УДК: 004.056.53 DOI: **10.33099/2311-7249/2026-55-1-35-43**

ІСМАГІЛОВ Артур Ільясович,
Інститут програмних систем Національної академії наук України, Київ, Україна,
https://orcid.org/0009-0002-1332-8147

СІНІЦИН Ігор Петрович,
доктор технічних наук, професор,
Інститут програмних систем Національної академії наук України, Київ, Україна,
https://orcid.org/0000-0002-4120-0784

НАУКОВО-МЕТОДИЧНИЙ ПІДХІД ДО ОПТИМІЗАЦІЇ ВИТРАТ НА КІБЕРБЕЗПЕКУ ПІДПРИЄМСТВА В УМОВАХ ОБМЕЖЕНОСТІ РЕСУРСІВ

У статті наведено результати дослідження, спрямованого на створення науково-методичного підходу до економічно обґрунтованого формування витрат на кібербезпеку підприємства в умовах обмеженості ресурсів та зростання кількості багатопрофільних загроз нульового дня. Особливу увагу надано поєднанню багаторівневого технологічного захисту (Defense-in-Depth) з кількісною оцінкою виробничих та фінансових втрат від кібератак, що дає змогу оптимізувати структуру інвестицій у кіберзахист.

Мета статті. *Розробленння науково-методичного підходу до оптимізації витрат на кібербезпеку підприємства в умовах зростання загроз нульового дня, що дає змогу визначити оптимальну структуру інвестицій у кібербезпеку, забезпечити раціональний розподіл бюджету та мінімізувати потенційні збитки від кіберінцидентів*

Методи дослідження. *У дослідженні застосовано методи економіко-математичного моделювання, порівняльного аналізу інструментів кіберзахисту, елементи ризик-орієнтованого підходу, а також кількісну оцінку прямих і непрямих втрат від простою виробництва. Для ілюстрації запропонованого підходу використано умовний приклад невеликого виробництва електронних комплектуючих подвійного призначення із розрахунком втрат від простою та показника окупності витрат на кібербезпеку (ROICC).*

Отримані результати дослідження. *Побудовано узагальнену таблицю інструментів кіберзахисту від загроз нульового дня із визначенням їх ефективності, недоліків, платформ реалізації та орієнтовної вартості за фіксованої кількості серверних хостів. Сформовано структуру річних витрат на кібербезпеку підприємства з урахуванням технологічних рішень і витрат на кваліфікований персонал. Запропоновано підхід до розрахунку загальних втрат від простою виробництва внаслідок успішної кібератаки, який охоплює прямі та непрямі складові (downtime losses, ремонт обладнання, штрафи, втрачені замовлення). Доведено, що вже за кілька діб простою сукупні збитки можуть перевищувати річні видатки на кібербезпеку, що обґрунтовує економічну доцільність превентивних інвестицій. На основі цього сформульовано показник окупності витрат на кібербезпеку (ROICC) як інструмент прийняття управлінських рішень щодо масштабу та структури захисних заходів.*

Теоретичне та практичне значення викладеного у статті *полягає в подальшому розвитку підходів до економічної оцінки кіберризиків шляхом інтеграції моделей оцінки загроз нульового дня, ризик-орієнтованої логіки та аналізу витрат у єдиний науково-методичний підхід до оптимізації кіберзахисту підприємства. Практичне значення полягає в можливості використання запропонованого підходу керівниками підприємств (особливо виробничих та критично важливих технологічних об'єктів) для обґрунтування бюджетів на кібербезпеку, ранжування та комплектації інструментів захисту, а також для оцінки ефекту від реалізації заходів у вигляді скорочення ймовірних втрат від кібератак.*

Ключові слова: *кібербезпека, загрози нульового дня, коефіцієнт окупності витрат на кібербезпеку, витратити на кібербезпеку.*

Вступ

В умовах ведення гібридних війн кіберпростір стає повноцінним театром бойових дій, у межах якого реалізуються як масові автоматизовані атаки, так і високотаргетовані загрози нульового дня, здатні паралізувати критичні виробничі та логістичні процеси. Для виробничих і технологічних підприємств подвійного призначення наслідки таких атак виходять далеко за межі звичайних інформаційних втрат, породжуючи суттєві економічні збитки, пов'язані з простоєм виробництва, пошкодженням обладнання, розривом контрактів і погіршенням репутації.

За таких умов традиційні підходи, що фокусуються переважно на технічних параметрах кіберзахисту, виявляються недостатніми. Вони переважно не відповідають на ключове для менеджменту питання: який рівень і структура витрат на кібербезпеку є економічно виправданими з урахуванням ймовірності реалізації загроз і потенційних виробничих втрат.

Нестача комплексних моделей, що пов'язують кіберризики із витратами та результатами діяльності підприємства, ускладнює прийняття обґрунтованих управлінських рішень, особливо в умовах обмеженості ресурсів. Саме тому розроблення науково-методичного підходу, який дає змогу порівнювати вартість багаторівневих систем захисту з очікуваними збитками від кібератак і визначати оптимальний рівень інвестицій у безпеку, набуває особливої актуальності.

Постановка проблеми. В поточних умовах стрімкого зростання кіберзагроз та ескалації атак нульового дня, забезпечення стійкості інформаційної інфраструктури підприємств набуває важливого значення. Особливо важливим окреслене питання є для виробничих, а також технологічних підприємств подвійного призначення, порушення роботи IT-систем яких безпосередньо впливає на безперервність виробничого процесу, якість продукції та економічну стабільність. Так, сучасні підприємства змушені враховувати багатопрофільні загрози, які вимагають застосування інтегрованих багаторівневих систем захисту, але обмеженість ресурсів і висока собівартість технологічних рішень зумовлюють потребу пошуку нових оптимальних рішень в даному контексті. Відсутність комплексного підходу, який би враховував співвідношення між ризиками, потенційними втратами та фактичними витратами на захист, створює прогалину в управлінні кіберризиками. Отже, розроблення та удосконалення науково-методичного підходу є надзвичайно актуальним завданням як для економічної науки, так і для практики управління сучасними підприємствами.

Аналіз останніх досліджень і публікацій. Аналіз наукової літератури, присвяченої окресленій проблематиці показав, що насьогодні існує значна кількість робіт в межах даного напряму дослідження. Так, у статті [1] запропоновано підхід до класифікації та оцінки витрат на забезпечення кібербезпеки підприємства, побудовано модель інтегрального показника ефекту від обмеження поширення інформації з урахуванням шкоди, вигоди, імовірностей і витрат на захист.

В дослідженні [2] проаналізовано економічні наслідки кіберзлочинності для компаній, запропоновано підходи до оцінки ефективності витрат на інформаційну безпеку, розглянуто показники, що дозволяють співвіднести обсяг інвестицій у захист із зменшенням ризиків і потенційних збитків.

Водночас, в статті [3] введено поняття «кібербезпека облікової інформації», що розмежовує інформаційну й кібербезпеку, описано групи загроз і комплекс організаційно-технічних заходів щодо захисту бухгалтерських даних.

Авторами [4] розроблено нечітку модель оцінки ризиків порушення конфіденційності проектної документації, що враховує неповноту та розмитість інформації. В статті продемонстровано, як через формалізацію структури документів і правил нечіткої логіки можна отримати кількісну оцінку інформаційного ризику, яку далі можна зв'язати з витратами на заходи захисту.

Схожим виступає дослідження [5], в якому описано нечітку модель оцінки ризиків для ERP-систем, яка дозволяє враховувати різні види загроз і рівні захищеності. Отриманий авторами показник ризику запропоновано використовувати як основу для розрахунку доцільного рівня витрат на кібербезпеку корпоративних систем.

Заслуговує на увагу стаття [6], автори якої обґрунтували багаторівневу модель виявлення загроз нульового дня в умовах воєнного стану та дефіциту фінансів, обчислювальних потужностей і персоналу. Показано, як легковагові методи поведінкового аналізу й самонавчання дозволяють балансувати між рівнем захисту й ресурсними обмеженнями, що важливо для обґрунтування економічно доцільних рішень протидії загрозам нульового дня.

Водночас, стаття [7] містить результати аналізу специфіки кіберзагроз для бізнесу під час війни в Україні, включно з фішингом, програмами-вимагачами, атаками нульового дня тощо, та їхні економічні наслідки. Автори підкреслюють необхідність зростання інвестицій у кіберзахист, адаптації стратегій безпеки і побудови систем управління ризиками.

В роботі [8] узагальнено класифікацію шкідливого програмного забезпечення, описано основні сценарії атак та економічні наслідки кібератак для компаній. Вченими запропоновано підходи до підвищення ефективності технічних і організаційних заходів протидії, що можна використати при обґрунтуванні структури витрат на захист від шкідливого програмного забезпечення і пов'язаних вразливостей нульового дня.

Стаття [9] присвячена системам захисту великих даних в електронному бізнесі, архітектурним рішенням та ключовим механізмам безпеки. При цьому автор робить наголос на тому, як складність і обсяг даних впливають на вимоги до захисту й обсяг витрат, що допомагає обґрунтувати підвищені інвестиції у безпеку даних на сучасних підприємствах.

У свою чергу, на основі SWOT-аналізу автор статті [10] моделює інформаційні ризики малого бізнесу, виділяючи загрози, вразливості та їхній вплив на діяльність підприємства. Завдяки чому, в статті запропоновано підхід до кількісного оцінювання ризиків, який можна інтегрувати в порядок вибору пріоритетних заходів та оптимізації витрат на кіберзахист.

Аналіз сучасних українських наукових публікацій підтверджує, що проблема підвищення кіберстійкості підприємств наразі залишається багатогранною та недостатньо опрацьованою в частині комплексного оцінювання. Значна частина українських досліджень присвячена розробленню моделей оцінки ризиків із застосуванням нечіткої логіки, проте вони здебільшого зосереджуються на класифікації загроз або вимірюванні рівня захищеності окремих систем та не пропонують інтегрованого підходу до оцінювання витрат на заходи протидії кіберзагрозам. Моделі, орієнтовані на прогнозування поведінки загроз нульового дня, значною мірою спрямовані на

оптимізацію виявлення, але не охоплюють економічних аспектів прийняття управлінських рішень у ресурсно-обмеженому середовищі. Дослідження, які висвітлюють кіберзагрози в умовах воєнного часу, підкреслюють високий рівень ризиків для підприємств, проте не пропонують інструментарію для визначення економічної доцільності інвестицій у кіберзахист.

Відповідно, незважаючи на наявність значної кількості робіт, спрямованих на аналіз ризиків, технічних та криптографічних засобів захисту чи окремих елементів безпекової інфраструктури, залишається нерозв'язаною комплексна наукова проблема визначення економічно обґрунтованого рівня витрат на багаторівневий кіберзахист, особливо в контексті багатопрофільних загроз нульового дня та обмежених ресурсів підприємства. Водночас недостатньо дослідженим є питання співвідношення між потенційними збитками від простою виробництва, ймовірністю реалізації загроз та фактичними інвестиціями у превентивні заходи.

Окреслене й зумовило **мету статті**, яка полягає в розробленні науково-методичного підходу до оптимізації витрат на кібербезпеку підприємства в умовах зростання загроз нульового дня, що дає змогу визначити оптимальну структуру інвестицій у кібербезпеку, забезпечити раціональний розподіл бюджету та мінімізувати потенційні збитки від кіберінцидентів.

Виклад основного матеріалу дослідження

Враховуючи напрацювання українських вчених і виявлені недоліки існуючих підходів, виникає потреба у розробленні науково-методичного підходу, який поєднає економічне моделювання, аналіз кіберризиків та оцінювання ефективності заходів протидії кіберзагрозам, у тому числі загрозам нульового дня в єдину систему прийняття управлінських рішень.

Передумовами створення науково-методичного підходу є зростання кількості високотаргетованих загроз нульового дня, орієнтованих на виробничі та технологічні підприємства подвійного призначення, а також відсутність у наявних підходах інтегрованого інструментарію, який поєднує оцінювання технічної ефективності засобів кіберзахисту з економічною оцінкою наслідків кібератак та бюджетними обмеженнями підприємства. Додатковою передумовою є необхідність прийняття управлінських рішень в умовах дефіциту фінансових, кадрових і обчислювальних ресурсів.

Об'єктом дослідження науково-методичного підходу є процес формування та оптимізації структури витрат підприємства на забезпечення кібербезпеки з урахуванням загроз нульового дня та потенційних економічних втрат від порушення безперервності виробничих процесів.

Коротка сутність науково-методичного підходу полягає у поєднанні багаторівневої архітектури кіберзахисту типу Defense-in-Depth з кількісною оцінкою прямих і непрямих втрат від простою виробництва та зіставленні цих втрат із витратами на впровадження і підтримку системи кібербезпеки шляхом розрахунку показника окупності витрат на кібербезпеку (Return on Investment in cybersecurity, далі (далі – ROICC)).

Призначення науково-методичного підходу полягає у забезпеченні науково обґрунтованого вибору складу та структури інструментів кіберзахисту підприємства, визначенні доцільного обсягу інвестицій у кібербезпеку та підтримці управлінських рішень щодо розподілу бюджету в умовах зростання кіберризиків.

Відмінність запропонованого підходу від відомих підходів полягає в тому, що він не обмежується лише оцінюванням рівня захищеності або інтегральних показників ризику, а безпосередньо пов'язує характеристики кіберзагроз нульового дня, конфігурацію багаторівневої системи захисту та економічні наслідки простою виробництва. Удосконалення підходу досягається завдяки введенню показника ROICC як інструмента кількісного порівняння альтернативних конфігурацій системи кіберзахисту з позиції економічної доцільності.

Науково-методичний підхід ґрунтується на низці обмежень і припущень, зокрема:

вважається, що базова конфігурація інфраструктури підприємства є стабільною протягом аналізованого періоду;

вартість простою виробництва розраховується на основі середніх показників випуску та прибутку;

частка втрат, не пов'язаних безпосередньо з простоєм (репутаційні втрати, зниження ринкової вартості бренду), не враховується або враховується опосередковано;

ймовірність реалізації загроз нульового дня не моделюється окремо, а оцінюється через сценарій настання інциденту.

Ввідними даними для реалізації науково-методичного підходу є: перелік інструментів кіберзахисту, що плануються до впровадження; їх вартість і вимоги до персоналу; кількість серверних хостів та особливості IT-інфраструктури підприємства; середньодобовий обсяг виробництва та прибуток з одиниці продукції; прогнозована тривалість простою; витрати на відновлення обладнання; втрати від невиконаних контрактів і штрафні санкції.

Математичний апарат науково-методичного підходу базується на використанні економіко-математичних методів оцінювання втрат і порівняльного аналізу витрат.

Алгоритм реалізації науково-методичного підходу передбачає послідовне виконання таких етапів:

формування переліку релевантних інструментів захисту від загроз нульового дня;

побудову конфігурації багаторівневої системи кіберзахисту;

розрахунок загальних витрат на впровадження та експлуатацію системи; визначення показників виробничих втрат у разі простою;

обчислення загальних економічних втрат від кібератаки; розрахунок значення ROICC;

порівняння альтернативних конфігурацій системи кіберзахисту та вибір оптимального варіанта за критерієм максимізації економічного ефекту.

Теоретичною областю застосування науково-методичного підходу є дослідження процесів формування кіберстійкості підприємств, моделювання взаємозв'язку між кіберризиками та економічними результатами діяльності, а також розвиток підходів до інтеграції ризик-орієнтованого управління в економічні моделі підприємства.

Практична область застосування результатів науково-методичного підходу охоплює діяльність керівників і служб кібербезпеки виробничих та технологічних підприємств подвійного призначення при формуванні бюджетів на кібербезпеку, ранжуванні інструментів захисту, плануванні чисельності та компетенцій персоналу, а також обґрунтуванні інвестицій у модернізацію безпекової інфраструктури.

Приклад використання науково-методичного підходу наведено для невеликого підприємства з виробництва електронних комплектуючих подвійного призначення, для якого сформовано багаторівневу конфігурацію засобів кіберзахисту та визначено сукупні річні витрати на рівні 202 500 у.о. Розрахунок втрат від простою тривалістю 24 години показав величину загальних збитків 47 832 у.о., а при простої 6 днів – 211 992 у.о., що перевищує річні витрати на кібербезпеку. Обчислення показника ROICC для сценарію простою понад п'ять діб дало додатне значення (ROICC ≈ 0,04), що підтверджує економічну доцільність інвестицій у запропоновану систему кіберзахисту.

Результат від використання науково-методичного підходу полягає у зменшенні очікуваних економічних втрат підприємства щонайменше на 20–25 % порівняно з варіантом фрагментарного або недостатнього фінансування кіберзахисту, що підтверджується зіставленням сукупних втрат від простою з річними витратами на забезпечення кібербезпеки та результатами розрахунку показника ROICC.

Аналіз наукових джерел свідчить, що передумовою формування оптимальної системи кіберзахисту є оцінка можливих технічних рішень та їх ефективності. Перш за все, проаналізуємо інструменти кіберзахисту підприємства від загроз нульового дня, результати такого аналізу представлені в табл. 1.

Таблиця 1

Результати аналізу інструментів кіберзахисту підприємств від загроз нульового дня *

№	Інструменти	Ефективність	Недоліки	Платформа	Вартість із розрахунку 30 серверних хостів
1	2	3	4	5	6
1.	Пісочниця (ізольоване середовище)	Для виявлення загроз нульового дня показує ефективність у такій взаємодії: «фуззер» → автоматичне сортування → детонаційна пісочниця з інструменталізацією → інтерактивна пісочниця для «важких» кейсів → аналітична дошка для виведення результату.	Деякі види вразливостей можуть не виявитися в автоматичній пісочниці — потрібні доповнення: ручний аналіз, аудит коду та просунутий фузинг.	OSS-Fuzz/ClusterFuzz	Безкоштовно (лише для проектів з відкритим похідним кодом)
2.	Виявлення на рівні програми	Для виявлення загроз нульового дня показує ефективність у такій взаємодії: RASP → WAAP → ADR → API Threat Protection, особливо якщо вони інтегровані з CI/CD та системою моніторингу.	Використання готових пропрієтарних програмних рішень може унеможливити застосування RASP/ADR-агентів та відповідно CI/CD.	Cloudflare, Imperva	6 000 у.е
3.	Пастки (decoy-системи)	Для виявлення спроб експлуатації вразливостей без знання про такі вразливості.	Фіксує вже вчинену дію, проти масових автоматизованих атак може спрацювати вже після зараження.	Labyrinth Deception Platform	13 000 у.е

Закінчення табл. 1

1	2	3	4	5	6
4.	Поведінковий аналіз та машинне навчання	Для здійснення збору фалів-протоколів роботи, телеметрії, кореляції, оброби моделі поведінки.	Для досягнення значного ефекту необхідне використання декількох рішень до прикладу CrowdStrike + Splunk/Exabeam + Mayhem.	CrowdStrike Falcon “Pro”, Splunk, Mayhem	3 500 у.е
5.	Управління вразливістю та швидке оновлення (patch management).	Для автоматизації процесів пошуку вразливостей та автоматизації процесу пошуку та встановлення виправлень.	Для досягнення значного ефекту необхідне поєднання регулярного пошуку вразливостей та саме їх усунення.	Qualys / OpenVAS. Windows: WSUS Linux: Ansible	3 000 у.е
6.	Мінімальні привілеї, сегментація	Для здійснення керуванням ідентифікацією та доступом та керуванням привілейованим доступом.	Для досягнення значного ефекту доцільно використовувати IAM та PAM.	Okta / OpenLDAP CyberArk	4 500 у.е
7.	Системи виявлення та запобігання вторгнення (IDS/IPS).	З метою запобігання мережевим атакам.	Сучасні системи IDS/IPS мають ефект при поєднані їх використання із SIEM, а також при інтеграції із EDR.	Cisco Stealthwatch, Zeek, Suricata	1 500 у.е

* Джерело: розроблено авторами.

Дані, наведені в табл. 1 демонструють, що жоден інструмент окремо не забезпечує повноцінного захисту від загроз нульового дня, оскільки ці загрози характеризуються невідомими сигнатурами та відсутністю патчів на момент атаки. Водночас, найбільш ефективним є поєднання декількох класів рішень, зокрема пісочниць, поведінкового аналізу, пасток, IDS/IPS та систем управління вразливостями. При цьому значна частина інструментів потребує висококваліфікованого персоналу, що суттєво збільшує загальні витрати на кіберзахист підприємства, а платформи з відкритим кодом скорочують прямі витрати, але потребують вищого рівня технічної експертизи, що змінює структуру, а не обсяг інвестицій.

Отже, доцільним є застосування багаторівневої архітектури захисту (Defense-in-Depth, DiD), що мінімізує ймовірність успішної атаки за рахунок комбінування засобів. Враховуючи те, що наразі найбільша ефективність протидії кіберзагрозам може бути досягнуто шляхом використання принципу багаторівневого захисту. Відповідно пропонується використовувати саме такий підхід. Розрахунок витрат на прикладі невеликого виробництва електронних комплектуючих подвійного призначення наведено в табл. 2.

Таблиця 2

Розрахунок витрат на прикладі невеликого виробництва електронних комплектуючих подвійного призначення *

№	Інструменти	Платформа	Вартість із розрахунку 30 серверних хостів
1	2	3	4
1.	Пісочниця (ізольоване середовище)	OSS-Fuzz/ClusterFuzz	-----
2.	Виявлення на рівні програми	Cloudflare	6 000 у.е
3.	Пастки (decoy-системи)	Labyrinth Deception Platform	13 000 у.е
4.	Поведінковий аналіз та машинне навчання	CrowdStrike Falcon «Pro», Splunk, Mayhem	3 500 у.е

Закінчення табл. 2

1	2	3	4
5.	Управління вразливістю та швидке оновлення (patch management).	OpenVAS. Windows: WSUS Linux: Ansible	-----
6.	Мінімальні привілеї, сегментація	OpenLDAP	-----
7.	Системи виявлення та запобігання вторгнення (IDS/IPS).	Zeek, Suricata	-----
8.	Кваліфікований персонал / офіцери кібербезпеки (шість фахівців)	-----	180 000 у.е
Загальна вартість:			202 500 у.е

* Джерело: розроблено авторами.

Як видно з таблиці 2, сукупні витрати на впровадження системи кіберзахисту становлять 202 500 у.е. на рік. Найвагомішою статтею є витрат на кваліфікований персонал кібербезпеки, що становить близько 88% загальної суми. Значна частина платформ є умовно безкоштовною, але потребують інтеграційних робіт, що збільшує операційні витрати. Проте використання лише технологічних рішень без персоналу призведе до різкого зниження ефективності всієї системи.

Зупинка виробництва (Downtime Losses) у зв'язку з несанкціонованим втручанням у роботу інформаційних систем виробництва, яке призвело до значних збоїв у роботі системи та як наслідок до зупинки роботизований систем лінії виробництва.

Вплив кібератаки оцінюється через прямі та непрямі втрати. Втрати від простоїв виробництва (Downtime Losses):

DL = Годинна вартості простою × Кількість годин простою

Прямі та непрямі втрати (Total Loss):

TL = *DC* + Втрати сировини + Ремонт обладнання + Штрафи + Втрата клієнтів

Приклад підрахунку для невеликого виробництва електронних комплектуючих подвійного призначення:

Виробництво: 5472 штук на добу.

Прибуток із одиниці: 6 у.е.

Простій: 24 годин (три дні).

Втрата сировини: 0.

Ремонт обладнання: 7000 у.е.

Втрата замовлень/штрафів: 8000 у.е.

DL = 1 368 × 24

Годинна вартості простою = 1 368 у.е.

Кількість годин простою = 24 години

DL = 32 832

TL = *DL* + Втрати сировини + Ремонт обладнання + Штрафи + Втрата клієнтів

TL = 32 832 + 0 + 7000 + 8000 + 0

TL = 47 832.

Ураховуючи вищевикладене, потрібні витрати на кібербезпеку (cybersecurity costs) становлять: 202 500 у.е на рік. Тобто втрати виробництва від однієї успішної кібератаки, яке призвело до зупинки ліні виробництва складає 47 832 у.е на добу, а річні витрати на забезпечення кібербезпеки повинні становити 202 500 у.е. Відповідно один день простою формує втрати, співставні з 23% річних витрат на кібербезпеку, в свою чергу за 6 днів простою втрати становлять 211 992 у.е., що перевищує річні інвестиції на 9 492 у.е. Навіть поодинокі інциденти можуть знівелювати економію від недостатнього фінансування кіберзахисту.

У свою чергу більший час простою збільшить розмір втрат, а декілька зупинок виробництва на рік призведе до того, що річні втрати підприємства перевищать видатки, які доцільно було витратити на забезпечення кібербезпеки. Ураховуючи зазначене в обчисленнях відіграють роль такі основні значення:

втрати від простоїв виробництва (Downtime Losses);

втрата сировини (приклад: зміни в IT-інфраструктурі призвели до приведенні сировини в брак);

вартість ремонту обладнання (відновлення після падіння інфраструктури);

втрата замовлень/штрафів (штрафні санкції та втрати продовольчих підрядників);

витати на забезпечення кібербезпеки (cybersecurity costs).

Отже втрати від простою 6 днів (144 год.) становлять 211 992 у.е., що більше ніж річні витрати на кібербезпеку (cybersecurity costs = 202 500 у.е.) на 9 492 у.е.

Візуалізація статистичних даних на графіку зображено на рис. 1. Якщо ROICC > 0**,** інвестиції в кіберзахист окупаються**,** оскільки запобігли більшим втратам. Для розглянутого прикладу під час простою > 5 днів:

$$ROICC \approx 0{,}04 \ (>0)$$

Отже, впровадження комплексної системи кіберзахисту вимагає суттєвих витрат, але економічні втрати від навіть одного тривалого простою значно перевищують річні інвестиції в безпеку. Запропонований науково-методичний підхід оцінювання витрат дає змогу чітко виявити критичні точки економічної доцільності, зокрема поріг у 5–6 днів простою. Розрахунок ROICC підтверджує, що система кіберзахисту є фінансово виправданою та забезпечує зменшення потенційних збитків. Підхід може бути використаний для планування бюджету кібербезпеки, моделювання ризиків та оптимізації архітектури захисту.

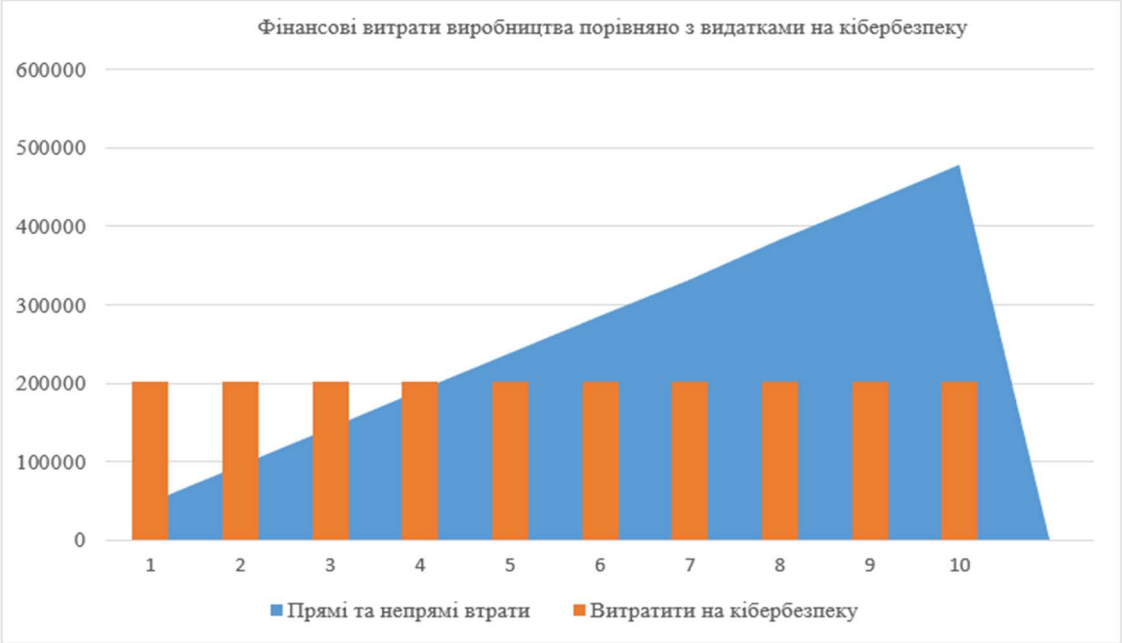

Рисунок 1 – Візуалізація статистичних даних [Розроблено авторами]

Графік, наведений на рис. 1 демонструє, що фінансові втрати від кібератаки понесені виробництвом на п'ятий день простою, будуть більшими ніж потрібні річні видатки на забезпечення кібербезпеки. Показник окупності витрат на кібербезпеку:

витрати без СС – скільки б виробництво втратило без інвестицій у систему кібербезпеки;

витрати з СС – втрати, які ще можливі, навіть із кіберзахистом (наприклад, частковий простій, збої, дрібні інциденти);

витрати на СС – скільки витрачено на систему кібербезпеки;

Якщо ROICC > 0, то окупаються інвестиції, а економія перевищує витрати.

Оцінювання ефективності витрат на кібербезпеку доцільно проводити за виразом:

$$\text{ROICC} = \frac{\text{Витрати без СС} - \text{Витрати з СС} - \text{Витрати на СС}}{\text{Витрати на СС}} \times 100\% \quad (1)$$

Висновки

В умовах війни та зростаючої ролі кіберпростору в забезпеченні безперервності виробничих процесів, конкурентоспроможності та економічної стійкості підприємств запропонований підхід до оптимізації витрат на кібербезпеку дає змогу по-новому оцінити критичність загроз нульового дня, а також обґрунтувати превентивні інвестиції у захисну інфраструктуру. Він демонструє, що навіть одна успішна кібератака, яка призводить до зупинки виробництва, може згенерувати втрати, співмірні або більші за річний бюджет на кібербезпеку, що підтверджує необхідність системного планування таких витрат.

Аналіз сучасних підходів до оцінювання кіберризиків та витрат на кіберзахист свідчить, що наявні моделі здебільшого зосереджуються на класифікації загроз, оцінці рівня захищеності окремих інформаційних систем або застосуванні нечіткої логіки для формалізації ризиків, але рідко інтегрують економічні параметри збитків і бюджетні обмеження підприємства в єдину систему ухвалення рішень.

Запропонований в статті підхід поєднує результат такого аналізу з конкретними інструментами багаторівневого кіберзахисту та їх вартісною характеристикою, що дозволяє перейти від загальнотеоретичних оцінок до практично орієнтованого економічного моделювання. Використання коефіцієнта окупності витрат на кібербезпеку (ROICC) забезпечує кількісне оцінювання ефекту від упровадження системи захисту, що дає змогу управлінцям порівнювати альтернативні конфігурації кіберзахисту та обирати такі, які максимально знижують ризики при заданому рівні ресурсних обмежень.

Практичне значення науково-методичного підходу зводиться до можливості застосовування як інструменту підтримки управлінських рішень у виробничих і технологічних компаніях подвійного призначення, де вартість простою є особливо високою. На основі наведеного підходу підприємства можуть формувати обґрунтовані бюджети на кібербезпеку, ранжувати інструменти захисту за критеріями ефективність/вартість, оцінювати наслідки зміни конфігурації захисних систем та визначати порогові значення тривалості простою, за яких інвестиції у кіберзахист стають критично необхідними.

Отримані результати також демонструють, що навіть за консервативних припущень щодо обсягів виробництва й тривалості простою сукупні збитки від

кібератак швидко перевищують витрати на впровадження багаторівневої системи захисту, особливо у випадку повторюваних інцидентів протягом року. Це підтверджує доцільність розгляду витрат на кібербезпеку не як обтяжливих операційних витрат, а як стратегічних інвестицій у стійкість бізнес-моделі та зниження ймовірності катастрофічних втрат.

Перспективи подальших досліджень. У подальших дослідженнях доцільно зосередитись на розширенні запропонованого підходу за рахунок урахування ймовірнісних характеристик загроз нульового дня, сценарного аналізу для різних типів підприємств і галузей, а також на інтеграції показників кіберстійкості в загальну систему фінансового та стратегічного контролінгу. Перспективним напрямом є також розроблення й обґрунтування коефіцієнту окупності витрат на кібербезпеку як головного інтегрального показника, який дасть змогу визначати доречність витрат підприємства на кібербезпеку.

Конфлікт інтересів. Автори повідомляють про відсутність конфліктів інтересів, що впливають на результати дослідження.

Фінансування. Фінансування дослідження не здійснювалося

Доступність даних. Дослідження виконано з використанням виключно відкритих даних, доступних у публічних джерелах

Використання засобів штучного інтелекту (далі – ШІ). Під час написання статті застосовувалися засоби ШІ, для оброблення списку бібліографічних джерел. Використання автором засобів ШІ не призвело до порушення авторських прав й етичних норм наукового дослідження, а згенерований контент (оформлення списку літератури) був перевірений і відповідає дійсності.

Список бібліографічних посилань

1. Лютий О. І., Калганова В. І., Стець К. М. Методи визначення витрат на кібербезпеку. *Моделювання та інформаційні системи в економіці.* 2022. № 102. 137–147 с. DOI: https://doi.org/10.33111/mise.102.11.

2. Барташевська Ю. М. Оцінка ефективності витрат компанії на інформаційну безпеку. *Науковий вісник Міжнародного гуманітарного університету. Серія: Економіка і менеджмент.* 2017. № 28. С. 87–90.

3. Вітер С. А., Світлишин І. І. Захист облікової інформації та кібербезпека підприємства. *Економіка і суспільство*. 2017. Вип. 11. С. 497–500. URL: https://economyandsociety.in.ua/journals/11_ukr/80.pdf (дата звернення: 11.02.2025).

4. Асєєва Л. А., Шушура О. М. Оцінка ризиків конфіденційності інформаційної безпеки проектів на основі нечіткої логіки. *Телекомунікаційні та інформаційні технології.* 2021. № 1. DOI: https://doi.org/10.31673/2412-4338.2021.0108895.

5. Міщенко А. В., Курило О. В., Золотухіна О. А. Нечітка модель оцінки ризиків інформаційної безпеки та підтримки рівня захищеності ERP-систем. *Телекомунікаційні та інформаційні технології*. 2020. № 1 (66). С. 142–151. DOI: https://doi.org/10.31673/2412-4338.2020.011451.

6. Ісмагілов А. І., Сініцин І. П. Модель виявлення багатопрофільних загроз нульового дня в умовах обмежених ресурсів. *Сучасні інформаційні технології у сфері безпеки та оборони.* 2025. № 2 (53). С. 26–34. DOI: https://doi.org/10.33099/2311-7249/2025-53-2-26-34.

7. Шостак Л. В., Федонюк А. А., Помазун О. О. Особливості кібербезпеки бізнесу в умовах воєнного часу. *Цифрова економіка та економічна безпека*. 2024. № 3 (12). С. 121–125. DOI: https://doi.org/10.32782/dees.12-22.

8. Гладка Ю. А., Галіцин В. Є. Протидія використанню шкідливого програмного забезпечення як різновиду кібератак. *Наука і техніка сьогодні*. 2024. № 4 (32). С. 894–908. DOI: https://doi.org/10.52058/2786-6025-2024-4(32)-894-908.

9. Бєгун А. В., Шкоденко Т. В. Аналіз особливостей систем захисту великих даних в електронному бізнесі. *Моделювання та інформаційні системи в економіці.* 2022. № 102. С. 24–32. DOI: https://doi.org/10.33111/mise.102.3.

10. Дзюба Л. Ф., Чмир О. Ю. Оцінювання ризиків інформаційної безпеки з використанням методів математичної статистики. *Вісник Львівського державного університету безпеки життєдіяльності*. 2022. № 26. DOI: https://doi.org/10.32447/20784643.26.2022.06.

SCIENTIFIC AND METHODOLOGICAL APPROACH TO OPTIMISING ENTERPRISE CYBERSECURITY COSTS UNDER RESOURCE CONSTRAINTS

ISMAHILOV Artur, The Institute of Software Systems of the National Academy of Sciences of Ukraine, Kyiv, Ukraine, https://orcid.org/0009-0002-1332-8147

SINITSYN Igor, Doctor of Technical Sciences, Professor, The Institute of Software Systems of the National Academy of Sciences of Ukraine, Kyiv, Ukraine, https://orcid.org/0000-0002-4120-0784

Formulation of the problem in general. *The paper presents the results of a study focused on developing a scientific and methodological framework for the economically grounded allocation of enterprise cybersecurity expenditures under resource constraints and the increasing prevalence of multi-vector zero-day threats.* ***The proposed*** *approach integrates a Defence-in-Depth architecture with a quantitative model to estimate operational and financial losses from cyber incidents. This integration enables the formal optimisation of the cybersecurity investment structure based on cost–loss trade-off analysis and constrained resource allocation.*

Research methods. *The study employs economic-mathematical modelling, comparative analysis of cybersecurity tools, elements of a risk-oriented approach, and quantitative evaluation of direct and indirect losses from production downtime. To illustrate the proposed methodology, a hypothetical case of a small manufacturer of dual-use electronic components is presented, including calculations of downtime-related losses and the Return on Investment in Cybersecurity Costs (ROICC).*

Literature review. *A review of the literature on risk analysis, technical and cryptographic protections, and infrastructure security components highlights an unresolved challenge: determining the economically justified level of investment in multi-layered cybersecurity amid complex zero-day threats and limited resources. The relationship between potential production losses, threat likelihood, and actual preventive expenditures remains underexplored.*

Research results*. The research offers a generalised classification of cybersecurity tools for mitigating zero-day threats, including their effectiveness, limitations, implementation platforms, and approximate cost for a fixed number of server hosts. An approach is proposed for calculating total production downtime losses resulting from a successful cyberattack, encompassing both direct and indirect components (downtime losses, equipment repair, penalties, and lost orders). The findings demonstrate that cumulative losses incurred after only a few days of downtime may exceed the enterprise's annual cybersecurity budget, underscoring the economic feasibility of preventive investments. Based on these results, the study proposes the ROICC indicator as a decision-support tool for determining the scale and configuration of protective measures.*

Research novelty. *The cybersecurity cost optimisation model proposed in this study is grounded in a comparison between annual investments in protective toolsets and the potential production losses due to operational downtime caused by cyberattacks. Employing a cybersecurity cost-effectiveness metric enables a quantitative evaluation of the benefits associated with implementing security measures, allowing decision-makers to assess alternative cybersecurity configurations and select those that optimally mitigate risks within predefined resource constraints*

Theoretical and practical significance. *The study advances approaches to the economic assessment of cyber risks by integrating zero-day threat assessment models, risk-oriented analysis, and cost-loss evaluation into a unified methodology for optimising enterprise cybersecurity. The practical relevance lies in the applicability of the proposed methodology for enterprise managers, particularly those operating in manufacturing and critical technological sectors, when justifying cybersecurity budgets, prioritising and selecting protective tools, and assessing the effectiveness of implemented measures in terms of reducing potential cyberattack-related losses.*

Conclusions and future work. *Future research should advance the proposed model by integrating probabilistic characteristics of zero-day threats, conducting scenario-based analyses across diverse enterprise types and industry sectors, and embedding cybersecurity resilience metrics within a comprehensive financial and strategic controlling framework. Furthermore, the development and rigorous validation of a cybersecurity cost-effectiveness coefficient is recommended as a principal integrative metric for assessing the efficiency and appropriateness of enterprise cybersecurity investments.*

Keywords: *cybersecurity, zero-day threats, Return on Investment in Cybersecurity Costs, cybersecurity expenditure optimisation.*

References

1. Liutyi, O. I., Kalhanova, V. I., Stets, K. M., (2022). Methods for determining cybersecurity costs. *Modeling and Information Systems in Economics.* 102. 137-147. DOI: https://doi.org/10.33111/mise.102.11. **2. Bartashevska, Yu. M.,** (2017). Assessment of the effectiveness of company expenditures on information security. *Scientific Bulletin of the International Humanitarian University. Series: Economics and Management*. 28, 87-90. **3. Viter, S. A., Svitlyshyn, I. I.,** (2025). Protection of accounting information and enterprise cybersecurity. *Economy and Society*. 11, 497-500. [online]. Available at: https://economyandsociety.in.ua/journals/11_ukr/80.pdf [Accessed: 11 February 2026]. **4. Asieieva, L. A., Shushura, O. M.,** (2021). Assessment of information security confidentiality risks of projects based on fuzzy logic. *Telecommunication and Information Technologies*. 1. DOI: https://doi.org/10.31673/2412-4338.2021.0108895.

5. Mishchenko, A. V., Kurylo, O. V., Zolotukhina, O. A., (2020). A fuzzy model for assessing information security risks and maintaining the security level of ERP systems. *Telecommunication and Information Technologies*. 1(66), 142-151. DOI: https://doi.org/10.31673/2412-4338.2020.011451.

6. Ismahilov, A. I., Sinitsyn, I. P., (2025). A model for detecting multi-profile zero-day threats under limited resources. *Modern Information Technologies in the Sphere of Security and Defence*. 2(53), 26-34. DOI: https://doi.org/10.33099/2311-7249/2025-53-2-26-34. **7. Shostak, L. V., Fedoniuk, A. A., Pomazun, O. O.,** (2024). Features of business cybersecurity under wartime conditions. *Digital Economy and Economic Security*. 3(12), 121-125. DOI: https://doi.org/10.32782/dees.12-22. **8. Hladka, Yu. A., Halitsyn, V. Ye.,** (2024). Counteracting the use of malicious software as a type of cyberattack. *Science and Technology Today*. 2024. 4(32), 894-908. DOI: https://doi.org/10.52058/2786-6025-2024-4(32)-894-908.

9. Biehun, A. V., Shkodenko, T. V., (2022). Analysis of the features of big data protection systems in e-business. *Modeling and Information Systems in Economics*. 102, 24-32. DOI: https://doi.org/10.33111/mise.102.3. **10. Dziuba, L. F., Chmyr, O. Yu.,** (2022). Assessment of information security risks using methods of mathematical statistics. *Bulletin of Lviv State University of Life Safety*. 26. DOI: https://doi.org/10.32447/20784643.26.2022.06.

Рукопис надійшов до редакції *10.03.2026*
Рукопис прийнято до друку після рецензування *30.03.2026*
Дата публікації *30.04.2026*