УДК 338.242
DOI https://doi.org/10.32782/2312-7872.2.2025.15

Шейко Ірина Анатоліївна
кандидат економічних наук, доцент,
доцент кафедри економічної кібернетики
та управління економічною безпекою,
Харківський національний університет радіоелектроніки
ORCID ID: 0000-0002-5770-3677

Степаненко Руслан Джаваншірович
аспірант,
Харківський національний університет радіоелектроніки
ORCID ID: 0009-0008-0586-0903

УПРАВЛІННЯ ЦИФРОВИМИ ВРАЗЛИВОСТЯМИ СУЧАСНОГО ПІДПРИЄМСТВА

Анотації. *В статті проведене комплексне дослідження цифрових ризиків та вразливостей, притаманних вітчизняним організаціям. Метою статті є вивчення теоретичних підходів до управління цифровими вразливостями підприємства та побудова концептуальної моделі їх усунення задля зниження впливу цифрових загроз. Проаналізовані цифрові загрози для українського бізнесу під час війни, а також інциденти кібербезпеки у країнах Європейського Союзу. Особлива увага приділена економічній вразливості організацій. Запропоноване авторське визначення поняття «економічна кібервразливість організації», під якою розуміється ступінь, до якого економічний стан організації схильний до збоїв або втрат, що виникають внаслідок внутрішніх структурних слабкостей або зовнішніх потрясінь, зокрема тих, що виникають внаслідок кіберзагроз. Систематизовані основні класи цифрових вразливостей, а саме: вразливості обладнання, програмного забезпечення, мережі, персоналу, системи управління. В досліджені запропонована концептуальна модель усунення цифрових вразливостей організації як процесу виявлення, оцінки та нейтралізації слабких місць у цифровій інфраструктурі компанії. Запропонована концептуальна модель може бути доповнена включенням до її складу цільових показників, системи KPI для оцінки ефективності реагування на цифрові загрози. Виділені типи активів організації із притаманними кожному типу цифровими вразливостями та загрозами, що виникають через наявність вразливостей. Особлива увага приділена цифровим вразливостям та загрозам фізичній та мереженій інфраструктурі. Наведений приклад систематизації активів, вразливостей та цифрових загроз для фінансової установи, виробничого підприємства та Інтернет-магазину. Таке структурування дозволяє краще ідентифікувати критичні цифрові ризики для кожного типу організації та адаптувати систему інформаційної безпеки відповідно до специфіки діяльності. Узагальнено й структуровано цифрові вразливості, можливі загрози та відповідні методи їх нейтралізації для виробничого підприємства, при цьому кожній вразливості поставлено у відповідність конкретну загрозу та інструмент її зниження. Запропоновані рішення спрямовані на забезпечення стійкого захисту виробничих процесів, які все більше інтегруються з цифровою інфраструктурою та залишаються вразливими до кібератак.*

Ключові слова: *кібербезпека, цифрова вразливість, економічна вразливість, управління цифровими ризиками, актив організації, усунення вразливостей.*

Постановка проблеми. У сучасних умовах цифровізації підприємства дедалі більше залежать від ІТ-інфраструктури для ведення бізнесу та взаємодії з партнерами. З ускладненням цифрових систем зростає їхня вразливість до кіберзагроз. Інциденти, пов'язані з витоком даних, атаками програм-вимагачів або збоями в хмарних сервісах, можуть призвести до серйозних фінансових і репутаційних втрат. Ефективне управління цифровими ризиками потребує аналізу вразливостей та поєднання технічних і стратегічних заходів: оцінки критичних ресурсів, систем раннього виявлення загроз і постійного вдосконалення політик безпеки.

Актуальність вивчення цифрових вразливостей зростає, оскільки більшість кібератак сьогодні є цілеспрямованими та базуються на методах соціальної інженерії, виходячи за межі суто технічних питань. Це вимагає від підприємств впровадження комплексних систем інформаційної безпеки, що поєднують управління ризиками, підготовку персоналу та адаптивні стратегії реагування. Таким чином, аналіз цифрових загроз і вразливостей є ключовим для зміцнення стійкості, збереження конкурентних переваг і сталого розвитку бізнесу в цифрову епоху.

Аналіз останніх досліджень і публікацій. У сучасних умовах значна увага приділяється дослідженню цифрових ризиків, а також методам їх контролю та мінімізації. Хоча основна частина досліджень зосереджена в технічній сфері, економічні наслідки кіберінцидентів активно аналізу-

ються як у вітчизняній, так і в зарубіжній науковій літературі. Зокрема, це відображено у працях О.І. Кузьменко [1], А.П. Максименка [2], В.К. Олефіра [4], Д.В. Смотрича [5], М.Г. Хаустової [6], Л.В. Шостак [7], У. Столлінгса [13], а також у звітах державних органів і міжнародних організацій [10–12]. Водночас спостерігається недостатня кількість досліджень, присвячених усуненню цифрових вразливостей як ключовому інструменту мінімізації цифрових ризиків.

Мета статті. Метою статті є вивчення теоретичних підходів до управління цифровими вразливостями підприємства та побудова концептуальної моделі їх усунення задля зниження впливу цифрових загроз.

Виклад основного матеріалу дослідження. Сучасні компанії активно впроваджують цифрові технології, зокрема штучний інтелект, машинне навчання, Інтернет речей і хмарні обчислення, що сприяє зростанню ефективності, гнучкості та прибутковості. Водночас цифровізація супроводжується зростанням як цифрових ризиків (нових загроз, пов'язаних виключно з цифровими технологіями: витоки даних, атаки програм-вимагачів, збої у хмарних сервісах, помилки в алгоритмах ШІ), так і трансформованих традиційних ризиків (вже відомі загрози, що посилюються у цифровому середовищі (наприклад, репутаційні втрати внаслідок активності в соцмережах, порушення логістики через кібератаки, фінансове онлайн-шахрайство) які набувають глобального масштабу. Цифрові ризики вирізняються швидкістю розвитку та здатністю масштабуватись через взаємозалежність ІТ-систем. Тому компаніям важливо глибоко розуміти вплив цифрових технологій на сучасну систему управління ризиками.

У сучасних умовах вітчизняний бізнес стикається з нагальною проблемою забезпечення інформаційної безпеки. Як зазначає В.К. Олефір, основними об'єктами кібератак є великі компанії та державні інституції – зокрема урядові органи, об'єкти критичної інфраструктури, оборонні підприємства та стратегічно важливі сектори економіки. Метою таких атак є не лише викрадення даних, а й дестабілізація критичних елементів інфраструктури [1].

У статті [2] автори розглядають типові загрози інформаційній безпеці та їх походження, включаючи зовнішні та внутрішні загрози, а також наголошують на недостатній розвиненості законодавчої бази щодо захисту інформації та протидії новим загрозам.

А.П. Максименко розглядає загрози цифрової економіки під час війни. Так, автор дає визначення цифровій глобалізації як «…поширенню економічних, технологічних, культурних та політичних практик та інструментів мережею Інтернет..» [3]. На прикладі збройних конфліктів у Іраку, Грузії, та в Україні узагальнено переваги та недоліки цифрової інфраструктури в умовах війни. Автор узагальнює загрози, пов'язані із цифровою трансформацією України в умовах військових дій та повоєнного відновлення: нестача інвестицій, непрозоре фінансування та рейдерські захвати, бюрократія і недостатній або надмірний нормативний супровід.

Л. Шостак, А. Федонюк [4] виділяють такі види загроз для вітчизняного бізнесу під час війни: дестабілізація інформаційної системи, шляхом нападів на критичну інфраструктуру; атак на сайти і сервери для отримання фінансової вигоди або політичних цілей або маніпуляції з даними; техніко-технологічна залежність від іноземних виробників ІТ-продукції; вразливість ІТ-інфраструктури компаній, яка проявляється у розосередженні працівників через віддалену роботу; відсутність належного контролю за кіберзахистом з боку державних інституцій.

О.І. Кузьменко та ін. розглядають виклики України у сфері кібербезпеки. Випадки порушення кібербезпеки становлять загрозу для безперервної діяльності будь-якого підприємства [5].

М.Г. Хаустова серед ризиків подальшого впровадження цифровізації в усіх сферах суспільства виділяє такі елементи: несанкціонований доступ, безробіття, цифрова нерівність, стирання етичних меж через непомірне використання штучного інтелекту [6].

З кіберзагрозами стикаються організації по всьому світу. В. Столлінгс і Л. Браун акцентують увагу на таких факторах посилення кіберзагроз [7]: цифровізація усіх сфер життя, вдосконалення кібератак через розвиток нових технологій, правова та етична відповідальність, коли компанії зобов'язані захищати персональні дані відповідно до норм законодавства.

За даними статистичної служби ЄС [8], у 2023 році кожне п'яте підприємство ЄС (21,54%) зазнало інцидентів безпеки, пов'язаних з ІКТ. наслідком інцидентів безпеки ІКТ була недоступність послуг ІКТ через збої апаратного або програмного забезпечення (17,97% підприємств).

За даними Європейського агентства з кібербезпеки ENISA [9], DDos-атаки та програми-вимагачі залишаються однією з найбільш впливових загроз для держав-членів ЄС. У трійку галузей, що найчастіше були об'єктом кібератак від липня 2023 до червня 2024 року входили публічне адміністрування, транспорт та фінансовий сектор – разом майже 40% інцидентів кібербезпеки припадали на ці сектори [9]. Це підвищує актуальність дослідження інформаційної безпеки як окремих організацій, так і секторів економіки.

У роботі [10] автори розглядають кількісні та якісні методи оцінки ризиків та пропонують методичний інструментарій такої оцінки в залежності від типу активів, що підлягають загрозам: персонал, фінанси, обладнання, дані, інфраструктура. Також наводяться поняття ризику, вразливості та загрози. Так, «…вразливість (vulnerability)– це все, що можна використати для отримання або заборони доступу до активу або іншим чином поставити актив під загрозу. Вразливості, як правило, є відсутністю захисту або використанням чогось, що можна використовувати для отримання доступу до активу…» [10]. Загроза – це будь-хто або будь-що, що може використати вразливість для отримання, зміни або заборони доступу до активу. Для кожної вразливості можуть бути декілька загроз. Ризик автори визначають як міру впливу чогось небажаного, а також як ймовірність його виникнення. Автори акцентують увагу, що ризик залежить выд цінності активу, його вразливостей та потенційних загроз.

Г.Г. Найман та Д.М. Гаркавенко [11] концентрують увагу на процесі управління вразливостями, як процесі зниження шкоди від реалізації загроз, з якими стикаються фахівці інформаційної безпеки і шляхи їх вирішення. Автори пропонують рішення із використання систем машиного навчання для вирішення подібних завдань.

У сучасних умовах разом із ризиками постає проблема вразливості суб'єктів економічної діяльності та їх активів перед загрозами, включаючи загрози військових дій та пошкоджень, дії конкурентів, кіберзагрози. Сам термін «вразливість» частіше зустрічається при розгляді питань кібербезпеки для інформаційних систем. Проте в економічній літературі зустрічається ширше використання цього терміну.

Так, Програма Розвитку ООН (UNDP) у звіті про людський розвиток (Human Development Report) [12] визначає вразливість як схильність до негативних потрясінь та невдач, які можуть перешкоджати прогресу в людському розвитку. У звіті розглядається економічна вразливість, як пов'язана як із зовнішніми факторами, такими як нестабільність торгівлі або стихійні лиха, так і зі структурними вразливостями, які виникають через нерівність та соціальні структури, що непропорційно впливають на певні групи.

У статті [13] економічна вразливість визначається як схильність економіки до екзогенних потрясінь, що виникають внаслідок економічної відкритості, тоді як економічна стійкість визначається як здатність економіки, спричинена політикою, протистояти наслідкам таких потрясінь або відновлюватися від них. На думку авторів [14], економічна вразливість стосується ризиків, спричинених зовнішніми/екзогенними потрясіннями для системи виробництва, розподілу та споживання.

На основі аналізу існуючих підходів до визначення термінів «економічна вразливість» в даному досліджені пропонується авторський підхід до визначення економічної кібервразливості організації.

Економічна кібервразливість організації – це ступінь, до якого економічний стан суб'єкта господарювання схильний до збоїв або втрат, що виникають внаслідок внутрішніх структурних слабкостей або зовнішніх потрясінь, зокрема тих, що виникають внаслідок кіберзагроз

На основі аналізу джерел [3–7, 10–14] виділені основні класи цифрових вразливостей та інструменти, які використовуються для їх мінімізації:

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

– *вразливості мережі:* вони виникають через слабкі місця в мережевій інфраструктурі, протоколах та конфігураціях. Системи виявлення вторгнень (IDS), віртуальні приватні мережі (VPN) та сегментація мережі є важливими інструментами для захисту мереж.

– *вразливості персоналу:* ці вразливості 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* включають недоліки в апаратних компонентах, такі як 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 неадекватну систему управління, 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. 1).

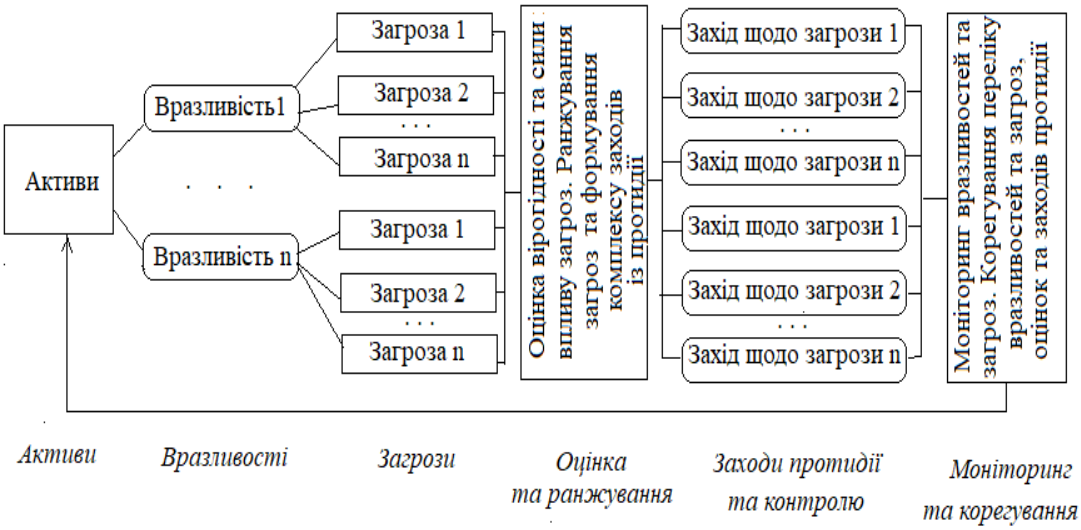

Рисунок 1 – Концептуальна модель усунення цифрових вразливостей організації

Джерело: сформовано авторами за даними джерел [8–10, 13]

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 рівнем ризику, масштабом та складністю усунення;
- нейтралізація шляхом оновлень, виправлень, видалення вразливих компонентів;
- 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 таблиці 1.

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.

Одним із ключових активів, що підлягають захисту від кіберзагроз, є фізична та мережева інфраструктура. Під фізичною інфраструктурою підприємства маються на увазі матеріальні компоненти інформаційних і технічних систем, що забезпечують функціонування цифрових активів. До них належать сервери, комп'ютери, комунікаційне обладнання, засоби електроживлення, системи охолодження, відеоспостереження, а також приміщення, де розміщено обладнання. Вона формує фізичне середовище для обробки, зберігання та передачі даних. Загрози, що стосуються фізичної інфраструктури, охоплюють: несанкціонований фізичний доступ до обладнання, крадіжку або пошкодження пристроїв, природні катастрофи, відключення від джерел електроживлення. Інструментами кіберзахисту для фізичної інфраструктури є Системи контролю доступу (картки, біометрія), системи відеоспостереження із аналітикою, датчики диму, температури, затоплення, прилади резервного живлення.

Мережева інфраструктура підприємства – це система технічних засобів і програмного забезпечення, яка забезпечує передачу, маршрутизацію, обробку та захист даних у межах корпоративної мережі.

Вона включає мережеві пристрої (комутатори, маршрутизатори, шлюзи), комунікаційні канали, сервери, протоколи обміну даними та засоби кіберзахисту. Загрозами мереженій інфраструктурі є DoS/DDoS-атаки, фішинг, дія шкідливого програмного забезпечення, включаючи програми-вимагачі, несанкціонований віддалений доступ, витік даних. Інструментами кіберзахисту для мереженої інфраструктури є міжмережеві екрани, системи виявлення та запобігання вторгненням, VPN

для захищеного доступу, сегментація мережі та політики доступу, антивірусні та антишпигунські засоби, засоби шифрування даних та моніторинг трафіку. Проте треба зазначити, що кіберзахист як фізичної, так і мереженої інфраструктури вимагає комплексного підходу, що включає технічні інструмент и разом із організаційними та процедурними заходами.

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, пошкодженя 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: сформовано авторами на основі джерел [10; 13]

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 (Таблиця 2). 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	Приклади
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 [10; 13]

Додатково систематизовано цифрові вразливості, потенційні загрози та методи протидії для виробничого підприємства, де кожній вразливості відповідають конкретні загрози та методи протидії (Таблиця 3).

Таблиця 3 – Приклади цифрових вразливостей, потенційних загроз та методів протидії для виробничого підприємства

Цифрова вразливість	Потенційна загроза	Методи протидії
Відкритий віддалений доступ (Remote Access)	Несанкціонований контроль обладнання, впровадження шкідливого ПЗ	VPN з двофакторною автентифікацією, контроль доступу, логування сесій
Відсутність оновлень ПЗ на SCADA/PLC	Експлуатація відомих вразливостей, зупинка виробничих процесів	Регулярні оновлення ПЗ, застосування патч-менеджменту, мережеве розділення
Слабка сегментація внутрішньої мережі	Поширення шкідливого ПЗ на критичні виробничі системи	Мережеве розмежування (зони OT/IT), VLAN, ізоляція систем управління
Недостатній моніторинг IoT-сенсорів	Маніпуляції з даними датчиків, саботаж обладнання	Постійний моніторинг трафіку, контроль аномалій, обмеження підключень
Використання стандартних або слабких паролів	Взлом облікових записів, повний контроль над системами	Впровадження політик складності паролів, багатофакторна автентифікація
Людський фактор (недостатнє навчання персоналу)	Фішинг, помилкове підключення до шкідливих пристроїв	Навчання з кібергігієни, інструкції реагування на інциденти

Джерело: сформовано авторами на основі джерел [10; 13]

Ці заходи мають на меті забезпечити надійний захист виробничих процесів, які дедалі більше залежать від цифрової інфраструктури та є вразливими до кібератак.

Висновки. У цьому дослідженні розглядаються питання цифрової вразливості активів суб'єктів господарювання як складової ширшого поняття економічної кібервразливості. Цифрова вразливість означає схильність осіб, організацій або систем до шкоди чи експлуатації у цифровому середовищі. Вона проявляється через кіберзагрози, витоки даних, онлайн-шахрайство, алгоритмічну упередженість або цифрові маніпуляції, і вказує на потребу в усвідомленні ризиків та проактивному захисті.

У межах дослідження запропоновано концептуальну модель усунення цифрових вразливостей. Вона поєднує організаційні активи, відповідні вразливості та цифрові загрози, з прикладами систематизації для банку, виробничого підприємства та інтернет-магазину. Модель може бути доповнена цільовими показниками для синхронізації із стратегічними орієнтирами компанії та системою KPI для оцінки ефективності реагування на цифрові ризики.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Кузьменко О. І., Маклюк О. В., Чернишова О. О. Кібербезпека бізнесу під час війни. *Економіка та суспільство*. 2022. № 44. DOI: https://doi.org/10.32782/2524-0072/2022-44-21

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

3. 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.

4. Олефір В. К. Вплив інформаційно-комунікаційних технологій на споживчі ринки. *Європейський науковий журнал Економічних та Фінансових інновацій*. 2024. № 1 (13). С. 256–264.

5. Смотрич Д. В., Браілко Л. Інформаційна безпека в умовах воєнного стану *Науковий вісник Ужгородського Національного Університету, Серія ПРАВО*. 2023. Випуск 77, частина 2. С. 121–127.

6. Хаустова М. Г. Вигоди, ризики та проблеми цифровізації суспільства: загальнотеоретичний аспект. *Електронне наукове видання «Аналітично-порівняльне правознавство»*. 2023. № 11. DOI: https://doi.org/10.24144/2788-6018.2023.05.135

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

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

9. Dincer H., Hacioglu U. Investigating the Economic Vulnerability Factors of Emerging Markets After the Global Financial Crisis of 2008 With a Hybrid Multi-Criteria Decision-Making Approach. in *Handbook of Research on Economic, Financial and Industrial Impacts of Infrastructure Development*. 2017. 21 p.

10.Global Information Assurance Certification (GIAC) An Introduction to Information Risk Assessment GSEC Practical. Version 1.4b. August, 8. 2003. URL: https://www.giac.org/paper/gsec/3156/introduction-information-risk-assessment/105258 (дата звернення: 20.06.2025)

11. European Union Agency for Cybersecurity (ENISA) 2024 Report on the state of cybersecurity in the union. November 2024. DOI: https://doi.org/10.2824/0401593. URL: https://www.enisa.europa.eu/publications (дата звернення: 21.06.2025)

12. Eurostat, Statistics explained. IT Security in enterprises. December 2024. URL: https://ec.europa.eu/eurostat/statistics-explained/SEPDF/cache/9132.pdf (дата звернення: 21.06.2025)

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

14. United Nations Development Programme (UNDP) Human Development Report 2014. Sustaining Human Progress: Reducing Vulnerabilities and Building Resilience. URL: https://www.undp.org/sites/g/files/zskgke326/files/migration/tr/2014-Human-Development-Report---English.pdf (дата звернення: 21.06.2025)

REFERENCES

1. Kuzmenko O. I., Makliuk O. V., Chernyshova O. O. (2022). Kiberbezpeka biznesu pid chas viiny [Cybersecurity of business during war]. *Ekonomika ta suspilstvo – Economy and society*. Vol. 44. DOI: https://doi.org/10.32782/2524-0072/2022-44-21 (in Ukrainian)

2. Maksymenko A. P. (2023) Realni ta potentsiini zahrozy tsyfrovoi ekonomiky v umovakh viiny [Real and potential threats to the digital economy in wartime]. *Ekonomichnyi prostir – Economic Space*. Vol. 188, pp. 41–49. (in Ukrainian)

3. Naiman H. H., Harkavenko D. M. (2021) Metody ta zasoby upravlinnia vrazlyvostiamy korporatyvnoi informatsiinoi systemy na osnovi mashynnoho navchannia [Methods and tools for managing vulnerabilities in corporate information systems based on machine learning]. *Suchasnyi zakhyst informatsii – Modern information protection*. Vol. 3(47), pp. 24–28. (in Ukrainian)

4. Olefir V. K. (2024) Vplyv informatsiino-komunikatsiinykh tekhnolohii na spozhyvchi rynky [The impact of information and communication technologies on consumer markets]. *Yevropeiskyi naukovyi zhurnal Ekonomichnykh ta Finansovykh innovatsii – European Scientific Journal of Economic and Financial Innovations*. Vol. 1 (13), pp. 256–264. (in Ukrainian)

5. Smotrych D. V., Brailko L. (2023) Informatsiina bezpeka v umovakh voiennoho stanu [Information security in martial law]. *Naukovyi visnyk Uzhhorodskoho Natsionalnoho Universytetu, Seriia Pravo – Scientific Bulletin of Uzhhorod National University, Law Series.* Vol. 77 (2), pp. 121–127. (in Ukrainian)

6. Khaustova M. H. (2023) Vyhody, ryzyky ta problemy tsyfrovizatsii suspilstva: zahalnoteoretychnyi aspekt [Benefits, risks and problems of digitalization of society: general theoretical aspect]. *Elektronne naukove vydannia "Analitychno-porivnialne pravoznavstvo" – Electronic scientific publication "Analytical and comparative law".* Vol. 11. DOI: https://doi.org/10.24144/2788-6018.2023.05.135 (in Ukrainian)

7. Shostak L., Fedoniuk A., Pomazun O. (2024) Osoblyvosti kiberbezpeky biznesu v umovakh voiennoho chasu [Peculiarities of business cybersecurity in wartime]. *Tsyfrova ekonomika ta ekonomichna bezpeka – Digital economy and economic security*. Vol. 3 (12), pp. 121–125. DOI: https://doi.org/10.32782/dees.12-22 (in Ukrainian)

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

9. Dincer H., Hacioglu U. (2017) Investigating the Economic Vulnerability Factors of Emerging Markets After the Global Financial Crisis of 2008 With a Hybrid Multi-Criteria Decision-Making Approach. *Handbook of Research on Economic, Financial and Industrial Impacts of Infrastructure Development*: monograph. 21 p. DOI: https://doi.org/10.4018/978-1-5225-2361-1.ch016

10. Global Information Assurance Certification (GIAC) An Introduction to Information Risk Assessment GSEC Practical. Version 1.4b. August, 8. 2003. Available at: https://www.giac.org/paper/gsec/3156/introduction-information-risk-assessment/105258 (accessed June 20, 2025)

11. European Union Agency for Cybersecurity (ENISA) 2024 Report on the state of cybersecurity in the union. November 2024. DOI: https://doi.org/10.2824/0401593. Available at: https://www.enisa.europa.eu/publications

12. Eurostat, Statistics explained. IT Security in enterprises. Data from December 2024. Available at: https://ec.europa.eu/eurostat/statistics-explained/SEPDF/cache/9132.pdf (accessed June 21, 2025)

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

14. 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)

Iryna Sheiko, Ruslan Stepanenko
Kharkiv National University of Radio Electronics

DIGITAL VULNERABILITIES MANAGEMENT OF MODERN ENTERPRISE

Abstract. *The article presents a comprehensive analysis of digital risks and vulnerabilities inherent to domestic organizations. The purpose of the article is to study theoretical approaches to managing digital vulnerabilities of an enterprise and to construct a conceptual model for their elimination in order to reduce the impact of digital threats. The study explores digital threats faced by Ukrainian businesses during wartime, as well as cybersecurity incidents within the European Union. Special emphasis is placed on the economic vulnerability of organizations. The author introduces a definition of "economic cyber*

vulnerability of an organization," described as the degree to which an organization's economic condition is susceptible to disruptions or losses stemming from internal structural weaknesses or external shocks, particularly those linked to cyber threats. The main classes of digital vulnerabilities are systematized, including vulnerabilities related to hardware, software, networks, personnel, and management systems. A conceptual model for addressing digital vulnerabilities is proposed, defined as a process of identifying, assessing, and mitigating weaknesses within an organization's digital infrastructure. This model can be expanded by incorporating performance indicators and a KPI system to evaluate the effectiveness of digital threat response. The article identifies various types of organizational assets prone to digital vulnerabilities and outlines the corresponding threats associated with each type. Particular attention is devoted to digital vulnerabilities and risks affecting physical and network infrastructure. Examples of structured systematization are provided for financial institutions, manufacturing enterprises, and online retail businesses. This approach facilitates the identification of critical digital risks specific to each sector and supports the customization of information security systems accordingly. For manufacturing enterprises, digital vulnerabilities, potential threats, and corresponding mitigation strategies are organized in a way that links each vulnerability to a specific threat and response tool. The proposed measures aim to ensure resilient protection of production processes, which are increasingly reliant on digital infrastructure and remain exposed to cyberattacks.

Keywords: *cybersecurity, digital vulnerability, economic vulnerability, management of digital risks, organizational asset, vulnerability mitigation.*