DOI: https://doi.org/10.30837/EK.2025.024

Степаненко Р.Д.,
здобувач вищої освіти,
Харківський національний університет радіоелектроніки
ORCID: https://orcid.org/0009-0008-0586-0903
Зінов'єв А.П.,
здобувач вищої освіти,
Харківський національний університет радіоелектроніки
ORCID: https://orcid.org/0009-0003-6343-9977
Мізін Д.С.,
здобувач вищої освіти,
Харківський національний університет радіоелектроніки
ORCID: *https://orcid.org/0009-0005-5692-5859*
Панько А.Д.,
здобувач вищої освіти,
Харківський національний університет радіоелектроніки
ORCID: https://orcid.org/0009-0006-8427-0359

ЦИФРОВІ ВРАЗЛИВОСТІ ТА РИЗИКИ У СУЧАСНОМУ БІЗНЕС-ЛАНДШАФТІ

У сучасній цифровій економіці інформаційно-комунікаційні технології (ІКТ) стали ключовим рушієм соціально-економічного розвитку, проте вони одночасно породжують нові форми вразливостей та ризиків. Сучасні компанії активно впроваджують цифрові технології – штучний інтелект, машинне навчання, Інтернет речей, хмарні обчислення – що підвищує ефективність, гнучкість і прибутковість бізнесу. Водночас цифровізація супроводжується зростанням цифрових ризиків (витоки даних, атаки програм-вимагачів, збої у хмарних сервісах, помилки алгоритмів ШІ) та трансформованих традиційних ризиків (репутаційні втрати, порушення логістики через кібератаки, фінансове

онлайн-шахрайство), які посилюються у цифровому середовищі й набувають глобального масштабу. Особливістю цифрових ризиків є їхня швидка еволюція та здатність до масштабування через взаємозалежність ІТ-систем, що потребує переосмислення підходів до управління ризиками у сучасних компаніях.

Зі зростанням складності цифрових систем підвищується їхня вразливість до кіберзагроз. Витоки даних, атаки програм-вимагачів чи збої в хмарних сервісах можуть спричиняти значні фінансові та репутаційні втрати. Ефективне управління цифровими ризиками передбачає системний аналіз вразливостей, оцінку критичних ресурсів і впровадження механізмів раннього виявлення загроз.

Сучасні кібератаки дедалі частіше мають цілеспрямований характер і ґрунтуються на соціальній інженерії, що виходить за межі технічних аспектів безпеки. Тому підприємства повинні формувати комплексні системи інформаційного захисту, які поєднують управління ризиками, навчання персоналу та адаптивні стратегії реагування. Аналіз цифрових ризиків є необхідною умовою підвищення стійкості та конкурентоспроможності бізнесу в умовах цифрової економіки.

Цифрові вразливості виникають через залежність економічних та соціальних систем від даних, мереж та автоматизованих процесів. Ці слабкі місця можуть виникати через недоліки програмного забезпечення, неадекватний захист даних, людські помилки або системну залежність від критичних цифрових інфраструктур.

Багато авторів розглядають цифрові ризики та пропонують механізми управління ними. Так, І. Б. Шевчук, Б. Я. Депутат і О. Є. Тарасенко виокремлюють такі основні ризики цифрового розвитку [1]:

− Інтернет речей (IoT) – уразливість систем до несанкціонованого втручання, кібертероризму та незаконного використання технологій;

− штучний інтелект і автоматизація – зростання безробіття, соціальної напруги, втрати приватності та ризики витоку комерційної інформації;

− блокчейн – вразливість безпеки, незмінність помилкових даних, можливість використання токенів для відмивання коштів;

− імпортна мікроелектроніка – загроза шпигунства через закладені технічні елементи;

− хмарні технології – залежність від телекомунікацій, розмитість відповідальності та зниження контролю за безпекою;

− стійкість Інтернету – ризики збоїв і нестабільності мережі;

− вплив на суспільну свідомість – маніпулювання поведінкою через аналіз великих даних;

− складність бізнес-моделей – дефіцит кваліфікованих кадрів і труднощі управління.

Н. І. Гражевська, А. М. Чигиринський, О. О. Хандій та Л. Л. Шамілева, узагальнюючи світовий досвід цифрової трансформації економік, виокремлюють такі негативні соціальні наслідки [2]:

− цифрова нерівність кадрів – розрив у рівні цифрових навичок, що спричиняє невідповідність кваліфікації працівників вимогам ринку праці;

− соціальна поляризація – звуження можливостей для формування середнього класу, посилення прекаризації та трудової міграції;

− соціально-психологічні наслідки – сегрегація населення за цифровими компетенціями, зниження мотивації та професійних навичок працівників.

Ведення бізнесу в Україні під час повномасштабної війни висуває нові вимоги до безпеки, включаючи протидію цифровим ризикам.

Так, А. П. Максименко аналізує загрози цифрової економіки в умовах війни, визначаючи цифрову глобалізацію як «поширення економічних, технологічних, культурних і політичних практик через мережу Інтернет» [3]. На прикладі конфліктів в Іраку, Грузії та Україні автор розглядає переваги й недоліки цифрової інфраструктури під час воєнних дій. Серед ключових загроз цифрової трансформації України в умовах війни та післявоєнного відновлення

він виокремлює нестачу інвестицій, непрозоре фінансування, рейдерські захоплення, надмірну бюрократію та недосконале нормативне регулювання.

Л. Шостак і А. Федонюк [4] виокремлюють основні загрози для українського бізнесу в умовах війни: дестабілізацію інформаційних систем через атаки на критичну інфраструктуру; кібератаки на сайти й сервери з метою фінансової вигоди, політичного впливу чи маніпуляції даними; техніко-технологічну залежність від іноземних виробників ІТ-продукції; вразливість корпоративної інфраструктури через віддалений формат роботи; а також недостатній контроль держави за забезпеченням кіберзахисту.

Кіберзагрози становлять глобальну проблему для організацій у всіх секторах. На думку В. Столлінгса та Л. Брауна [5], їхнє посилення зумовлюють три ключові фактори: всеохопна цифровізація, розвиток технологій, що підвищує ефективність атак, а також правова й етична відповідальність бізнесу за захист персональних даних.

За даними статистичної служби ЄС [6], у 2023 році близько 21,5% підприємств ЄС зіткнулися з інцидентами, пов’язаними з інформаційно-комунікаційними технологіями. Найпоширенішим наслідком таких інцидентів була недоступність ІКТ-послуг через збої апаратного чи програмного забезпечення (17,9% випадків).

Європейське агентство з кібербезпеки (ENISA) [7] відзначає, що DDoS-атаки та програми-вимагачі залишаються серед найсерйозніших загроз у ЄС. У період з липня 2023 по червень 2024 року майже 40% кібератак були спрямовані проти сфер публічного управління, транспорту та фінансів. Це підкреслює зростаючу потребу у дослідженні інформаційної безпеки як на рівні окремих організацій, так і в масштабах економічних секторів.

Між 2000 і 2023 роками база даних Європейського репозиторію кіберінцидентів (EuRepoC) зафіксувала 2506 політично мотивованих кібератак, з яких 12 відсотків припадало на Китай, а за ним – на Росію з 11,6 відсотка. Однак більшість цих шкідливих інцидентів – 45 відсотків – залишаються невідомими. У Звіті ENISA про ландшафт загроз за 2024 рік також

підкреслюється невід'ємна складність визначення походження атак, зазначаючи, що в одній із трьох атак зловмисник був невідомий [7].

Подібна ситуація спостерігається і в Україні. Так, за даними Міністерства фінансів України [8], ще до початку повномасштабного вторгнення, майже 20% усіх світових кібератак були спрямовані проти України – за цим показником ми поступалися лише США. У 2022 році, за даними Державного центру кіберзахисту [9], кількість атак зросла майже утричі. З 24 лютого до кінця року команда CERT-UA зафіксувала 2 194 кіберінциденти, зокрема 120 – у фінансовому секторі, 156 – у комерційних структурах і 92 – у сфері телекомунікацій та розробки ПЗ. Серед виявлених подій інформаційної безпеки основну частину, а саме 58.8%, становлять події, пов’язані зі шкідливим програмним кодом (Malicious Code). Спроби втручання (Intrusion Attempts) займають 17,6%, тоді як збір інформації зловмисником (Information Gathering) становить 12,1%. Інші події (Other) складають 8,3%, порушення властивостей інформації (Information Content Security) та порушення доступності (Availability) займають 2,7% та 0,5% відповідно. Понад 90% опрацьованих кіберінцидентів стосуються організацій урядового сектору [9].

Попри складну ситуацію та численні виклики, Україна успішно протистоїть загрозам у сфері кібербезпеки. У Національному індексі кібербезпеки [10], який щорічно укладає Фонд електронного врядування Естонії, вона посідає 13-те місце серед 160 країн – вище за Австрію, Швейцарію, Ірландію та Норвегію.

У сучасних умовах поряд із ризиками актуалізується проблема вразливості суб’єктів економічної діяльності та їхніх активів перед різними загрозами – військовими, конкурентними та кіберзагрозами. Поняття «вразливість» традиційно використовується в контексті кібербезпеки, проте в економічній науці воно має ширше значення.

Згідно зі звітом Програми розвитку ООН (UNDP) *Human Development Report* [11], вразливість трактується як схильність до негативних потрясінь, що перешкоджають людському розвитку. Економічна вразливість, за цим

підходом, зумовлюється як зовнішніми факторами – наприклад, нестабільністю торгівлі чи природними катастрофами, – так і внутрішніми структурними дисбалансами, пов’язаними з нерівністю.

Інші дослідники [12] розглядають економічну вразливість як схильність економіки до екзогенних шоків, що випливають із відкритості ринків, тоді як економічна стійкість визначається здатністю системи протистояти цим шокам або відновлюватися після них. Таким чином, економічна вразливість відображає рівень ризику, спричиненого зовнішніми впливами на виробництво, розподіл і споживання ресурсів.

Г. Г. Найман і Д. М. Гаркавенко [13] зосереджують увагу на управлінні вразливостями як процесі мінімізації шкоди від реалізації кіберзагроз, з якими стикаються фахівці з інформаційної безпеки. Дослідники пропонують застосовувати системи машинного навчання для підвищення ефективності такого управління.

На основі аналізу існуючих підходів до визначення термінів «економічна вразливість» в даному досліджені пропонується авторське визначення економічної кібервразливості організації – це ступінь, до якого економічний стан суб’єкта господарювання схильний до збоїв або втрат, що виникають внаслідок внутрішніх структурних слабкостей або зовнішніх потрясінь, що виникають внаслідок кіберзагроз.

На основі аналізу джерел [1-5, 12-14] виділені основні класи цифрових вразливостей та інструменти, які використовуються для їх мінімізації (рис. 1):

– вразливості програмного забезпечення: помилки коду та недоліки дизайну програмних продуктів. Статичний та динамічний аналіз коду, системи керування виправленнями та методи безпечного кодування допомагають зменшити ці вразливості;

– вразливості мережі: виникають через слабкі місця в мережевій інфраструктурі, протоколах та конфігураціях. Тут на поміч приходять системи виявлення вторгнень (IDS), віртуальні приватні мережі (VPN) та сегментація мережі;

Рисунок 1 – Типи цифрових вразливостей

Джерело: сформовано авторами на основі [1-5, 12-14]

– процесні (операційні) вразливості – недоліки в бізнес-процесах, неузгодженість між системами безпеки та операційними процедурами, відсутність резервування та контролю змін;

– вразливості персоналу: виникають через людські помилки, такі як фішингові атаки, соціальна інженерія та погані методи безпеки. Навчальні програми, інформаційні кампанії та багатофакторна аутентифікація допомагають зменшити ризики, пов'язані з поведінкою людини;

– вразливості обладнання, включаючи недоліки в апаратних компонентах (слабке шифрування, фізичне втручання). Безпечна конструкція обладнання, регулярні оновлення прошивки та шифрування на апаратному рівні є критично важливими засобами захисту;

– вразливості системи управління виникають через слабкість управлінських процесів, відсутність політик інформаційної безпеки, неефективне управління доступом, недостатню підготовку персоналу, прогалини у відповідності нормативним вимогам. Встановлення надійних політик безпеки, проведення регулярних аудитів та забезпечення дотримання відповідних стандартів допомагають зменшити ці ризики.

На основі аналізу теоретичних підходів до управління цифровими ризиками у дослідженні запропонована концептуальна модель усунення цифрових вразливостей організації (рис. 2) [14].

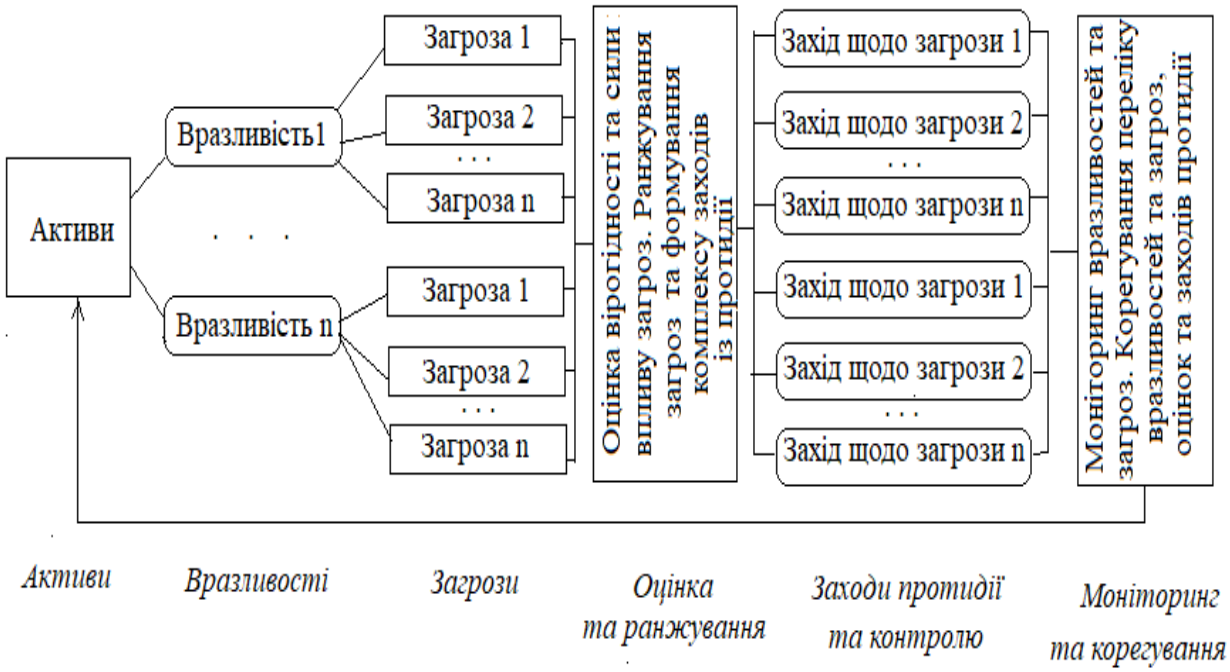

Рисунок 2 – Концептуальна модель усунення цифрових вразливостей організації

Джерело: [14]

Усунення вразливостей – це процес виявлення, оцінки та нейтралізації слабких місць у цифровій інфраструктурі компанії (IT-системи, мережі, додатки, пристрої). Основні етапи усунення вразливостей включають:

– виявлення та систематизація типів активів підприємства, що мають цифрові вразливості. До таких активів належать: інформаційні системи, мережева та фізична інфраструктура, корпоративні додатки, клієнтська база, персонал підприємства, система управління, партнерські відносини із третіми сторонами;

– виявлення вразливостей, що притаманні кожному типу активів організації шляхом сканування, тестування коду та конфігурацій;

– систематизація загроз, що характері для кожної вразливості;

– ранжування загроз за масштабом та складністю усунення;

– нейтралізація шляхом оновлень, виправлень;

– моніторинг у реальному часі для оперативного реагування.

Типи активів організації, цифрові вразливості, які пов'язані з кожним типом активів, цифрові загрози, що можуть виникати через ці вразливості, а також методи контролю або протидії: представлені у табл. 1 [14].

Таблиця 1 – Відповідність типів активів організації цифровим загрозам та методам контролю та протидії

Тип активу	Цифрові вразливості	Цифрові загрози	Методи контролю / протидії
Фізична інфраструктура	Відсутність контролю доступу, незахищене обладнання	Фізичне втручання, пошкодження серверів, крадіжка даних	Контроль доступу, відеоспостереження, охорона
Мережева інфраструктура	Відкриті порти, слабка автентифікація	DDoS-атаки, проникнення до внутрішньої мережі перехоплення трафіку	Брандмауери, VPN, IDS/IPS, сегментація мережі
Інформаційні системи	Недостатній кіберзахист, несвоєчасне оновлення	Втрата даних, кібератаки несанкціонований доступ	Шифрування, резервне копіювання, антивірус, контроль доступу
Корпоративні додатки	Уразливості ПЗ, небезпечні інтеграції	Витік даних, маніпуляції з даними	Аудит коду та безпеки ПЗ, оновлення, контроль доступу
Клієнтська база	Незашифровані персональні дані, надлишковий доступ	Витік персональних даних, шахрайство, регуляторні санкції, компрометація довіри	Шифрування, аудит доступу, відповідність GDPR/ЗУ «Про захист персональних даних»
Персонал підприємства	Недостатнє навчання, соціальна інженерія	Фішинг, інсайдерські загрози	Навчання, багатофакторна автентифікація, політики безпеки
Система управління	Централізований доступ без багато-рівневого захисту	Захоплення контролю над процесами, спотворення управлінських рішень	Розмежування повно-важень, контроль журналів, регулярний аудит
Партнерські відносини з третіми сторонами	Небезпечні API, ненадійні канали обміну даними	Інфікування систем через контрагента, витік через сторонні сервіси	Контракти з кіберзахисту, аудит партнерів, сегментація доступу

Джерело: [14]

Подібна систематизація активів, вразливостей, цифрових загроз та методів контролю може допомогти керівному складу зрозуміти, які саме активи підприємства потенційно піддаються цифровим загрозам і які заходи можна прийняти для зменшення ризиків.

Типи активів, цифрових вразливостей та загроз залежать від галузі, у якій працює організація. В межах даного дослідження конкретизовані активи, вразливості та загрози для фінансової установи, виробничого підприємства та Інтернет-магазину (табл. 2) [14]. Таке структурування дозволяє краще ідентифікувати критичні цифрові ризики для кожного типу організації та адаптувати систему інформаційної безпеки відповідно до специфіки діяльності.

Таблиця 2 – Приклади активів**,** цифрових вразливостей та цифрових загроз окремо для банку**,** виробничого підприємства та інтернет-магазину

Категорія	Приклад
Фінансова установа, банк	
Активи	Банківська система (core banking), база клієнтів, платіжні шлюзи, банкомати
Вразливості	Вразливості API, фішинг персоналу, застарілі протоколи шифрування
Загрози	Крадіжка коштів, несанкціоновані перекази, блокування доступу до рахунків (DoS)
Виробниче підприємство	
Активи	Системи SCADA/PLC, виробничі лінії, IoT-сенсори, технічна документація
Вразливості	Відкритий віддалений доступ, відсутність оновлень програмного забезпечення, слабка сегментація мережі
Загрози	Зупинка виробництва, саботаж обладнання, промислове шпигунство
Інтернет-магазин	
Активи	Веб-сайт, база даних клієнтів, платіжна система, система обліку товарів
Вразливості	неавтентифікований доступ до панелі адміністрування, використання сторонніх скриптів
Загрози	Витік персональних та платіжних даних, підміна сайту (фішинг), несанкціоновані транзакції

Джерело: сформовано авторами на основі джерел [14]

Таким чином, у даному досліджені запропонована концептуальна модель усунення цифрових вразливостей організації, що може бути доповнена показниками KPI для синхронізації із стратегією розвитку підприємства. Ефективне управління цифровими вразливостями вимагає системного та

міждисциплінарного підходу, інтеграції технологічних інновацій з інституційними механізмами управління. Здатність прогнозувати, пом'якшувати та адаптуватися до цифрових ризиків стала критичним фактором стійкості та конкурентоспроможності в цифрову епоху.

Перелік джерел посилання

1. Шевчук І. Б., Депутат Б. Я., Тарасенко О. Є. Цифровізація та її вплив на економіку України: переваги, виклики, загрози й ризики. *Причорноморські економічні студії*. 2019. № 47-2. С. 173-177. URL: http://bses.in.ua/journals/2019/47_2_2019/34.pdf.

2. Гражевська Н. І., Чигиринський А. М. Цифрова трансформація економіки в умовах посилення глобальних ризиків і загроз. *Економіка та держава*. 2021. № 8. С. 53-57.

3. Максименко А. П. Реальні та потенційні загрози цифрової економіки в умовах війни. *Економічний простір*. 2023. № 188. С. 41-49.

4. Шостак Л., Федонюк А., Помазун О. Особливості кібербезпеки бізнесу в умовах воєнного часу. *Цифрова економіка та економічна безпека*. 2024. № 3(12). С.121-125.

5. Stallings W., Brown L. Computer security: Principles and practice (4th ed.). 2017. New York: Pearson Education, Inc. 800 p.

6. Eurostat, Statistics explained. IT Security in enterprises. December 2024. URL: https://ec.europa.eu/eurostat/statistics-explained/SEPDF/cache/9132.pdf (дата звернення: 21.09.2025).

7. European Union Agency for Cybersecurity (ENISA) 2024 Report on the state of cybersecurity in the union. November 2024. DOI: 10.2824/0401593. URL: https://www.enisa.europa.eu/publications (дата звернення: 21.09.2025).

8. Міністерство фінансів України. Спецпроєкт «Кібербезпека бізнесу під час війни» URL: https://www.project.minfin.com.ua/kiberbezpeka-biznesu-pid-chas-vijny# (дата звернення: 15.10.2025).

9. Оперативний центр реагування на кіберінциденти Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України. Звіт про роботу системи виявлення вразливостей і реагування на кіберінциденти та кібератаки за 2024 р. URL: https://scpc.gov.ua/api/files/72e13298-4d02-40bf-b436-46d927c88006.

10. e-Governance Academy, Estonia. National Cyber Security Index. URL: https://ncsi.ega.ee/ncsi-index/ (дата звернення: 15.10.2025).

11. United Nations Development Programme (UNDP) Human Development Report 2014. Sustaining Human Progress: Reducing Vulnerabilities and Building Resilience. Available at: https://www.undp.org/sites/g/files/zskgke326/files/migration/tr/2014-Human-Development-Report---English.pdf (accessed June 21, 2025).

12. Briguglio L., Cordina G., Farrugia N., Vella S. Economic vulnerability and resielence: concepts and measurements. *Oxford development studies*. 2009. 37(3). pp. 229-247.

13. Найман Г. Г., Гаркавенко Д. М. Методи та засоби управління вразливостями корпоративної інформаційної системи на основі машинного навчання. *Сучасний захист інформації*. 2021. № 3(47). С. 24-28.

14. Шейко І. А., Степаненко Р. Д. Управління цифровими вразливостями сучасного підприємства. *Економіка і управління*. 2025. № 2(104) С. 112-119. DOI: https://doi.org/10.32782/2312-7872.2.2025.15.

15. Полозова Т. В., Ткаченко А. Г., Осадчук І. О., Осадчук М. О. Механізми мінімізації ризиків економічної безпеки в процесі цифрової трансформації підприємств. *Сталий економічний розвиток: інноваційні підходи та стратегічні перспективи: колективна монографія* / За заг. ред. д.е.н., проф. Т. В. Полозової. Харків: ХНУРЕ, 2024. С. 248-261.