

Значну увагу приділяють захисту від інсайдерських загроз через моніторинг поведінки співробітників та використання DLP-систем. Інвестиції в штучний інтелект і автоматизацію посилюють здатність компаній виявляти та реагувати на кіберзагрози в реальному часі. Безпека хмарних сервісів розвивається через гібридні рішення та вдосконалене шифрування, а моніторинг даркнету допомагає попереджати витоки даних.

Таблиця 1

Основні тренди посилення інформаційної безпеки корпоративного розвитку у військовий час

№ з/п	Найменування тренду	Коротка характеристика
1	Зміщення фокусу на кіберстійкість (Cyber Resilience)	Не лише запобігання атакам, а й здатність швидко відновлюватися після інцидентів. Розробка стратегій резервного копіювання та швидкого відновлення даних.
2	Посилена багатофакторна автентифікація (MFA)	Використання не лише паролів, а й біометрії, апаратних токенів або OTP (одноразових паролів). Обов'язкове застосування MFA для критичних систем та доступу до корпоративних VPN.
3	Zero Trust Architecture (ZTA)	Концепція «не довіряй, а перевіряй»: кожен запит на доступ вважається потенційно небезпечним. Мінімізація привілеїв користувачів та перевірка кожної дії.
4	Захист від інсайдерських загроз	Моніторинг поведінки співробітників для виявлення підозрілої активності. Використання DLP (Data Loss Prevention) для запобігання витоку даних.
5	Інвестування в AI та автоматизацію кібербезпеки	Використання штучного інтелекту для аналізу загроз у реальному часі. Автоматичне виявлення та реагування на аномалії.
6	Розвиток безпеки хмарних сервісів	Перехід на гібридні або мультихмарні середовища з покращеним шифруванням. Використання CASB (Cloud Access Security Broker) для моніторингу доступу до хмари.
7	Кібергігієна та навчання персоналу	Регулярні тренінги з фішингу, соціальної інженерії та безпечного користування IT-ресурсами. Створення культури безпеки на всіх рівнях компанії.
8	Моніторинг темної мережі (Dark Web Monitoring)	Виявлення компрометованих акаунтів, витоку конфіденційних даних. Використання спеціалізованих сервісів для перевірки даних у даркнеті.
9	Кіберстрахування	Компанії все більше інвестують у страхові поліси на випадок кібератак. Зменшення фінансових ризиків у разі успішних атак.
10	Зміцнення безпеки мобільних пристроїв	Використання MDM (Mobile Device Management) для контролю доступу. Політики BYOD (Bring Your Own Device) з обмеженням доступу до корпоративних даних.

Сформовано авторами

Крім технологічних рішень, важливу роль відіграє людський фактор – посилюється навчання персоналу з питань кібергігієни та соціальної інженерії. Кіберстрахування стає додатковим фінансовим інструментом управління ризиками, а безпека мобільних пристроїв забезпечується через MDM-системи та контроль доступу в межах політики BYOD. Всі ці заходи спрямовані на комплексне зміцнення кібербезпеки корпоративного середовища в умовах цифровізації.

Динаміка кібератак на українські підприємства протягом 2022–2024 років демонструє значне зростання (рис. 1). Згідно з даними Державної служби спеціального зв'язку та захисту інформації України [8], у 2022 році було зафіксовано 1324 цільових кібератаки проти українських установ та компаній.

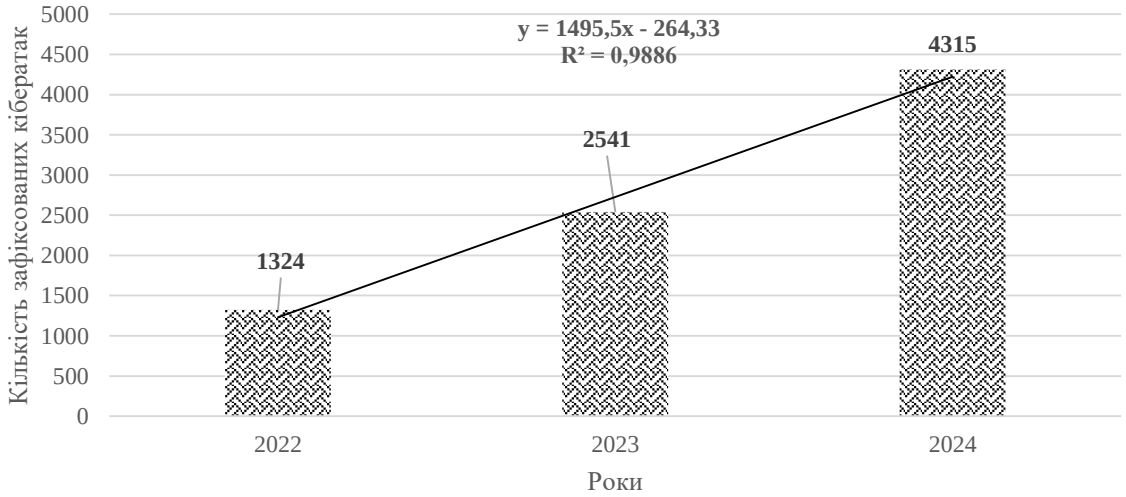

Рис. 1. Динаміка кількості кібератак у період з 2022 по 2024 роки

Складено авторами за даними [8]

У 2023 році кількість кіберінцидентів зросла майже вдвічі, досягнувши 2541 випадку. Ця тенденція продовжилася у 2024 році, коли було зафіксовано 4315 кіберінцидентів, що на 69,8% більше порівняно з 2023 роком. Рівняння лінійної регресії вказує, що щорічне зростання кібератак у середньому становить 1495,5 випадків. Значення коефіцієнта детермінації свідчить про дуже сильний зв'язок між роками повномасштабної

війни та кількістю зафіксованих атак, тобто лінійна модель добре пояснює динаміку змін. Основними мішенями хакерів залишаються місцеві органи влади, урядові структури, сектор безпеки та оборони, енергетика, комерційні організації та телекомунікації. Найпоширеніші види атак – розповсюдження шкідливого програмного забезпечення, фішинг, несанкціоновані підключення та компрометація облікових записів або систем.

Із початку січня до 20 лютого 2025 року зафіксовано кібератаки щонайменше на 25 українських підприємств, що спеціалізуються на розробці автоматизованих систем управління технологічними процесами (АСУТП) та електромонтажних роботах, а також на чотири компанії, які займаються проєктуванням і виробництвом обладнання для сушіння, транспортування та зберігання зерна [8]. Аналіз портфоліо та тендерної документації свідчить, що постачальники рішень АСУТП співпрацюють із сотнями українських підприємств. На етапі первинної компрометації зловмисники маскуються під потенційних замовників, ведучи листування протягом кількох днів і заохочуючи жертву відкрити PDF-документ із нібито «технічною документацією», що містить спотворений вміст.

Виявлена активність вказує на цілеспрямовані спроби зловмисників отримати доступ до комп'ютерних мереж постачальників послуг, щоб надалі використовувати отримані дані для компрометації підприємств у різних галузях промисловості. У березні 2024 року вдалося запобігти масштабній хакерській атаці, спрямованій на дестабілізацію інформаційно-комунікаційних систем близько 20 підприємств енергетичного сектора, а також водо- та теплопостачання в десяти регіонах України. Крім того, з другої половини 2024 року експерти відзначають активне застосування кіберзловмисниками нових тактик, технік та процедур. Зокрема, вони використовують шкідливі PDF-документи, відкриття яких призводить до несанкціонованого проникнення в мережі жертви [8]. Дослідження серії взаємопов'язаних атак, що відбулися з липня 2024 року по лютий 2025 року, свідчить про те, що хакерське угруповання здійснювало цільові атаки не лише на українські підприємства-постачальники, а й на компанії з Сербії, Чехії та інших країн.

Аналізуючи результати опитування Європейського Союзу «Використання інформаційно-комунікаційних технологій (ІКТ) та електронна комерція на підприємствах» [9], можемо зазначити, що в 2024 році 92,76% підприємств ЄС із 10 і більше співробітниками або самозайнятими особами використовували принаймні один захід для забезпечення цілісності, доступності та конфіденційності даних та ІКТ-систем. Більш ніж 1 з 3 підприємств (35,50%) повідомили, що мають документи, які встановлюють заходи, практики або процедури безпеки ІКТ. У п'ятої частини підприємств (21,82%) ці документи були визначені або переглянуті протягом останніх 12 місяців. 59,97% підприємств ЄС повідомили своєму персоналу про свої зобов'язання щодо питань безпеки ІКТ. Нарешті, 1 з 5 підприємств (21,54%) зазнало наслідків через інциденти безпеки, пов'язані з ІКТ, у 2023 році.

Аналогічні дослідження у сфері використання ІКТ автори статті провели спільно із Громадською організацією «Центр стратегічного розвитку та реформ». Упродовж червня – листопада 2024 року опитування пройшли представники корпоративного сектора трьох Західних областей України (Тернопільської, Львівської та Івано-Франківської) із метою визначення ключових загроз у сфері ІКТ та методів їх запобігання. Обирати можна було декілька варіантів відповідей. Похибка дослідження склала не більше 2,1%. Результати дослідження представимо у порівнянні із результатами дослідження європейських підприємств (рис. 2).

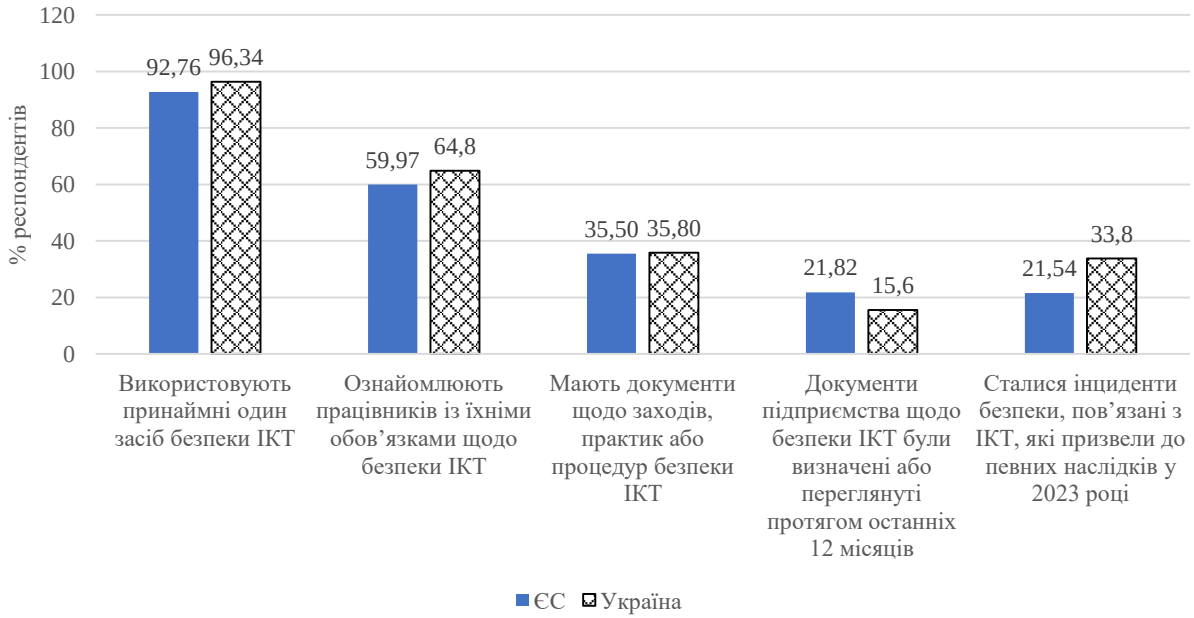

Рис. 2. Безпека ІКТ на підприємствах ЄС та України у 2024 році

Побудовано авторами за даними [9] і за результатами власних досліджень

Більшість підприємств як в Україні, так і в ЄС використовують хоча б один засіб безпеки ІКТ, причому в Україні цей показник навіть дещо вищий (96,34% проти 92,76%). Рівень ознайомлення працівників із їхніми обов'язками щодо безпеки ІКТ в Україні також вищий, ніж у ЄС (64,8% проти 59,97%), що свідчить про кращу поінформованість у цій сфері.

Водночас документування заходів безпеки залишається на низькому рівні в обох регіонах, хоча показники майже однакові (35,80% в Україні та 35,50% у ЄС). Ще нижчим є рівень перегляду політик безпеки ІКТ за останній рік: у ЄС такі документи оновлювалися у 21,82% підприємств, а в Україні – лише у 15,6%. Інциденти безпеки ІКТ, що спричинили певні наслідки, траплялися частіше в Україні (33,8%) порівняно з ЄС (21,54%), що може свідчити про вищий рівень кіберзагроз або недостатню ефективність впроваджених заходів безпеки в українських підприємствах. Загалом, хоча досліджувані українські корпорації широко використовують засоби кібербезпеки та інформують персонал, рівень формалізації політик та їх перегляду залишається низьким, що може сприяти зростанню кількості інцидентів.

Проведемо порівняння рівня впровадження заходів безпеки ІКТ серед підприємств України та ЄС (рис. 3). Загалом підприємства в ЄС демонструють вищий рівень застосування засобів безпеки порівняно з українськими компаніями. Практично всі підприємства як в Україні, так і в ЄС використовують принаймні один засіб безпеки ІКТ, однак у ЄС цей показник дещо вищий (96,41% проти 92,76%). Найпоширенішим методом залишається надійна автентифікація за паролем, яку застосовують 96,41% європейських компаній та 83,69% українських. Також популярним є резервне копіювання даних, яке використовують 84,72% підприємств ЄС і 79,23% українських.

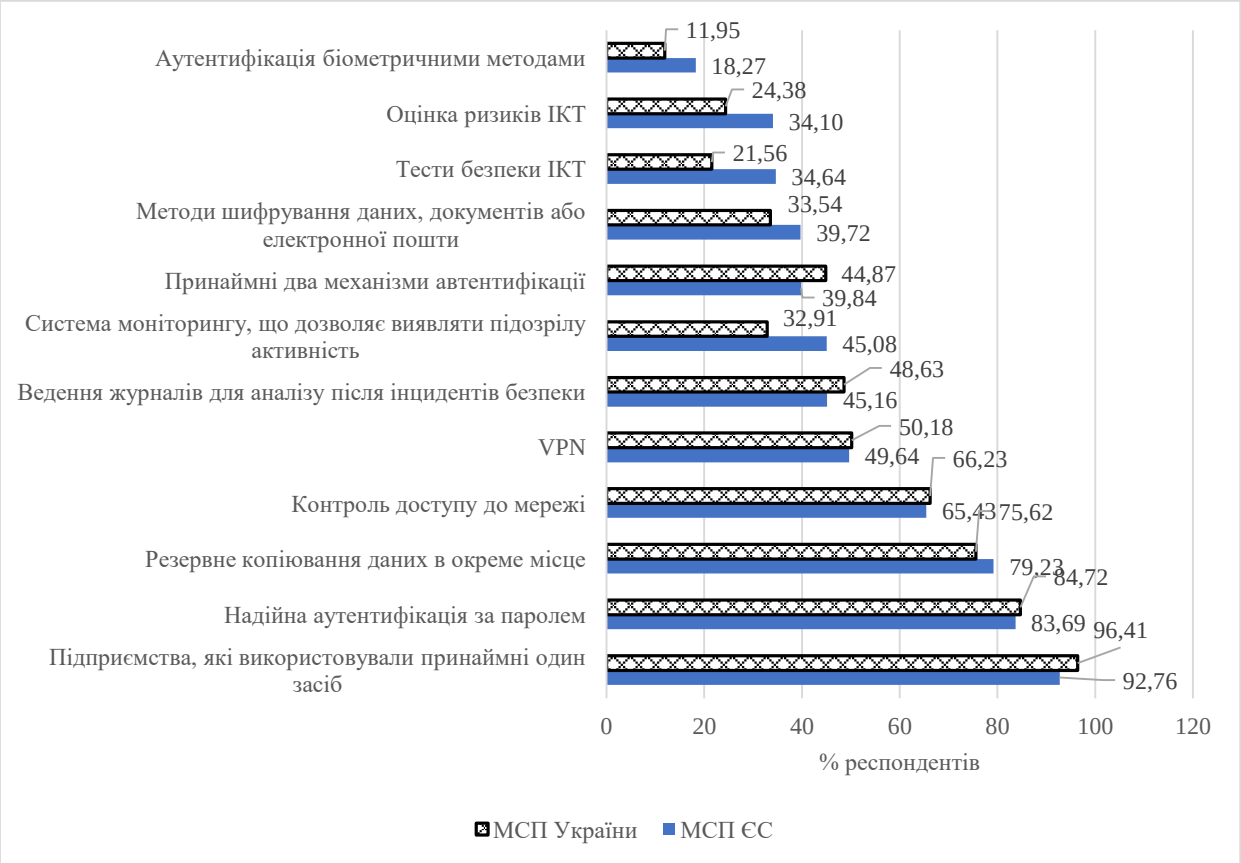

Рис. 3. Заходи безпеки ІКТ, що використовувалися підприємствами ЄС та України у 2024 році

Разом з тим, у складніших засобах безпеки ІКТ спостерігається значний розрив між українськими та європейськими компаніями. Наприклад, контроль доступу до мережі застосовують 75,62% корпорацій у ЄС та 65,43% в Україні. Використання VPN також більш поширене серед європейських компаній (66,23%) порівняно з українськими (49,64%). Аналогічна ситуація з веденням журналів для аналізу інцидентів безпеки – 48,63% у ЄС проти 45,16% в Україні.

Найбільші розриви помітні у впровадженні моніторингових систем для виявлення підозрілої активності (45,08% у ЄС і 32,91% в Україні), багаторівневої автентифікації (44,87% проти 39,84%) та шифрування даних (39,72% у ЄС та 33,54% в Україні). Найменше поширеною є автентифікація біометричними методами, яку застосовують лише 18,27% підприємств у ЄС та 11,95% в Україні. Отже, можемо зазначити, що європейські підприємства демонструють більш комплексний підхід до кібербезпеки, активно використовуючи не лише базові, а й розширені засоби захисту. Водночас вітчизняні корпорації також впроваджують ключові заходи безпеки, хоча поки що з меншою інтенсивністю.

Минулого року 35,5% підприємств ЄС мали документи, які встановлюють заходи, практики чи процедури безпеки ІКТ. Частки понад 50% зареєстровані у Фінляндії (59,41%), Данії (59,11%) і Португалії (54,29%). З іншого боку, менше 20% підприємств мали документи щодо заходів, практик або процедур безпеки ІКТ у Греції (18,28%), Угорщині (13,75%) та Болгарії (13,67%) (рис. 4).

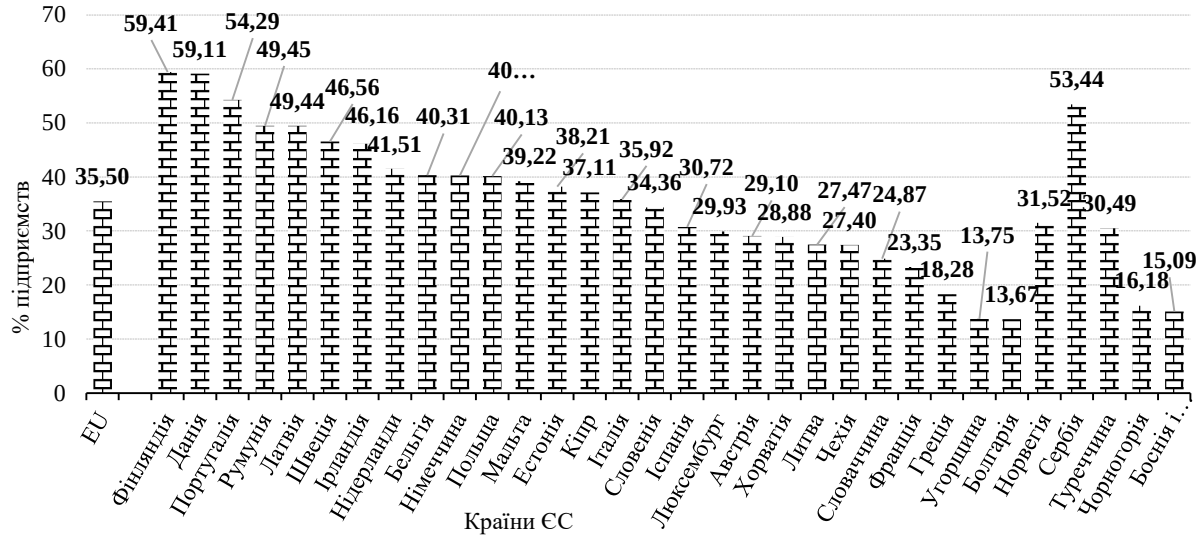

Рис. 4. Підприємства, які розробили та використовували документи щодо заходів, практик або процедур безпеки ІКТ у розрізі країн ЄС у 2024 році

У 2024 році майже 3 із 5 підприємств ЄС (59,97%) повідомили своїх працівників про їхні зобов'язання щодо питань безпеки ІКТ (рис. 5).

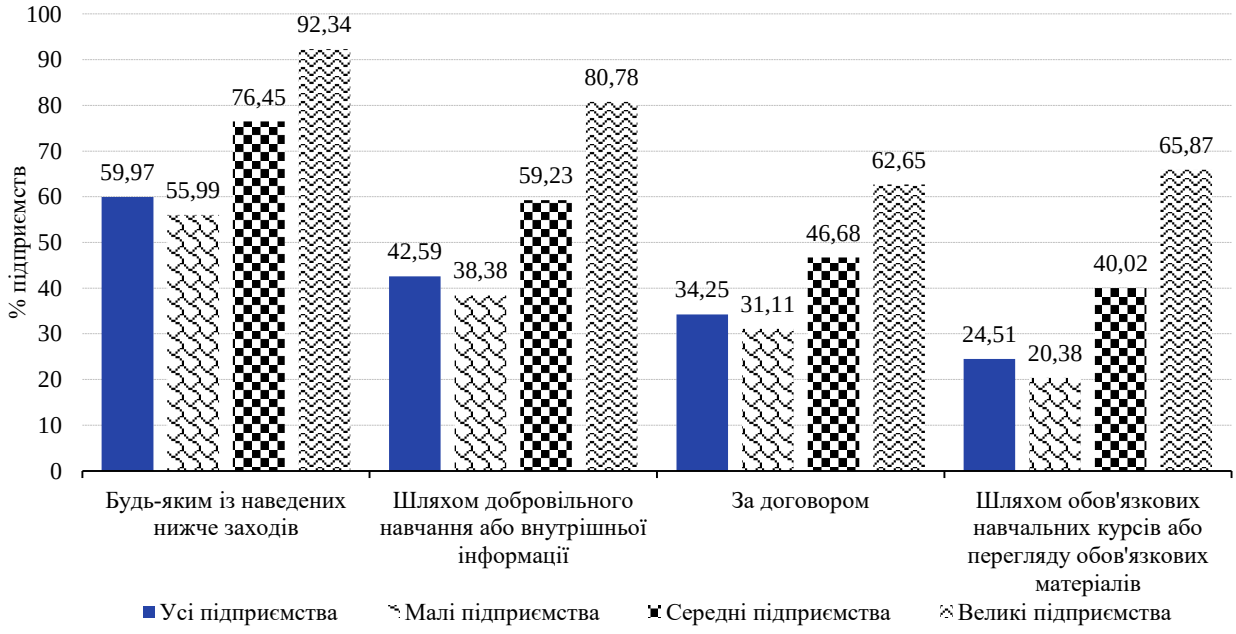

Рис. 5. Підприємства ЄС, які в 2024 році інформували працівників про свої зобов'язання щодо питань безпеки ІКТ, за розміром

Найпоширенішим методом, який застосовується для підвищення обізнаності працівників щодо безпеки ІКТ у досліджуваних вітчизняних корпораціях (рис. 6), є впровадження санкцій за порушення правил (82,36% випадків). Також значна частина компаній використовує підписання зобов'язань про дотримання політики ІКТ-безпеки при прийомі на роботу (78,95%) та регламенти й посадові інструкції (78,94%). Більшість організацій впроваджують систему моніторингу активності для виявлення підозрілих дій (76,32%) та використовують роз'яснювальні матеріали (76,85%). Важливими механізмами комунікації є електронні листи та повідомлення в корпоративних чатах (62,96%), а також зворотний зв'язок і консультації (68,92%).

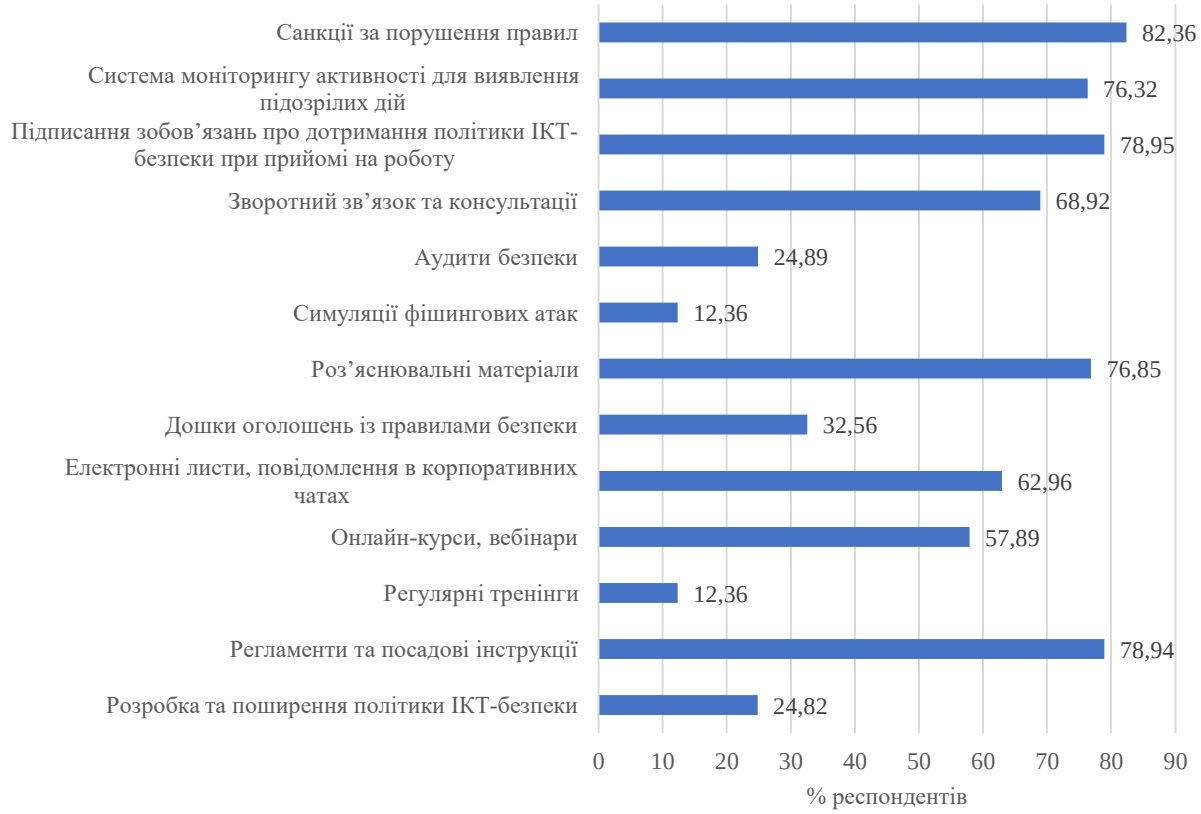

Рис. 6. Методи та засоби, які використовували вітчизняні корпорації для інформування працівників про зобов'язання щодо питань безпеки ІКТ

Результати власних досліджень

Менш поширені заходи включають проведення онлайн-курсів і вебінарів (57,89%), розміщення дошок оголошень із правилами безпеки (32,56%) та аудит безпеки (24,89%). Найменш популярними є симуляції фішингових атак та регулярні тренінги (по 12,36%). Загалом досліджувані корпорації роблять акцент на документуванні політик безпеки, моніторингу та санкціях за порушення, проте недостатньо уваги приділяють практичним тренінгам і симуляціям атак, що могло б ефективніше підвищувати рівень кіберграмотності працівників.

Найбільш поширеним наслідком, спричиненим інцидентами безпеки ІКТ для європейських підприємств у 2024 році, була недоступність послуг ІКТ через апаратні або програмні збої (17,97% підприємств). Для порівняння, про недоступність послуг ІКТ через атаки ззовні (наприклад, атаки програм-вимагачів, атаки типу «відмова в обслуговуванні») повідомили 3,43% підприємств (рис. 7). Про знищення або пошкодження даних через збій апаратного чи програмного забезпечення повідомили 3,87% підприємств, тоді як зараження шкідливим програмним забезпеченням або несанкціоноване вторгнення призвели до знищення або пошкодження даних у 1,89% підприємств. Найрідше підприємства повідомляли про розкриття конфіденційних даних через вторгнення, фармінг чи фішинг-атаку або навмисні дії власних працівників (1,57%) або через ненавмисні дії власних працівників (1,15%).

Щодо вітчизняних представників корпоративного сектору, то, як свідчать результати опитування, найбільш поширеними наслідками були: фінансові втрати, оскільки кібератаки призводили до прямих фінансових збитків через крадіжку коштів, вимагання викупу або втрату бізнес-можливостей (18,3% опитаних); компрометація даних – багато підприємств стикалися з витоками конфіденційної інформації, що призводило до втрати довіри клієнтів та партнерів (24,3%); перебої у роботі, адже атаки на IT-інфраструктуру викликали зупинку бізнес-процесів, що негативно впливало на продуктивність та доходи компаній (28,9%); репутаційні ризики, оскільки публічність інцидентів безпеки підривала репутацію підприємств (16,3%), а також юридичні наслідки такі як штрафи, судові позови (8,3%).

Отже, результати аналізу європейської практики та дослідження сучасного вітчизняного корпоративного сектору свідчать про велику кількість проблемних моментів у забезпеченні інформаційної безпеки. Цифрові технології значно прискорюють розвиток компаній, підвищуючи ефективність бізнес-процесів, продуктивність та конкурентоспроможність. Поряд з цим бізнес змушений активніше впроваджувати заходи інформаційної безпеки, зокрема кіберстійкість, багатофакторну автентифікацію та Zero Trust. Динаміка кібератак в Україні демонструє стрімке зростання, а основними цілями залишаються

державні та стратегічно важливі компанії. Попри високу поінформованість працівників українських підприємств щодо безпеки ІКТ, рівень формалізації політик залишається низьким, що може сприяти збільшенню кількості кіберінцидентів. Зважаючи на сучасні тренди цифровізації бізнесу та беручи до уваги прогресивний європейський досвід, автори дослідження сформували модель організації та управління корпоративною інформаційною безпекою (рис. 8).

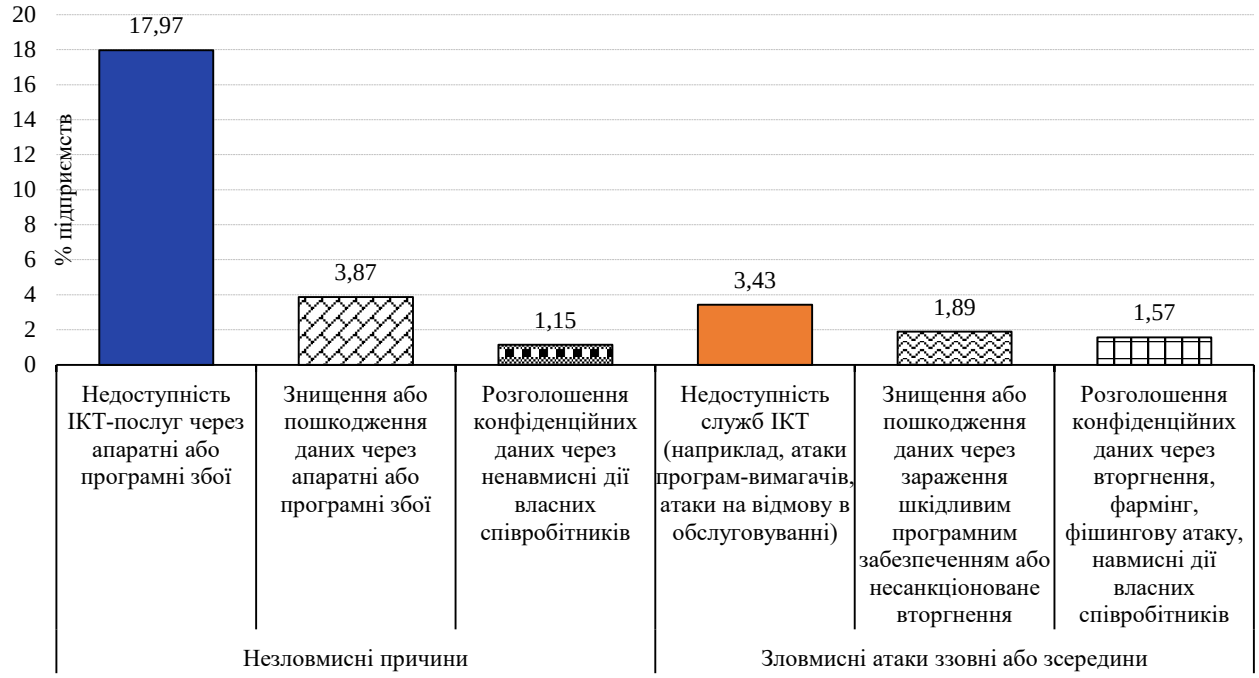

Рис. 7. Підприємства ЄС, які в 2024 році стикалися з інцидентами безпеки, пов'язаними з ІКТ, що призвели до наслідків, за видами інцидентів

Запропонована модель інформаційної безпеки корпоративного розвитку сприятиме мінімізації кіберзагроз, буде забезпечувати стійкість бізнесу та підвищувати довіру партнерів та клієнтів. Інтеграція сучасних цифрових інструментів дозволить не лише захистити дані, а й забезпечити ефективний розвиток компанії в умовах цифрової трансформації.

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

Дослідження цифрових ризиків та інформаційної безпеки корпоративного сектору підтвердило зростаючу загрозу кібератак, особливо в умовах воєнного часу. Виявлено, що основними викликами для підприємств є несанкціонований доступ до даних, витоки конфіденційної інформації, фішингові атаки та використання шкідливого програмного забезпечення. Визначено, що ефективний захист корпоративної інформаційної інфраструктури вимагає комплексного підходу, який включає технологічні, організаційні та регуляторні механізми.

Аналіз європейського досвіду у сфері кібербезпеки засвідчив вищий рівень впровадження заходів інформаційного захисту серед підприємств ЄС у порівнянні з українськими компаніями. Попри високу поінформованість українських компаній, рівень формалізації політик безпеки та їх регулярного перегляду залишається недостатнім. Запропонована модель організації та управління інформаційною безпекою підприємств включає ключові компоненти: організаційну структуру, технологічні рішення, управління ризиками, захист корпоративних даних та аудит безпеки. Впровадження цієї моделі сприятиме мінімізації кіберзагроз та забезпеченню стабільності бізнес-процесів.

Подальші дослідження можуть бути зосереджені на розробці методологій оцінки ефективності заходів кібербезпеки та їх впливу на фінансові показники підприємств. Актуальним напрямом є аналіз ролі штучного інтелекту у виявленні та запобіганні кіберзагрозам, а також дослідження можливостей використання блокчейн-технологій для підвищення безпеки даних. Важливою є оцінка рівня готовності підприємств до впровадження стандартів ISO 27001 та NIST CSF. Крім того, перспективним є дослідження соціальної інженерії та впливу людського фактора на рівень інформаційної безпеки, а також розробка стратегій підвищення кіберстійкості малих і середніх підприємств.

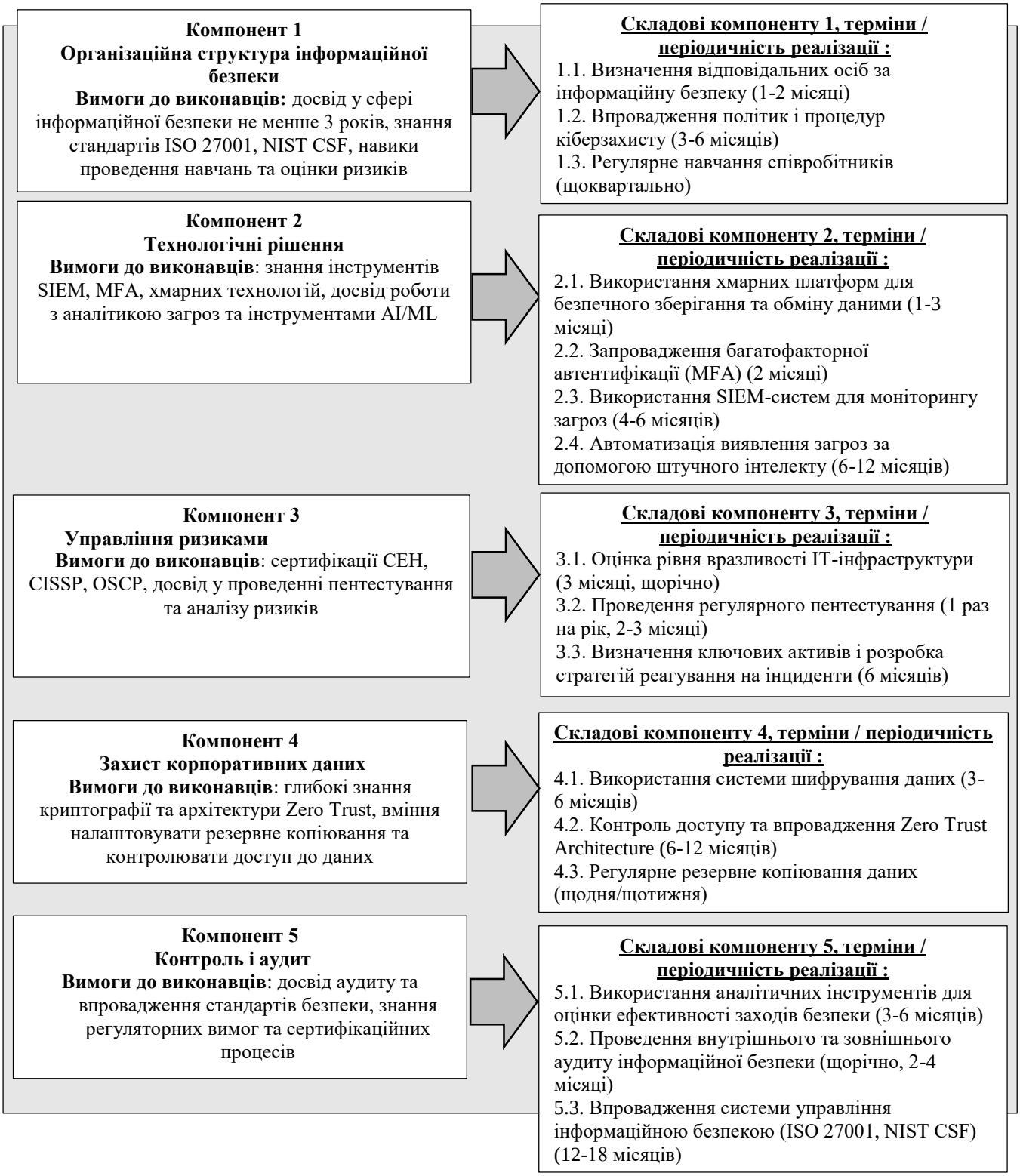

Рис. 8. Модель організації та управління корпоративною інформаційною безпекою в умовах цифровізації

Література

1. Чубаєвський В.І. Корпоративна інформаційна безпека : монографія. Київ : Держ. торг.-екон. ун-т, 2022. 272 с.

2. Ляхович О.О., Оплачко І.О. Економічна безпека та транспарентність підприємств в умовах цифровізації. *Вісник НУВГП. 2021*. Випуск 2(94). Серія «Економічні науки». С. 100 – 110.

3. Доронін І.М. Цифровий розвиток та національна безпека у контексті правових проблем. *Інформація і право*. 2019. № 1(28). С. 29 – 36.

4. Валіулліна З.В. Інформаційна безпека корпоративної економіки в умовах глобалізаційних процесів. *Вісник Дніпропетровського університету*. 2016. Випуск 6. Серія: Менеджмент інновацій. С. 34 – 43.

5. Liu J., Wu W., Shi K., Wu C. (2021). Research on the Impact of Information Security Certification and Concealment on Financial Performance: Impact of ISO 27001 and Concealment on Performance. *Journal of Global Information Management*. Volume 30. Issue 3. 1-16.

6. Fonseca-Herrera O., Rojas A., and Florez H. A. (2021). Model of an Information Security Management System Based on NTC-ISO/IEC 27001 Standard. IAENG. *International Journal of Computer Science*. Volume 48, Issue 2.

7. Hallman R., Major M. and Romero-Mariona J. (2021). Determining a Return on Investment for Cybersecurity Technologies in Networked Critical Infrastructures. *International Journal of Organizational and Collective Intelligence (IJOCI)*. Issue 11(2). DOI: 10.4018/IJOCI.2021040105

8. Хакери масово атакують розробників та постачальників рішень АСУТП, щоб дістатися до критично важливих українських підприємств. *Офіційний сайт Державної служби спеціального зв'язку та захисту інформації України*. URL: https://surl.li/lutddf (дата звернення: 15.03.2025)

9. ICT security in enterprises. *Eurostat*. URL: https://surl.li/nwtjwh (accessed: 18.03.2025)

10. Петляк Н., Хохлачова Ю. Аналіз сучасного стану кібератак в Україні під час війни. *Захист інформації*. 2024. Том 26. №1. С. 187 – 196. DOI: 10.18372/2410-7840.26.18842

References

1. Chubaievskyi V.I. Korporatyvna informatsiina bezpeka [Corporate information security]: monohrafiia. Kyiv : State University of Trade and Economics, 2022. 272 s.

2. Liakhovych O.O., Oplachko I.O. Ekonomichna bezpeka ta transparentnist pidpryiemstv v umovakh tsyfrovizatsii [Economic security and transparency of enterprises in the context of digitalization]. *Visnyk NUWEE*. 2021. Vypusk 2(94). Seriia «Ekonomichni nauky». S. 100 – 110.

3. Doronin I.M. Tsyfrovyi rozvytok ta natsionalna bezpeka u konteksti pravovykh problem [Digital development and national security in the context of legal issues]. *Informatsiia i pravo*. 2019. № 1(28). S. 29 – 36.

4. Valiullina Z.V. Informatsiina bezpeka korporatyvnoi ekonomiky v umovakh hlobalizatsiinykh protsesiv [Information security of the corporate economy in the context of globalization processes]. *Visnyk Dnipro National Univercity*. 2016. Vypusk 6. Seriia: Menedzhment innovatsii. S. 34 – 43.

5. Liu J., Wu W., Shi K., Wu C. (2021). Research on the Impact of Information Security Certification and Concealment on Financial Performance: Impact of ISO 27001 and Concealment on Performance. *Journal of Global Information Management*. Volume 30. Issue 3. 1-16.

6. Fonseca-Herrera O., Rojas A., and Florez H. A. (2021). Model of an Information Security Management System Based on NTC-ISO/IEC 27001 Standard. IAENG. *International Journal of Computer Science*. Volume 48, Issue 2.

7. Hallman R., Major M. and Romero-Mariona J. (2021). Determining a Return on Investment for Cybersecurity Technologies in Networked Critical Infrastructures. *International Journal of Organizational and Collective Intelligence (IJOCI)*. Issue 11(2). DOI: 10.4018/IJOCI.2021040105

8. Khakery masovo atakuiut rozrobnykiv ta postachalnykiv rishen ASUTP, shchob distatysia do krytychno vazhlyvykh ukrainskykh pidpryiemstv [Hackers are massively attacking developers and suppliers of automation and process control solutions to reach critical Ukrainian enterprises]. *Ofitsiinyi sait Derzhavnoi sluzhby spetsialnoho zviazku ta zakhystu informatsii Ukrainy*. URL: https://surl.li/lutddf (accessed: 15.03.2025)

9. ICT security in enterprises. *Eurostat*. URL: https://surl.li/nwtjwh (accessed: 18.03.2025)

10. Petliak N., Khokhlachova Yu. Analiz suchasnoho stanu kiberatak v Ukraini pid chas viiny [Analysis of the current state of cyberattacks in Ukraine during the war]. *Zakhyst informatsii*. 2024. Tom 26. №1. S. 187 – 196. DOI: 10.18372/2410-7840.26.18842