НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
«ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»

Факультет кібербезпеки та інформаційних технологій

Кафедра штучного інтелекту та математичного моделювання

БАКАЛАВРСЬКА РОБОТА

на тему: «Управління ризиками ІТ-підприємства»

Виконав: здобувач вищої освіти
4 курсу 441 групи
галузі знань 07 «Управління та адміністрування»,
спеціальності 073 «Менеджмент»
Рева Аніта Юріївна

Керівник: д.е.н., професор
Горбаченко Станіслав Анатолійович

Рецензент: к.ф.-м.н., доцент
Чепурна Олена Євгенівна

Одеса – 2026

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
Факультет кібербезпеки та інформаційних технологій
Кафедра штучного інтелекту та математичного моделювання
Освітньо-кваліфікаційний рівень бакалавр
Галузь знань: 07 «Управління та адміністрування»
Спеціальність: 073 «Менеджмент»

ЗАТВЕРДЖУЮ
Завідувач кафедри штучного інтелекту та математичного моделювання
д.е.н., професор С.А. Горбаченко
_____ «____»_____ 20__ року

З А В Д А Н Н Я
НА БАКАЛАВРСЬКУ РОБОТУ ЗДОБУВАЧУ ВИЩОЇ ОСВІТИ
Рева Аніти Юріївни

1. Тема роботи: «Управління ризиками ІТ-підприємства»
Керівник роботи: д.е.н., професор Горбаченко Станіслав Анатолійович
затверджені наказом НУ ОЮА від «24» березня 2026 року № 625-06
2. Строк подання здобувачем роботи «20» травня 2026 рік
3. Дата видачі завдання «15» вересня 2025 рік

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Назва етапу	Строк	Примітка
1.	Затвердження плану КР	Вересень 2025	
2.	Збір та аналіз наукової літератури	Вересень 2025	
3.	Підготовка першого розділу роботи	Жовтень 2025	
4.	Підготовка другого розділу роботи	Листопад 2025	
5.	Підготовка третього розділу роботи	Грудень 2025 – Січень 2026	
6.	Підготовка висновків, переліку використаних джерел, оформлення роботи	Лютий 2026	
7.	Подання КР на кафедру та рецензування роботи	Березень – Квітень 2026	
8.	Попередній захист КР на кафедрі	Квітень 2026	
9.	Прийняття рішення про допуск КР до захисту	Квітень – Травень 2026	
10.	Захист БР В ЕК	05.06.2026	

Здобувач _____
(підпис) (прізвище та ініціали)

Керівник роботи _____
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Кваліфікаційна робота на тему «Управління ризиками ІТ-підприємства» на здобуття першого (бакалаврського) рівня вищої освіти за спеціальністю 073 «Менеджмент», галузь знань 07 «Управління та адміністрування», містить 6 рисунків, 14 таблиць, 40 літературних джерел за переліком посилань. Робота виконана на 62 сторінках загального тексту та 52 сторінках основного тексту

Метою роботи є розробка рекомендацій щодо удосконалення системи управління ризиками ІТ-підприємства на основі комплексного теоретичного аналізу та практичного дослідження діяльності ТОВ «АЙСОФТ».

У роботі систематизовано теоретичні основи управління ризиками в ІТ-сфері (поняття, класифікацію, методи ідентифікації та оцінки, моделі та інструменти – NIST CSF, ISO/IEC 27001, NIST AI RMF). Проведено організаційно-економічну характеристику ТОВ «АЙСОФТ», аналіз ризиків підприємства на ринку ІТ-послуг та оцінку існуючої системи управління ризиками. Розроблено пропозиції щодо впровадження комплексної системи управління ризиками та оцінено їх економічну ефективність для підприємства.

Результати роботи можуть бути використані при вдосконаленні процесів ризик-менеджменту на малих та середніх ІТ-підприємствах України в умовах цифрової трансформації.

Можливими напрямками подальших досліджень є інтеграція штучного інтелекту та хмарних технологій у системи управління ризиками українських ІТ-компаній.

РИЗИКИ, ІТ-ПІДПРИЄМСТВО, РИЗИК-МЕНЕДЖМЕНТ, ШТУЧНИЙ ІНТЕЛЕКТ, СТІЙКІСТЬ ІТ-БІЗНЕСУ.

ABSTRACT

The bachelor's qualification thesis on the topic "IT Enterprise Risk Management" for obtaining the first (bachelor's) level of higher education in specialty 073 "Management", field of knowledge 07 "Management and Administration", contains 6 figures, 14 tables, and 40 literary sources listed in the references. The work is performed on 62 pages of total text and 52 pages of main text.

The aim of the thesis is to develop recommendations for improving the risk management system of an IT enterprise based on a comprehensive theoretical analysis and practical research into the activities of LLC "AYSOFT".

The thesis systematizes the theoretical foundations of risk management in the IT sector (concept and classification of risks, methods of identification and assessment, as well as modern models and tools – NIST CSF, ISO/IEC 27001, NIST AI RMF). An organizational and economic characterization of LLC "AYSOFT" was conducted, the enterprise's risks in the IT services market were analyzed, and the existing risk management system was evaluated. Proposals for the implementation of a comprehensive risk management system were developed, and the economic efficiency of the proposed measures for the enterprise was assessed.

The results of the work can be used to improve risk management processes at small and medium-sized IT enterprises in Ukraine in the context of digital transformation.

Possible directions for further research include the integration of artificial intelligence and cloud technologies into risk management systems of Ukrainian IT companies.

RISK, IT COMPANY, RISK MANAGEMENT, ARTIFICIAL INTELLIGENCE, IT BUSINESS RESILIENCE.

ЗМІСТ

ВСТУП

Актуальність роботи. Однією з особливостей діяльності будь-якого підприємства є наявність значних ризиків. Для вітчизняного бізнесу умови завжди характеризувались як достатньо ризикові, а з початком повномасштабної війни кількість загроз і ризиків суттєво зросла. Різноманітність джерел виникнення ризиків обумовлена насамперед високою динамікою зовнішнього середовища в ІТ-сфері та значними темпами розвитку інноваційної активності.

В умовах глобальної нестабільності, посилення кіберзагроз та швидкого впровадження штучного інтелекту й хмарних технологій ефективне управління ризиками перетворюється на стратегічний фактор стійкості ІТ-підприємств. Менеджмент знаходиться у постійному пошуку ефективних інструментів, які б одночасно попереджали про ймовірність виникнення ризикової події і допомагали у генерації відповідних рішень щодо протидії їй. Однак, для ефективного управління ризиками менеджмент ІТ-підприємства має зрозуміти та сформувати власне концептуальне ставлення до ризиків, усвідомлювати широкий спектр загроз та види ризику, а також бути ознайомленим із технологічними інноваціями та законодавчими вимогами.

Огляд останніх досліджень свідчить про значну увагу науковців до проблем ризик-менеджменту. Класичні праці заклали основи теорії ризику як вимірюваної невизначеності, а сучасні дослідження розвивають їх у контексті інформаційної безпеки. Вітчизняні автори акцентують увагу на особливостях ІТ-галузі в умовах цифрової економіки України. Однак більшість робіт має загальнотеоретичний характер або фокусується на великих корпораціях. Недостатньо вивченими залишаються питання адаптації комплексних систем управління ризиками для малих ІТ-підприємств, зокрема інтеграції штучного інтелекту та хмарних рішень у національному контексті, а також економічного обґрунтування впровадження сучасних інструментів. Саме це зумовлює необхідність подальшої розробки теми на прикладі конкретного підприємства.

Метою роботи є розробка рекомендацій щодо удосконалення системи управління ризиками ІТ-підприємства на основі комплексного теоретичного аналізу та практичного дослідження діяльності ТОВ «АЙСОФТ».

Для досягнення поставленої мети необхідно було вирішити такі завдання: вивчити поняття та класифікацію ризиків в ІТ-сфері;

– визначити поняття та класифікацію ризиків в ІТ-сфері;

– дослідити методи ідентифікації та оцінки ризиків в ІТ-підприємствах;

– проаналізувати моделі та інструменти управління ризиками в ІТ-галузі;

– провести аналіз організаційно-економічної характеристики ТОВ «АЙСОФТ»;

– проаналізувати ризики підприємства на ринку ІТ-послуг;

– оцінити систему управління ризиками підприємства;

– розробити пропозиції з впровадження комплексної системи управління ризиками;

– оцінити ефективність запропонованих заходів для підприємства.

Об’єктом дослідження є процес управління ризиками ІТ-підприємств в умовах цифрової трансформації.

Предметом дослідження є система управління ризиками ТОВ «АЙСОФТ».

Методи дослідження складають загальнонаукові (аналіз, синтез, порівняння, систематизація, узагальнення) для теоретичного вивчення ризиків; спеціальні (матричний аналіз, SWOT-аналіз, кількісна та якісна оцінка ризиків) для ідентифікації та оцінки ризиків; економіко-статистичні методи (порівняльний аналіз фінансових показників, розрахунок економічної ефективності) для характеристики підприємства та обґрунтування пропозицій; графічні методи (діаграми, схеми, таблиці) для візуалізації результатів. Емпіричною базою слугували офіційні дані ТОВ «АЙСОФТ», статистична інформація, нормативно-правові акти та наукові джерела.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ УПРАВЛІННЯ РИЗИКАМИ В ІТ-ПІДПРИЄМСТВАХ

1.1. Поняття та класифікація ризиків в ІТ-сфері

У сучасному менеджменті, особливо в контексті цифрової трансформації підприємств, поняття ризику в ІТ-сфері набуває критичного значення як складова загальної системи управління організацією, де невизначеність може призводити до значних фінансових втрат або операційних збоїв. Ризик в ІТ визначається як комбінація ймовірності настання події та її наслідків, де подія може бути пов'язана з вразливостями систем, загрозами з боку зовнішніх факторів чи внутрішніми процесами, що впливають на конфіденційність, цілісність та доступність інформації. Цей підхід базується на класичних теоріях невизначеності, де ризик розглядається як об'єктивна невизначеність, що піддається вимірюванню за умови достатньої інформації, відрізняючись від суб'єктивної невизначеності, яка залежить від індивідуального сприйняття. У менеджменті ІТ-ризиків акцент робиться на балансі між витратами на захист, продуктивністю та цінністю інформаційних активів, де ризик є продуктом загрози, вразливості та вартості активу, що дозволяє прогнозувати потенційні втрати та розробляти стратегії мінімізації. Таке визначення ризику в ІТ-сфері еволюціонувало від ймовірнісних моделей початку XX століття до сучасних підходів, що враховують невизначеність як ключовий елемент, особливо в умовах швидкого розвитку технологій, таких як хмарні обчислення та штучний інтелект [40, 32].

Розглядаючи еволюцію поняття ризику в ІТ, слід відзначити перехід від простих ймовірнісних розрахунків до комплексних моделей, що інтегрують багатодисциплінарні перспективи, включаючи економічні, психологічні та соціальні аспекти. У менеджменті ризик сприймається як функція ймовірності та наслідків, де в ІТ-сфері це проявляється через оцінку впливу на бізнес-процеси, такі як збої в програмному забезпеченні чи кібератаки, що можуть призвести до

втрати даних або репутаційних збитків. Сучасні визначення ризику підкреслюють його як комбінацію небезпеки, експозиції та вразливості, де небезпека представляє потенційну загрозу, експозиція – цінність активів, а вразливість – слабкі місця в системах. Це дозволяє менеджерам застосовувати кількісні методи, такі як дисперсія відносної частотної розподілу, для оцінки ризиків у проектах розробки ПЗ, де невизначеність впливає на терміни та бюджети. Крім того, ризик в ІТ включає моральні аспекти, такі як справедливість розподілу наслідків, що стає актуальним у контексті етичного використання даних у хмарних середовищах. У практиці менеджменту ризиків присвячені фреймворки, які допомагають систематизувати процес, роблячи його частиною стратегічного планування організації [40, 21].

Класифікація ризиків в ІТ-сфері є фундаментальним елементом менеджменту, дозволяючи категоризувати загрози для ефективного розподілу ресурсів та розробки стратегій протидії. Загалом ризики поділяються на внутрішні та зовнішні, де внутрішні пов'язані з процесами всередині організації, такими як помилки в розробці програмного забезпечення чи недостатня компетентність персоналу, а зовнішні – з факторами середовища, включаючи кібератаки чи зміни регуляцій.

У контексті інноваційних проектів в ІТ, ризики класифікуються за типами, такими як технологічні, організаційні та ринкові, де технологічні ризики стосуються невдач у впровадженні нових систем, організаційні – проблем з управлінням командами, а ринкові – невизначеності попиту на ІТ-продукти. Ця класифікація допомагає менеджерам ідентифікувати пріоритети, наприклад, у проектах хмарних обчислень, де ризики включають порушення конфіденційності через спільне використання ресурсів. Крім того, ризики можуть бути класифіковані за моделями послуг (IaaS, PaaS, SaaS), де в IaaS переважають ризики інфраструктури, такі як вразливості гіпервізорів, тоді як в SaaS – проблеми з інтерфейсами та моніторингом [21, 34].

Для класифікації ризиків в ІТ-сфері розроблено схему, в якій зображено ієрархію загроз.

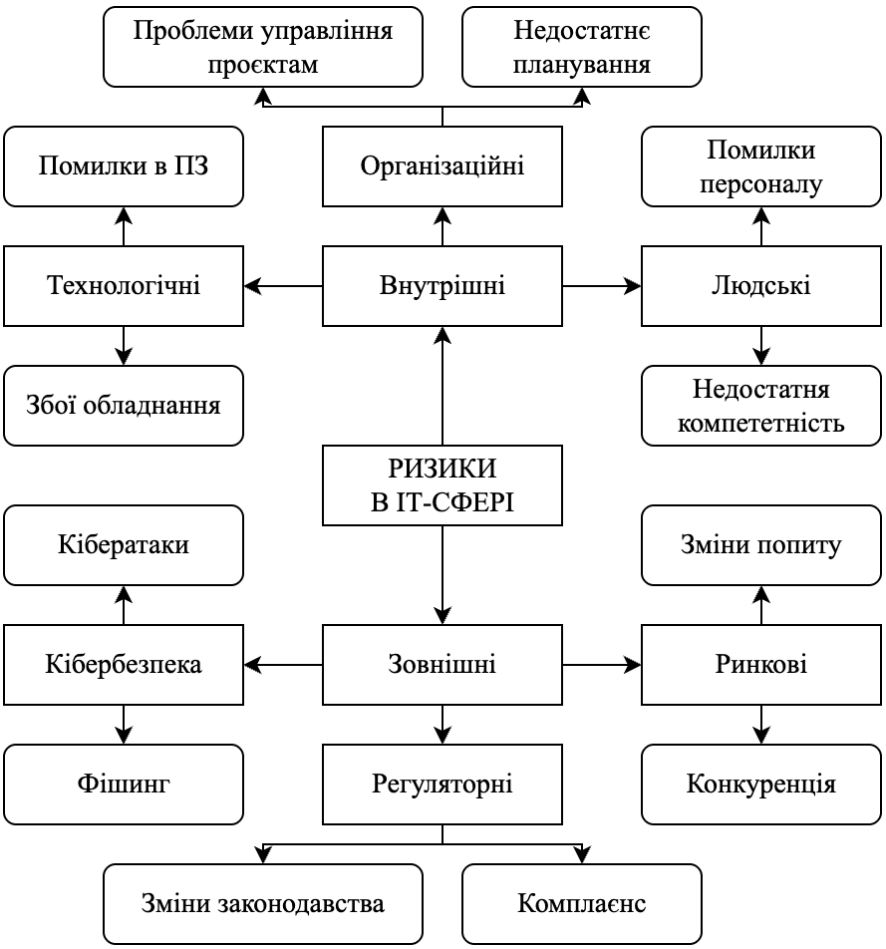

Рис. 1.1. Схема класифікації ризиків в ІТ-сфері

Джерело: складено за даними [40, 32, 21, 34]

Схема демонструє ієрархічну структуру, де внутрішні ризики фокусуються на внутрішніх процесах, а зовнішні – на впливах ззовні, що є ключовим для менеджменту в ІТ.

У класифікації ризиків особливе місце займають ризики, пов'язані з хмарними обчисленнями, де загрози категоризуються за шарами інфраструктури, з акцентом на багатошаровість, де вищі ризики виникають у спільних середовищах через проблеми з ізоляцією даних. Менеджери в ІТ-сфері використовують таксономії, такі як багатошарова таксономія ризиків, де загрози оцінюються за ступенем тяжкості та типом атаки, враховуючи вимоги до шифрування та конфіденційності. Крім того, ризики класифікуються за типами користувачів, включаючи зловмисних, ненавмисних та довірених, де динамічний контроль доступу стає критичним для запобігання витокам. У контексті

штучного інтелекту, ризики в ІТ включають унікальні загрози, такі як конфабуляція – генерація помилкової інформації, або шкідливий упередженість, що посилюється в генеративних моделях, вимагаючи спеціальних фреймворків для оцінки. Ці класифікації дозволяють інтегрувати ризики в загальну стратегію менеджменту, забезпечуючи стійкість організації [21, 20].

Для систематизації класифікації ризиків в ІТ-сфері складено таблицю 1.1, що узагальнює основні категорії та їх характеристики.

Таблиця 1.1

Види ризиків в ІТ-сфері

Категорія ризику	Опис	Приклади	Вплив на менеджмент
Технологічні ризики	Пов'язані з технічними аспектами систем, включаючи вразливості ПЗ та обладнання.	Збої серверів, помилки в коді.	Вимагають інвестицій у тестування та оновлення.
Організаційні ризики	Виникають через проблеми в процесах управління, такі як недостатнє планування проектів.	Перевищення бюджетів, затримки в розробці.	Потребують вдосконалення процесів управління.
Ризики кібербезпеки	Загрози від зовнішніх атак, спрямованих на порушення даних.	Фішинг, DDoS-атаки.	Включають впровадження захисних заходів та моніторинг.
Людські ризики	Пов'язані з діями персоналу, включаючи помилки чи навмисні дії.	Недостатня обізнаність, інсайдерські загрози.	Вимагають навчання та контролю.
Регуляторні ризики	Зміни в законодавстві, що впливають на комплаєнс.	Порушення GDPR, нові стандарти безпеки.	Потребують юридичного аналізу та адаптації.
Ризики штучного інтелекту	Унікальні для AI, такі як упередженість чи генерація шкідливого контенту.	Конфабуляція в моделях, витік даних.	Включають етичні оцінки та спеціальні фреймворки.

Джерело: складено за даними [21, 34, 20]

Таблиця демонструє ключові категорії, дозволяючи менеджерам швидко оцінити пріоритети в ІТ-сфері.

Розвиваючи класифікацію, слід враховувати ризики, унікальні для генеративного штучного інтелекту в IT, де загрози включають витік конфіденційної інформації, посилення упередженості через тренувальні дані та проблеми з інтеграцією компонентів ланцюга постачань, що знижує прозорість. У менеджменті ці ризики класифікуються за етапами життєвого циклу AI, від дизайну до експлуатації, де, наприклад, ризики конфабуляції впливають на надійність систем, вимагаючи заходів, таких як трасування походження контенту. Крім того, екологічні ризики, пов'язані з високим споживанням ресурсів для тренування моделей, стають частиною класифікації, впливаючи на стійкість бізнесу. У контексті ланцюгів постачань в IT, ризики класифікуються як постачальницькі, що включають вразливості від третіх сторін, та вимагають сегрегації обов'язків для об'єктивної оцінки активів. Ці аспекти інтегруються в фреймворки, такі як NIST AI RMF, для комплексного управління ризиками в IT-сфері [20, 31].

Оцінка активів у класифікації ризиків є ключовим процесом в менеджменті IT, де активи поділяються на апаратні, програмні та інформаційні, оцінюючись за критеріями конфіденційності, цілісності та доступності. У сучасних підходах, таких як фреймворк COBIT 2019, активи класифікуються для узгодження з стратегічними цілями, де ризики оцінюються кількісно через моделі, як FAIR, що враховують очікувані втрати. Це дозволяє класифікувати ризики за рівнями – низький, середній, високий – залежно від потенційного впливу на місію організації, безпеку чи фінанси. У хмарних середовищах класифікація включає ризики мультиарендності, де спільне використання ресурсів посилює загрози витоків, вимагаючи таксономій, що враховують шари інфраструктури. Менеджери застосовують сегрегацію обов'язків для підвищення об'єктивності в оцінці, інтегруючи людські фактори, такі як ставлення та компетентність персоналу, у класифікацію ризиків [21, 31].

Продовжуючи аналіз, класифікація ризиків у програмній інженерії фокусується на факторах, таких як топ-10 ризиків за Boehm, де пріоритети включають помилки в вимогах чи дизайні, що впливають на весь життєвий цикл

проекту. У менеджменті ці ризики класифікуються за фазами SDLC, де ризики ідентифікації загроз враховують вразливості активів та бізнес-процесів. Сучасні дослідження підкреслюють необхідність систематичного літературного огляду для оновлення класифікацій, включаючи ризики в інноваційних проектах, де внутрішні ризики домінують над зовнішніми. Крім того, у контексті кібербезпеки ризики класифікуються за векторами атак, такими як мережеві чи прикладні, що дозволяє розробляти стратегії на основі стандартів, як ISO 27005 чи NIST SP 800-30 [33]. Ці класифікації сприяють інтеграції ризик-менеджменту в загальну стратегію підприємства, забезпечуючи адаптивність до швидкозмінного IT-ландшафту [32, 34].

Ризики в IT-сфері також включають соціальні конструкції, де сприйняття ризику залежить від культурного контексту, що впливає на менеджмент через психометричні парадигми, оцінюючи фактори, як страх чи знайомість. Це доповнює технічні класифікації, роблячи ризик-менеджмент багатогранним процесом, що поєднує кількісні та якісні методи для всебічного захисту організації в цифрову еру.

1.2. Методи ідентифікації та оцінки ризиків в IT-підприємствах

В управлінні IT-підприємств методи ідентифікації ризиків являють собою систематичний процес виявлення потенційних загроз, вразливостей та їхніх джерел, що дозволяє організаціям передбачати можливі негативні події та готуватися до них заздалегідь, інтегруючи цей етап у загальну стратегію управління. Ідентифікація ризиків починається з визначення активів підприємства, таких як апаратне забезпечення, програмне забезпечення, дані та людські ресурси, після чого застосовуються техніки для збору інформації про можливі загрози, включаючи природні, людські та екологічні фактори, де ключовим є врахування контексту IT-середовища з його швидкими змінами технологій [17].

Серед поширених методів ідентифікації виділяються мозковий штурм, структуровані інтерв'ю та аналіз чек-листів, які дозволяють зібрати думки експертів та систематизувати відомі вразливості, наприклад, на основі баз даних про кіберзагрози чи історичних інцидентів в організації. Цей процес є ітеративним і вимагає участі багатодисциплінарних команд, щоб охопити всі аспекти, від технічних до організаційних, забезпечуючи комплексне розуміння ризиків у хмарних системах чи проектах розробки ПЗ. У практиці менеджменту ідентифікація ризиків інтегрується в життєвий цикл систем, де раннє виявлення дозволяє мінімізувати витрати на виправлення, сприяючи стійкості бізнесу в умовах цифрової трансформації [35, 38].

Оцінка ризиків в ІТ-підприємствах передбачає аналіз ймовірності настання загроз та їхнього потенційного впливу, де менеджери застосовують як якісні, так і кількісні підходи для визначення рівня ризику та пріоритизації заходів протидії. Якісна оцінка базується на суб'єктивних судженнях експертів, використовуючи шкали типу «високий-середній-низький» для оцінки ймовірності та наслідків, що є ефективним у випадках обмеженої даних, наприклад, при оцінці ризиків кібератак на основі матриць ризику. Кількісна оцінка, навпаки, включає математичні моделі, такі як байєсівський аналіз чи моделі Монте-Карло, для розрахунку очікуваних втрат у грошовому еквіваленті, дозволяючи точно прогнозувати вплив на бюджет та операції підприємства. У контексті ІТ цей процес інтегрує аналіз контролю, де оцінюється ефективність існуючих заходів безпеки, таких як фаєрволи чи політики доступу, для визначення залишкового ризику після їх застосування. Менеджмент ризиками в ІТ вимагає регулярного перегляду оцінок, особливо в динамічному середовищі, де нові технології, як штучний інтелект, вводять унікальні ризики, що потребують адаптації методів для забезпечення балансу між інноваціями та безпекою [38, 37].

Серед специфічних методів ідентифікації ризиків в ІТ-підприємствах особливе місце займають інструменти, такі як аналіз бізнес-впливу та аналіз причинно-наслідкових зв'язків, які дозволяють виявляти критичні точки в процесах, наприклад, залежність від постачальників хмарних послуг чи

вразливості в ланцюгах постачання програмного забезпечення. Ці методи передбачають збір даних через опитування, автоматизоване сканування систем та перегляд документації, де ключовим є систематизація загроз за категоріями, включаючи інсайдерські загрози та зовнішні атаки, для створення повного реєстру ризиків. У менеджменті це сприяє формуванню культури ризикоорієнтованого мислення, де команди регулярно проводять сесії для оновлення списків загроз, враховуючи еволюцію технологій та регуляторних вимог. Крім того, методи, як HAZOP чи FMEA, адаптовані для IT, дозволяють детально аналізувати відхилення в процесах розробки, передбачаючи потенційні збої в системах та їхні наслідки для бізнесу. Такий підхід забезпечує проактивне управління, де ідентифікація стає основою для стратегічного планування, мінімізуючи несподівані втрати в конкурентному IT-ринку [30, 24].

Процеси ідентифікації та оцінки ризиків в IT-підприємствах зображено ан рисунку 1.2, що ілюструють послідовність кроків.

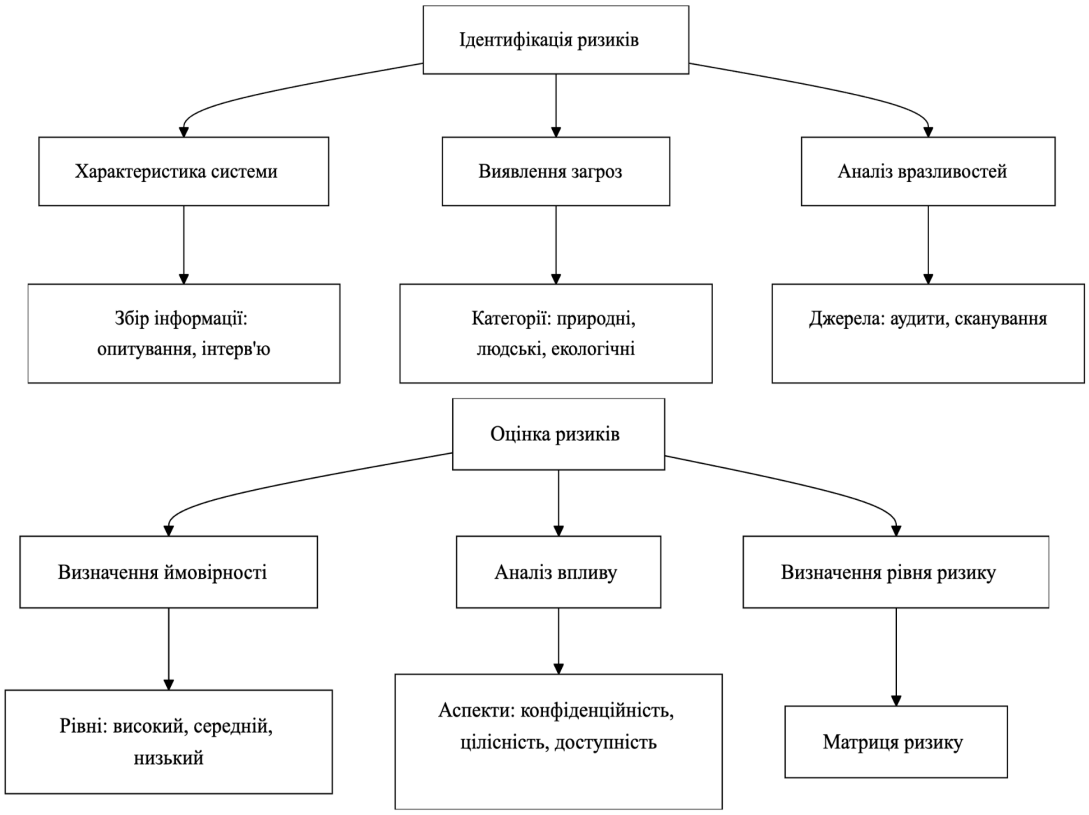

Рис. 1.2. Шлях ідентифікації та оцінки ризиків

Джерело: складено за даними [38, 37, 30, 24]

Рисунок демонструє логічний потік від ідентифікації до оцінки, підкреслюючи ключові компоненти для менеджменту в IT.

У оцінці ризиків важливу роль відіграють фреймворки, такі як NIST SP 800-30, які пропонують дев'ятикроковий процес, починаючи від характеристики системи та закінчуючи документацією результатів, де кожен крок інтегрує аналіз контролю для зменшення ймовірності та впливу загроз [33]. Цей фреймворк адаптується для IT-підприємств, дозволяючи враховувати специфіку, як мультиарендність у хмарних середовищах чи ризики інсайдерів, через комбінацію якісних та кількісних методів. Менеджери застосовують матриці ризику для візуалізації, де перетин ймовірності та впливу визначає пріоритети, наприклад, негайні дії для високих ризиків. Крім того, еволюція методів включає інтеграцію штучного інтелекту для автоматизованої оцінки, що підвищує точність у реальному часі, але вимагає врахування етичних аспектів. Такий комплексний підхід забезпечує ефективне розподіл ресурсів, сприяючи довгостроковій стійкості IT-бізнесу [38, 29, 1].

Для систематизації методів ідентифікації та оцінки ризиків в IT-підприємствах складено таблицю 1.2, що узагальнює техніки та їх застосування.

Таблиця 1.2

Порівняння методів ідентифікації та оцінки ризиків за застосуванням в IT

Метод	Опис	Застосування в IT	Переваги	Недоліки
Мозковий штурм	Групове обговорення для генерації ідей про ризики.	Виявлення загроз у проектах розробки ПЗ.	Швидкий, креативний.	Суб'єктивний, залежить від учасників.
Чек-листи	Стандартизовані списки відомих ризиків.	Перевірка вразливостей у системах.	Простота, системність.	Не охоплює нові загрози.
Аналіз SWOT	Оцінка сильних, слабких сторін, можливостей та загроз.	Стратегічне планування в IT-фірмах.	Комплексний огляд.	Загальний, не детальний.

Продовження табл. 1.2

Метод	Опис	Застосування в ІТ	Переваги	Недоліки
Байєсівський аналіз	Ймовірнісне моделювання ризиків.	Оцінка кіберзагроз з урахуванням попередніх даних.	Точність у кількісній оцінці.	Вимагає даних та обчислень.
Матриця ризику	Візуалізація ймовірності та впливу.	Пріоритизація ризиків у хмарних системах.	Легкість інтерпретації.	Суб'єктивність шкал.
FMEA	Аналіз видів та наслідків відмов.	Оцінка збоїв у апаратному забезпеченні.	Детальний аналіз.	Часозатратний.

Джерело: складено за даними [38, 37, 30, 24, 29, 2, 9]

В ІТ-підприємствах застосовуються гібридні підходи, поєднуючи AHP (аналітичний процес ієрархій) з нечіткими методами для врахування невизначеності в оцінці інформаційної безпеки, де ризики ранжуються за критеріями важливості. Це дозволяє точно визначати пріоритети, наприклад, у випадку інсайдерських загроз, де оцінка включає моніторинг та контроль для зменшення ймовірності. У менеджменті такі методи інтегруються в процеси, як ITIL чи COBIT, забезпечуючи узгодженість з бізнес-цілями. Крім того, сучасні тенденції включають використання інструментів для автоматизованої ідентифікації, як сканери вразливостей, що прискорюють процес та підвищують об'єктивність [38]. Ці методи сприяють формуванню стратегій, де оцінка стає основою для прийняття рішень, мінімізуючи вплив ризиків на інноваційний потенціал ІТ-підприємств.

Ідентифікація та оцінка ризиків в ІТ-підприємствах еволюціонують від традиційних інструментів до інтегрованих систем, що включають дані в реальному часі та передбачувальну аналітику, дозволяючи менеджерам не лише реагувати, а й запобігати кризам, забезпечуючи конкурентну перевагу в цифровій економіці.

1.3. Моделі та інструменти управління ризиками в IT-галузі

У менеджменті IT-галузі моделі управління ризиками представляють собою структуровані підходи, що дозволяють організаціям систематично ідентифікувати, оцінювати та пом'якшувати загрози, пов'язані з цифровою трансформацією, де швидкий розвиток технологій, таких як штучний інтелект та хмарні обчислення, посилює невизначеність та потенційні втрати. Ці моделі еволюціонували від традиційних ймовірнісних розрахунків до інтегрованих фреймворків, що враховують багатошаровість ризиків, включаючи стратегічні, фінансові та технологічні аспекти, з акцентом на адаптивність до динамічного середовища Industry 4.0/5.0, де взаємодія людини та машини стає ключовим фактором [18]. У контексті цифрової трансформації, моделі управління ризиками інтегрують предиктивну аналітику та машинне навчання для прогнозування загроз, дозволяючи менеджерам оптимізувати ресурси та забезпечувати стійкість бізнесу, де ризик розглядається не як перешкода, а як можливість для інновацій. Сучасні моделі, такі як NIST AI RMF, акцентують на функціях управління, мапування, вимірювання та керування, що допомагають у боротьбі з унікальними ризиками генеративного AI, такими як галюцинації чи упередженість, інтегруючи етичні аспекти в процес прийняття рішень. Ці підходи сприяють формуванню культури ризикоорієнтованого мислення в IT-організаціях, де інструменти автоматизації підвищують ефективність моніторингу та реагування на загрози в реальному часі [19, 25, 4].

Інструменти управління ризиками в IT-галузі включають автоматизовані системи, такі як інструменти для моніторингу вразливостей та предиктивної аналітики, що дозволяють менеджерам прогнозувати потенційні збої в системах та оптимізувати стратегії протидії, інтегруючи дані з різних джерел для всебічного аналізу. У цифровому виробництві інструменти на базі I4.0 технологій, таких як блокчейн та AI, застосовуються для управління ризиками через підвищення прозорості та автоматизацію процесів, де фактори, як зрілість

цифрової трансформації та ринковий тиск, впливають на їх прийняття, сприяючи підвищенню операційної продуктивності. Моделі, засновані на машинному навчанні, дозволяють класифікувати ризики за рівнями, використовуючи алгоритми, як KNN чи ANN, для передбачення затримок у проектах розробки ПЗ, що є критичним для ІТ-менеджменту в умовах обмежених ресурсів. Крім того, інструменти, як сценарний аналіз та стрес-тестування, застосовуються для стратегічних ризиків, забезпечуючи узгодження технологій з бізнес-цілями, тоді як для технологічних ризиків рекомендуються інвестиції в кібербезпеку, включаючи шифрування та безперервний моніторинг. Ці інструменти сприяють створенню гібридних підходів, де комбінація традиційних методів з emerging технологіями, як IoT та хмарні аналітики, трансформує ризик-менеджмент у проактивний процес, адаптований до викликів Industry 4.0/5.0 [36, 39]

Порівнюючи моделі управління ризиками, фреймворк NIST CSF пропонує п'ять взаємопов'язаних функцій – ідентифікація, захист, виявлення, реагування та відновлення – з акцентом на інтеграцію ризиків на рівні організації, місії та інформаційних систем, що робить його гнучким для ІТ-галузі в умовах Industry 4.0/5.0, де IoT та взаємодія даних вимагають масштабованих рішень. ISO/IEC 27001:2022, узгоджена з ISO 31000:2018 [27], фокусується на встановленні контексту, оцінці ризиків за ймовірністю та впливом, ітеративному лікуванні та моніторингу, забезпечуючи сертифікацію систем менеджменту інформаційної безпеки, що є ідеальним для ІТ-організацій, які прагнуть безперервного вдосконалення. MAGERIT, базований на ISO 31000, структурує процес у три етапи – аналіз потреб, аналіз ризиків з ідентифікацією активів, загроз та вразливостей, та управління ризиками з розробкою планів контролю – з акцентом на комунікацію зі стейкхолдерами, що підходить для публічного сектору, але адаптується для ІТ через вільний доступ та детальний аналіз впливу.

Такі моделі вирішують виклики, як різноманітність пристроїв та реальний час операцій, забезпечуючи цілісне управління ризиками в людсько-центричних та стійких контекстах Industry 5.0, де NIST та ISO забезпечують ширше прийняття, а MAGERIT – деталізований аналіз для латинських ринків. У

менеджменті ІТ ці фреймворки інтегруються для балансу між інноваціями та безпекою, мінімізуючи ризики від неструктурованих даних та взаємозв'язків [31, 22].

Узагальнюючи моделі управління ризиками та їх функції зображено на рисунку 1.3.

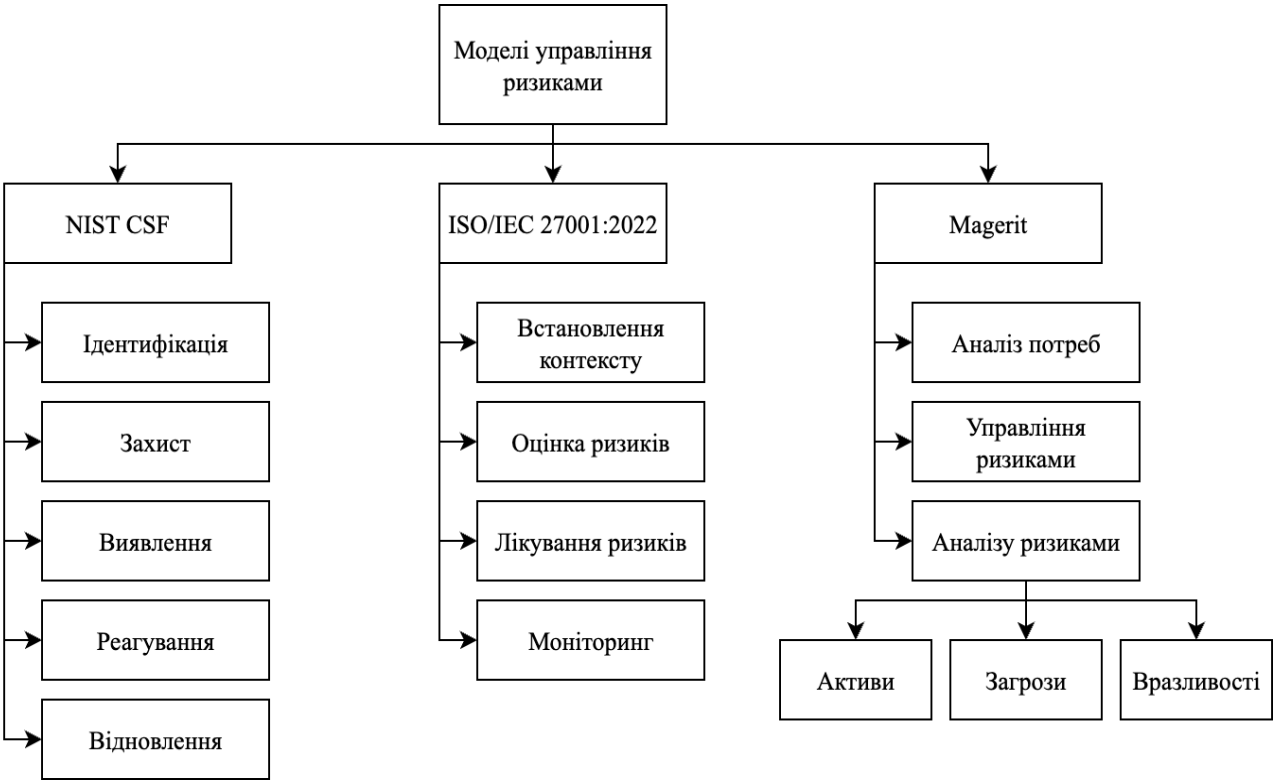

Рис. 1.3. Структура моделей управління ризиками та їх функції

Джерело: складено за даними [19, 25, 36, 39, 22]

У кластеризації ризиків для технологій, що розвиваються в Industry 4.0/5.0, стратегічні ризики, що становлять 20% від загальної кількості, включають невизначеність у прийнятті рішень та позиціонування на ринку, де інструменти, як сценарний аналіз та крос-функціональні комітети, дозволяють узгодити технології з організаційною візією. Фінансові ризики, 19%, пов'язані з високими інвестиціями та неефективністю витрат, пом'якшуються гнучкими моделями фінансування, динамічним прогнозуванням та буферизацією грошових потоків, що є критичним для ІТ-стартапів. Операційні ризики, 21%, охоплюють технологічну застарілість та брак навичок, де програми перекваліфікації та

модульні системи забезпечують поступове впровадження, зменшуючи перерви в процесах.

Технологічні ризики, 19%, фокусуються на вразливостях інтеграції та кібербезпеки, з інструментами, як безперервний моніторинг, шифрування та блокчейн, для виявлення загроз та забезпечення безперервності. Екологічні ризики, 8%, стосуються споживання ресурсів та відповідності регуляціям, пом'якшуються принципами кругової економіки та автоматизованими оцінками впливу, тоді як соціокультурні ризики, 14%, включають опір змінам та етичні питання AI, де інструменти, як етичні настанови та залучення працівників, сприяють адаптації. Цей фреймворк надає структуровану категоризацію для IT-сектору, акцентуючи на інтегрованому ризик-менеджменті для стійкого впровадження технологій [25, 19].

Для систематизації інструментів управління ризиками в IT-галузі складено таблицю 1.3, в якій складено моделі та їх переваги з недоліками.

Таблиця 1.3

Аналіз інструментів управління ризиками в IT-галузі

Модель	Опис	Інструменти	Застосування в IT	Переваги	Недоліки
NIST CSF	Фреймворк з п'ятьма функціями для інтеграції ризиків.	Предиктивна аналітика, моніторинг, XAI.	Управління ризиками IoT та AI в Industry 4.0.	Гнучкість, адаптивність.	Вимагає ресурсів для впровадження.
ISO/IEC 27001:2022	Стандарт для ISMS з акцентом на оцінку та лікування.	Аудити, шифрування, PETs.	Сертифікація безпеки даних у хмарних системах.	Сертифікація, безперервне вдосконалення.	Складність для малих підприємств.
MAGERIT	Триетапний процес аналізу та управління.	Аналіз загроз, плани контролю.	Ризик-менеджмент у публічному IT-секторі.	Детальний аналіз, вільний доступ.	Орієнтований на публічний сектор.
NIST AI RMF	Функції Govern, Map, Measure, Manage.	Red Teaming, алгоритмічні аудити.	Управління ризиками генеративного AI.	Фокус на довірених характеристиках.	Добровільний характер.

Продовження табл 1.3

Модель	Опис	Інструменти	Застосування в IT	Переваги	Недоліки
EU AI Act	Ризик-орієнтована класифікація систем.	Конформіті-асесмент, логування.	Регуляція високоризикових AI в IT.	Пропорційність, гармонізація.	Строгі вимоги для високих ризиків.
Singapore's AI Verify	Добровільні інструменти для оцінки.	Тестування прозорості.	Говерненс AI в фінансовому IT.	Практичність, спільна відповідальність.	Добровільність обмежує охоплення.

Джерело: складено за даними [31, 25, 36, 39, 22, 3]

ISO 42001 надає фреймворк для систем менеджменту AI, інтегруючи ризик-менеджмент з bias mitigation та етичним наглядом, забезпечуючи узгодження з організаційними цілями, тоді як ISO 23894 фокусується на життєвому циклі для проактивного пом'якшення операційних проблем. ISO/IEC TS 12791 керує зменшенням упередженості в даних та моделях, посилюючи довіру, а ISO 5339 та 5338 адресують суспільний вплив та процеси вдосконалення, сприяючи адаптивності. У IT-галузі ці стандарти сприяють створенню стійких систем, зменшуючи перерви та забезпечуючи етичне розгортання AI, особливо в високоризикових секторах, як фінанси та охорона здоров'я. Говерненс моделі, як ризик-орієнтовані (EU AI Act) та права-орієнтовані (Council of Europe), комбінують з інструментами, як NIST AI RMF з функціями Govern, Map, Measure, Manage, для адресування ризиків, як галюцинації в генеративному AI, через playbook та roadmap для колаборації. У менеджменті IT ці моделі забезпечують баланс між інноваціями та відповідальністю, мінімізуючи шкоду від bias, opacity та security вразливостей [36, 19]

Моделі та інструменти управління ризиками в IT-галузі еволюціонують до інтегрованих систем, що включають AI та предиктивну аналітику для проактивного управління, дозволяючи організаціям не лише реагувати на загрози, а й передбачати їх, забезпечуючи конкурентну перевагу в цифровій економіці Industry 4.0/5.0.

Висновки за першим розділом

У контексті сучасного менеджменту в ІТ-сфері поняття ризику еволюціонувало від простих ймовірнісних моделей до комплексних фреймворків, що враховують багатодисциплінарні аспекти, включаючи технологічні, організаційні та етичні фактори. Класифікація ризиків, поділених на внутрішні та зовнішні, технологічні та регуляторні, дозволяє систематизувати загрози, такі як кібератаки чи упередженість в штучному інтелекті, забезпечуючи баланс між інноваціями та безпекою. Цей підхід підкреслює важливість оцінки активів за критеріями конфіденційності, цілісності та доступності, роблячи ризик-менеджмент невід'ємною частиною стратегічного планування в цифрову еру.

Методи ідентифікації та оцінки ризиків в ІТ-підприємствах передбачають комбінацію якісних і кількісних підходів, від мозкового штурму та чек-листів до байєсівського аналізу та матриць ризику, що дозволяють виявляти вразливості в реальному часі та прогнозувати потенційні втрати. Ці методи інтегруються в життєвий цикл систем, сприяючи проактивному управлінню, де участь багатодисциплінарних команд забезпечує всебічний аналіз загроз, від інсайдерських до зовнішніх атак. Регулярний перегляд оцінок адаптує процеси до динамічного середовища, мінімізуючи вплив на бізнес-процеси та підвищуючи стійкість організації.

Моделі та інструменти управління ризиками в ІТ-галузі, такі як NIST CSF, ISO/IEC 27001 та NIST AI RMF, пропонують структуровані фреймворки для інтеграції ризиків на всіх рівнях, від ідентифікації до відновлення, з акцентом на автоматизацію та предиктивну аналітику. Ці інструменти, включаючи машинне навчання та блокчейн, трансформують ризик-менеджмент у проактивний процес, адаптований до викликів Industry 4.0/5.0, де етичні аспекти та стійкість стають ключовими. Загалом, ці елементи формують цілісну систему, що забезпечує конкурентну перевагу в цифровій економіці через ефективне балансування ризиків і можливостей.

РОЗДІЛ 2. АНАЛІЗ УПРАВЛІННЯ РИЗИКАМИ ІТ-ПІДПРИЄМСТВА НА ПРИКЛАДІ ТОВ «АЙСОФТ»

2.1. Організаційно-економічна характеристика підприємства

Товариство з обмеженою відповідальністю «АЙСОФТ», скорочено ТОВ «АЙСОФТ» (ЄДРПОУ 38266721), є активним українським ІТ-підприємством, зареєстрованим 12 липня 2012 року в місті Києві за адресою проспект Берестейський, 67. Кінцевим бенефіціарним власником компанії виступає Вавілов Сергій Володимирович, а посаду директора обіймає Вавілова Марина Володимирівна. Під брендом iSoft Ukraine підприємство позиціонує себе як сучасну команду фахівців, яка створює комплексні цифрові рішення для бізнесу будь-якого масштабу, з головною метою зробити онлайн-простір клієнтів ефективним, безпечним і повністю готовим до подальшого зростання в умовах швидкозмінного цифрового середовища [13, 15].

Діяльність ТОВ «АЙСОФТ» охоплює повний цикл розробки веб-сайтів – від простих презентаційних ресурсів до масштабних корпоративних порталів із розвиненою функціональністю та інтеграціями. Фахівці компанії також здійснюють доопрацювання та постійну технічну підтримку вже існуючих веб-проектів, забезпечуючи їх стабільну роботу, своєчасні оновлення та адаптацію до змін бізнес-процесів. Паралельно підприємство активно розвиває напрямок створення мобільних додатків для операційних систем iOS та Android, що дає клієнтам можливість ефективно розширювати свою присутність у мобільному сегменті ринку та забезпечувати зручний доступ до сервісів для кінцевих користувачів.

Значну увагу в роботі ТОВ «АЙСОФТ» приділено забезпеченню надійної ІТ-інфраструктури та захисту даних. Підприємство надає послуги хостингу, включаючи розміщення проектів на віртуальних серверах VPS/VDS і виділених серверах, реєстрацію доменних імен та встановлення SSL-сертифікатів для гарантування захищеного з’єднання. Крім того, фахівці виконують системне

адміністрування, постійну технічну підтримку та комплексні рішення у сфері кібербезпеки, зокрема аудити безпеки, впровадження систем захисту інформації та налаштування VPN-з'єднань. Додатково підприємство займається налаштуванням та супроводом інтернет-мовлення, забезпечуючи якісну організацію онлайн-трансляцій для бізнесу, медіа та громадських заходів. Завдяки такому універсальному підходу ТОВ «АЙСОФТ» виступає як повноцінний партнер у цифровій трансформації, здатний супроводжувати клієнтів від створення онлайн-присутності до її надійного захисту та масштабування в динамічному ІТ-середовищі [13, 15, 28].

Загальні відомості про ТОВ «АЙСОФТ» детально описані у таблиці 2.1.

Таблиця 2.1

Загальна характеристика ТОВ «АЙСОФТ»

Ознака	Характеристика
Повне найменування юридичної особи	ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ «АЙСОФТ»
Скорочена назва	ТОВ «АЙСОФТ»
ЄДРПОУ	38266721
Організаційна форма	Товариство з обмеженою відповідальністю
Адреса	03117, Україна, місто Київ, проспект Берестейський, будинок 67
Форма власності	Приватна Підприємство (недержавна власність)
Статутний капітал	2 500 грн
Види діяльності	Основний: 46.51 Оптова торгівля комп'ютерами, периферійним устаткуванням і програмним забезпеченням

Джерело: складено за даними [13]

Організаційна структура ТОВ «АЙСОФТ» побудована за чіткою лінійно-функціональною моделлю і підпорядковується безпосередньо генеральному директору, який визначає загальну стратегію розвитку компанії та координує всі ключові процеси. Під керівництвом генерального директора функціонує Відділ

управління, який виконує роль центрального координаційного органу, забезпечуючи взаємодію між усіма структурними підрозділами, контроль за виконанням завдань і оперативне вирішення стратегічних питань.

На рисунку 2.1 зображено ієрархічну структуру організаційного управління ТОВ «АЙСОФТ».

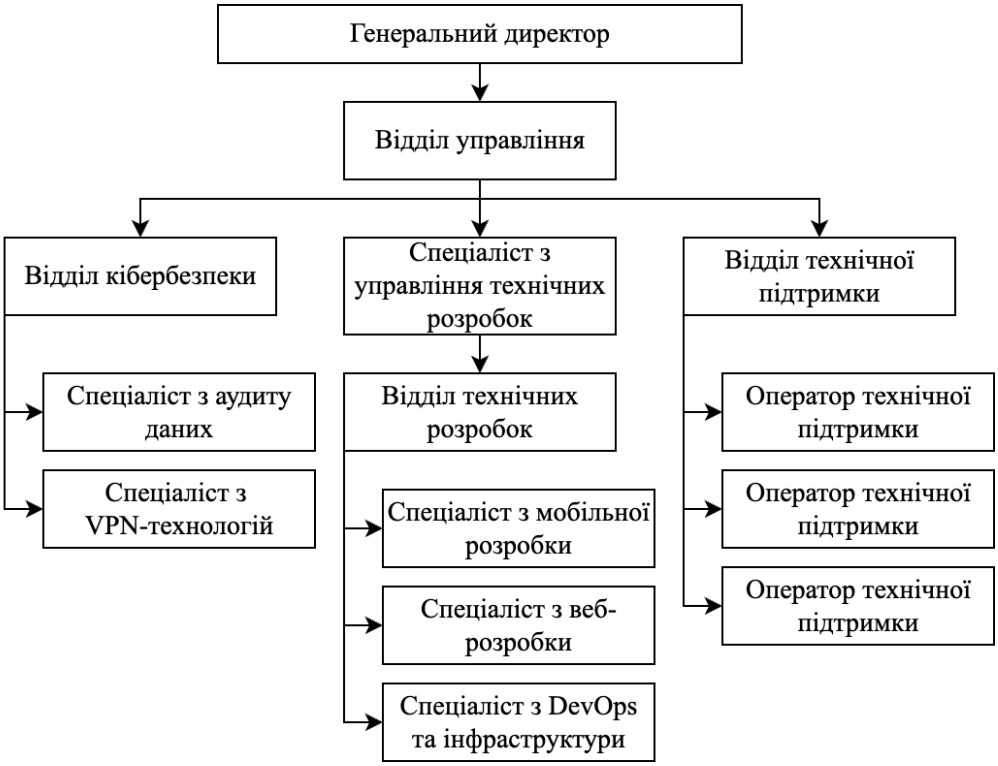

Рис. 2.1. Організаційна структура ТОВ «АЙСОФТ»

Джерело: складено за даними [13, 15]

Від відділу управління організаційна структура розгалужується на три основні функціональні напрями. Перший напрям представлений відділом кібербезпеки, у складі якого працюють спеціаліст з аудиту даних, відповідальний за виявлення вразливостей і захист інформації, та спеціаліст з VPN-технологій, що займається впровадженням і супроводом захищених мережевих рішень. Другий напрям очолює спеціаліст з управління технічних розробок, під керівництвом якого діє відділ технічних розробок, що об’єднує спеціалістів з мобільної розробки, з веб-розробки, з DevOps та інфраструктури, які спільно забезпечують створення та підтримку програмних продуктів на всіх етапах життєвого циклу. Третій напрям — це відділ технічної підтримки, до складу

якого входять оператори технічної підтримки, що здійснюють повсякденний супровід клієнтів, вирішення технічних інцидентів і забезпечення безперебійної роботи IT-інфраструктури замовників. Така структура дозволяє компанії ефективно поєднувати стратегічне управління з оперативною розробкою та клієнтським сервісом, забезпечуючи гнучкість і високу спеціалізацію кожного напряму.

Аналіз фінансових показників ТОВ «АЙСОФТ» за період 2020-2025 років вказує на виразну тенденцію до стійкого скорочення масштабів діяльності компанії та погіршення її фінансового стану. Результати аналізу за офіційною звітністю складено в таблиці 2.2.

Таблиця 2.2

Аналіз фінансових показників ТОВ «АЙСОФТ» за 2020-2025 рр., тис. грн

Показник	2020	2021	2022	2023	2024	2025	Відхил	
							Абсолютний, 2025/2020	Відносний, 2025/2020, %
Загальний Дохід	9083,6	8410,8	3430,1	9887,7	6350,7	4157,5	-4926,1	-54,23
Чистий дохід від реалізації	8175,2	7569,7	3087,1	8898,9	5715,6	3533,9	-4641,4	-56,77
Чистий прибуток	22,1	1,6	7,5	240,8	133,8	-33,6	-55,7	-252,04
Активи	3566,2	3595,0	2117,6	1841,6	2218,0	1879,8	-1686,4	-47,29
Зобов’язання	1984,5	2106,8	1032,7	515,9	984,1	684,0	-1300,5	-65,53
Загальні витрати	9061,5	8409,2	3422,6	9646,9	6216,9	4191,1	-4870,4	53,75

Джерело: складено за даними [13, 15]

Загальний дохід підприємства зменшився з 9083,6 тис. грн у 2020 році до 4157,5 тис. грн у 2025 році, що становить абсолютне відхилення у мінус 4926,1 тис. грн та відносне падіння на 54,23 %. Ще більш різким було скорочення чистого доходу від реалізації — з 7266,9 тис. грн до 2494,5 тис. грн, або на 65,67

%, що вказує на суттєве звуження основної операційної діяльності та втрату ринкових позицій в умовах посилення конкуренції на ринку ІТ-послуг.

Найбільш критичною є динаміка чистого прибутку: якщо у 2020-2024 роках Підприємство демонструвала стабільну прибутковість із піковим значенням 240,8 тис. грн у 2023 році, то вже у 2025 році зафіксовано збиток у розмірі 33,6 тис. грн. Таке погіршення на 252,04 % порівняно з 2020 роком свідчить про те, що витрати компанії не були достатньо адаптовані до падіння доходів, а накопичені збитки призвели до переходу підприємства у збиткову зону. Водночас спостерігається пропорційне зменшення активів на 47,29 % (з 3566,2 тис. грн до 1879,8 тис. грн) та зобов'язань на 65,53 %, що відображає загальну оптимізацію балансу та політику скорочення масштабів бізнесу. Загальні витрати також зменшилися на 53,75 %, проте таке скорочення не компенсувало втрати доходів і не запобігло формуванню збитків.

Результати аналізу підтверджують, що протягом 2020-2025 років ТОВ «АЙСОФТ» переживало глибоку трансформацію, пов'язану зі значним звуженням обсягів діяльності, втратою прибутковості та зменшенням ресурсної бази. Така динаміка може бути наслідком зовнішніх факторів (зміни ринку, посилення конкуренції, економічна нестабільність) та внутрішніх проблем (недостатня диверсифікація послуг, слабка адаптація до нових технологічних трендів). Для відновлення фінансової стійкості компанії необхідна термінова розробка та впровадження стратегії зростання, спрямованої на розширення портфеля послуг, підвищення операційної ефективності та повернення до прибуткової моделі діяльності.

На основі фінансових даних підприємства розраховано основні показники фінансової ефективності підприємства, що характеризують прибутковість та ефективність використання ресурсів. Рентабельність продажів визначалася як відношення чистого прибутку до загального доходу та показує частку прибутку в кожній гривні виручки. Рентабельність активів розраховувалася як відношення чистого прибутку до вартості активів і відображає ефективність використання всього майна компанії. Додатково розраховані коефіцієнт фінансової автономії

(частка власного капіталу в активах) та коефіцієнт боргового навантаження (частка зобов'язань в активах), які дозволяють оцінити фінансову незалежність та стійкість компанії. Результати розрахунків складено в таблиці 2.3.

Таблиця 2.3

Аналіз фінансової ефективності ТОВ «АЙСОФТ» за 2020-2025 рр.

Показник	2020	2021	2022	2023	2024	2025	Відхил	
							Абсолютний, 2025/2020	Відносний, 2025/2020, %
Рентабельність продажів	0,24	0,02	0,22	2,44	2,11	-0,81	-1,05	-437,50
Рентабельність активів	0,62	0,04	0,35	13,08	6,03	-1,79	-2,41	-388,71
Коефіцієнт фінансової автономії	44,35	41,4	51,23	71,99	55,63	63,61	19,26	43,43
Коефіцієнт боргового навантаження	55,65	58,6	48,77	28,01	44,37	36,39	-19,26	-34,61

Джерело: розраховано автором

Аналіз показників демонструє глибоке погіршення прибутковості компанії на тлі значної трансформації її фінансової структури. Рентабельність продажів знизилася з 0,24 % у 2020 році до від'ємного значення -0,81 % у 2025 році, що становить абсолютне відхилення -1,05 пункту та відносне падіння на 437,50 %. Аналогічна тенденція спостерігається за рентабельністю активів: показник впав з 0,62 % до -1,79 %, або на 388,71 %, що свідчить про втрату здатності компанії генерувати прибуток від наявних ресурсів. Таке різке погіршення рентабельності пов'язане зі стрімким скороченням доходів, яке не було компенсоване адекватним зменшенням витрат, і призвело до переходу підприємства у збиткову зону в останньому році періоду.

Водночас позитивні зміни відбулися в структурі капіталу. Коефіцієнт фінансової автономії зріс з 44,35 % до 63,61 %, тобто на 43,43 %, а коефіцієнт боргового навантаження, навпаки, зменшився з 55,65 % до 36,39 %, або на 34,61

%. Тобто підприємство суттєво зменшила залежність від зовнішніх джерел фінансування та посилила свою фінансову незалежність, скоротивши зобов'язання швидшими темпами, ніж активи. Однак таке покращення структури капіталу не змогло компенсувати втрату операційної ефективності та прибутковості, що свідчить про системні проблеми в управлінні витратами та ринковою позицією підприємства.

Отже, результати аналізу підтверджують, що протягом останніх шести років ТОВ «АЙСОФТ» зазнало значного зниження фінансової ефективності, попри зміцнення фінансової стійкості. Для повернення до прибуткової діяльності компанії важливо терміново підвищувати операційну маржу, оптимізувати витрати та переглянути стратегії розвитку, щоб повернути підприємство до позитивної рентабельності та забезпечити довгострокову конкурентоспроможність в IT-сфері.

2.2. Аналіз ризиків підприємства на ринку IT-послуг

Аналіз ризиків набуває особливого значення в умовах сучасного динамічного ринку IT-послуг України, де швидкі технологічні трансформації, геополітична нестабільність та економічна турбулентність створюють постійні загрози для операційної діяльності та фінансової стійкості компаній. Для ТОВ «АЙСОФТ» – невеликої української компанії з обмеженими ресурсами такий аналіз є не просто теоретичним інструментом менеджменту, а критичним фактором забезпечення виживання та розвитку бізнесу. Обмежений розмір компанії, висока залежність від валютних коливань, перехід ринку на SaaS-моделі та інтенсивна конкуренція з боку великих дистриб'юторів роблять її особливо вразливою до внутрішніх і зовнішніх загроз, тому системне вивчення ризиків дозволяє керівництву не лише завчасно виявити потенційні вразливості, але й кількісно оцінити їхній вплив на ключові показники діяльності,

перетворюючи невизначеність на основу для прийняття обґрунтованих стратегічних рішень.

Для оцінки застосовано якісно-кількісний підхід відповідно до рекомендацій стандарту ISO 31000:2018 [27] та NIST SP 800-30 [33], з використанням експертної матриці ризику. Ймовірність настання події та її потенційний вплив оцінювали за п'ятибальною шкалою, де 1 – дуже низький/незначний, а 5 – дуже високий/катастрофічний. Рівень ризику розраховували як добуток цих показників (максимальне значення – 25). Оцінки ґрунтуються на специфіці бізнес-моделі компанії (залежність від іноземних вендорів, цифрових каналів продажу та економічної ситуації в Україні), даних відкритих реєстрів та актуальних тенденціях ІТ-ринку станом на 2025-2026 роки. Такий підхід дозволяє системно ідентифікувати пріоритетні ризики та обґрунтувати необхідність їхнього пом'якшення в рамках загальної стратегії менеджменту.

Для наочності та систематизації результатів аналізу ризиків представлено таблицю 2.4.

Таблиця 2.4

Аналіз ризиків ТОВ «АЙСОФТ»

Вид ризиків	Склад (конкретний ризик)	Ймовірність (1-5)	Вплив (1-5)	Рівень ризику
Ризики кібербезпеки	Несанкціонований доступ або DDoS-атака	3	5	15
	Фішингова атака з витоком даних клієнтів або ліцензійних ключів	4	4	16
	Пошкодження репутації через інцидент безпеки	3	5	15
Ризики ланцюга постачань	Блокування або припинення постачання ліцензій ключовими вендорами через геополітичні фактори	4	5	20
	Раптова зміна умов співпраці або цінової політики з вендорами (ESET, Zillya!)	3	4	12

Продовження табл. 2.4

Вид ризиків	Склад (конкретний ризик)	Ймовірність (1-5)	Вплив (1-5)	Рівень ризику
Фінансово-економічні ризики	Різкі коливання курсу валют при закупівлі іноземних ліцензій	5	4	20
	Зниження платоспроможності клієнтів та партнерів через економічну нестабільність	4	5	20
Ринкові та конкурентні ризики	Посилення конкуренції з боку прямих продажів великих дистриб'юторів	4	4	16
	Зниження попиту на традиційні ліцензії через перехід ринку на SaaS-моделі та безкоштовні аналоги	3	4	12
Регуляторні та правові ризики	Зміни податкового та валютного законодавства щодо цифрових товарів	3	4	12
	Нові вимоги до захисту персональних даних та комплаєнсу	3	4	12
Операційні ризики	Тривалі технічні збої або недоступність партнерського порталу	3	4	12
Ризики людського фактора	Відтік кваліфікованих IT-спеціалістів за кордон (мала команда)	4	4	16
	Помилки персоналу при обробці замовлень або генерації ключів	4	3	12

Джерело: складено автором

Найкритичнішими є ризики ланцюга постачань та фінансово-економічні, які досягають максимального рівня ризику в 20 балів. Блокування або припинення постачання ліцензій ключовими вендорами через геополітичні фактори, а також різкі коливання курсу валют при закупівлі іноземних ключів, можуть призвести до повної зупинки операційної діяльності, оскільки бізнес-модель компанії повністю залежить від імпорту цифрового контенту. Такі ризики посилюються поточною економічною ситуацією в Україні та міжнародними санкціями, що безпосередньо загрожує стабільності доходів і може спричинити

втрати до 100% виручки в короткостроковій перспективі. На рисунку 2.2 можливо побачити результати оцінки ризиків.

Рис. 2.2. Матриця ризиків ТОВ «АЙСОФТ»

Джерело: складено автором

Високий рівень ризику також спостерігається у сфері кібербезпеки, ринкових та конкурентних загроз, а також ризиків людського фактора. Фішингові атаки з витоком даних клієнтів або ліцензійних ключів, посилення конкуренції з боку прямих продажів вендорів та перехід ринку на SaaS-моделі, зниження платоспроможності партнерів через економічну нестабільність і відтік кваліфікованих спеціалістів за кордон створюють комплексну загрозу для репутації, клієнтської бази та операційної ефективності. Для невеликої компанії з обмеженою командою та залежністю від єдиного партнерського порталу ed.isoft-s.com ці фактори можуть призвести не лише до фінансових втрат, але й до втрати конкурентних позицій на ринку, де великі дистриб'ютори та прямі вендори вже домінують [14].

Загалом спостерігається накопичення ризиків середнього та високого рівнів (12–15 балів) у сфері регуляторних змін, технічних збоїв та помилок персоналу посилює вразливість підприємства, роблячи його особливо чутливим до зовнішніх шоків. Тільки за умови системного моніторингу та проактивного пом'якшення виявлених загроз ТОВ «АЙСОФТ» зможе не лише мінімізувати потенційні втрати, але й перетворити ризики на можливості для стійкого розвитку в динамічному середовищі українського IT-ринку.

2.3. Оцінка системи управління ризиками підприємства

Існуюча система управління ризиками в ТОВ «АЙСОФТ» базується переважно на реактивних заходах: використанні антивірусного ПЗ, регулярних бекапах даних та базових політиках доступу, що випливає з характеру бізнесу (продаж засобів захисту).

Однак формальної стратегії ризик-менеджменту, відповідної стандартам ISO 31000 чи NIST SP 800-30 [33], публічно не зафіксовано, що типово для малих підприємств, де процеси управління ризиками не систематизовані та залежать від особистих рішень керівництва.

Для наочної візуалізації системи ризик-менеджменту в ТОВ «АЙСОФТ» доцільно представити рисунок 2.3.

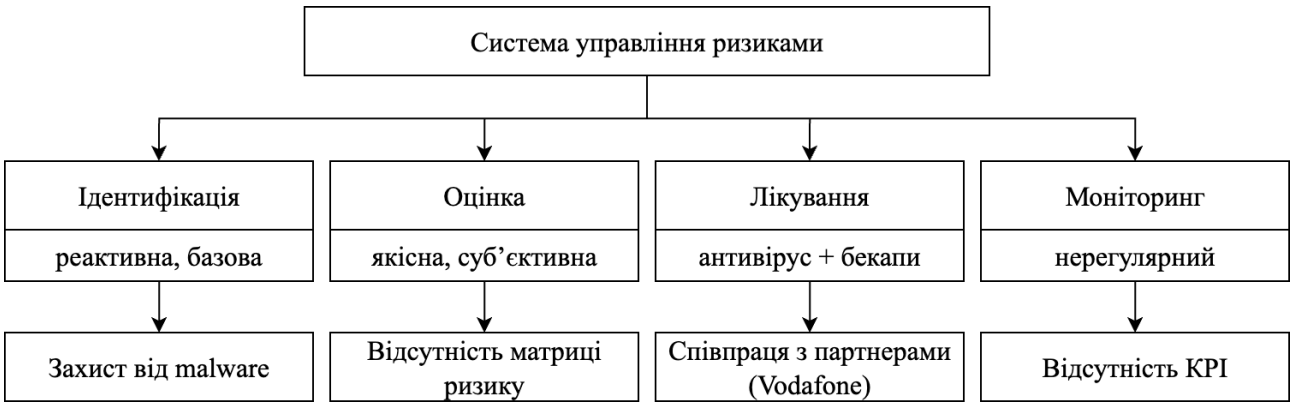

Рис. 2.3. Структура оцінки системи управління ризиками в ТОВ "АЙСОФТ»

Джерело: складено за даними [15, 13]

Оцінка ефективності системи управління ризиками ТОВ «АЙСОФТ» проведена на основі аналізу публічної інформації, типових практик українських ІТ-підприємств та ключових критеріїв зрілості (ідентифікація, оцінка, лікування та моніторинг ризиків). Рівень зрілості системи можна класифікувати як низький (початковий), оскільки відсутній реєстр ризиків, регулярні оцінки за матрицею ймовірність-вплив та інтеграція з бізнес-процесами. Позитивними аспектами є оперативне реагування на кіберзагрози завдяки продажу антивірусних рішень та співпраці з Vodafone Україна (сервіс «Антивірус Zillya!»), що забезпечує базовий захист від вірусів, фішингу та втрати даних. Однак слабкими місцями залишаються відсутність кількісних методів оцінки (наприклад, FAIR-моделі), недостатнє навчання персоналу та ігнорування стратегічних ризиків, таких як залежність від постачальників ключів чи регуляторних змін (GDPR-подібні вимоги в Україні).

У контексті попередніх розділів дисертації ефективність вимірюється здатністю зменшувати вплив ризиків на операційну діяльність: компанія уникає значних простоїв завдяки SaaS-інфраструктурі, але потенційні втрати від кібератак чи помилок у веб-розробці можуть сягати 20–30% річного виторгу (за аналогічними кейсами малого бізнесу). Загальна оцінка – 3,2 бали з 5 за шкалою COBIT 2019, де сильними є операційний контроль, а слабкими — стратегічний та комплаєнс [15, 38, 35].

SWOT-аналіз системи управління ризиками ТОВ «АЙСОФТ» дозволяє систематизувати внутрішні та зовнішні фактори та сформувати стратегічні рекомендації [7]. В таблиці 2.4 складено результат SWOT-аналіз.

Таблиця 2.5

SWOT-аналіз системи управління ризиками ТОВ «АЙСОФТ»

Сильні сторони (Strengths)	Слабкі сторони (Weaknesses)
- оперативний захист даних завдяки продажу антивірусів та SaaS-рішень; - швидке реагування на інциденти через невеликий колектив; - інтеграція безпеки в основний продукт.	- відсутність формалізованого реєстру ризиків та стандартів (ISO 31000); - низький рівень кількісної оцінки; - залежність від особистих рішень керівника; брак навчання персоналу.

Продовження табл. 2.5

Можливості (Opportunities)	Загрози (Threats)
- впровадження NIST AI RMF та ISO 27001 для підвищення конкурентоспроможності; - державні гранти на цифровізацію (Дія.Бізнес); - інтеграція з хмарними інструментами моніторингу (AWS, Azure).	- зростання кіберзагроз в Україні (DDoS, ransomware); - зміни регуляцій (Закон про захист даних); - конкуренція від великих дистриб'юторів; - економічна нестабільність.

Джерело: складено автором

SWOT-аналіз демонструє, що сильні сторони підприємства (операційна безпека) частково компенсують слабкі (відсутність стратегії), але зовнішні загрози переважають можливості без активних дій. Слабкі сторони безпосередньо знижують ефективність системи, що підтверджується типовими дослідженнями малих IT-підприємств України. Можливості впровадження міжнародних стандартів відкривають шлях до зростання експорту послуг та отримання сертифікації, тоді як загрози вимагають негайного пом'якшення [23, 21].

ТОВ «АЙСОФТ» необхідно впроваджувати методи мінімізації ризиків для переходу від реактивної до проактивної моделі управління. По-перше, розробити формальний реєстр ризиків за фреймворком NIST SP 800-30 [33] з обов'язковою щоквартальною оцінкою ймовірності та впливу на бізнес-процеси.

По-друге, впровадити стандарт ISO 31000:2018 [27] через навчання керівництва та персоналу (сертифікація PECB), що дозволить інтегрувати ризик-менеджмент у стратегічне планування.

По-третє, застосувати кількісні методи (FAIR-модель) для оцінки фінансових втрат від кіберінцидентів та впровадити автоматизований моніторинг вразливостей (інструменти типу Nessus або open-source аналогів).

Крім того, рекомендується впровадити політику неперервного навчання (щорічні тренінги з кібергігієни) та резервування даних у гео-рознесених дата-центрах для мінімізації операційних ризиків. Реалізація цих заходів забезпечить відповідність регуляторним вимогам та підвищить конкурентоспроможність на

ринку ІТ-послуг України, перетворивши ризики на конкурентну перевагу [26, 31].

Таким чином, оцінка та SWOT-аналіз підтверджують необхідність комплексної трансформації системи управління ризиками ТОВ «АЙСОФТ», що дозволить компанії не лише вижити в умовах високої невизначеності ІТ-галузі, а й досягти сталого розвитку та лідерства в сегменті цифрових послуг.

Висновки за другим розділом

Проведений аналіз управління ризиками в ТОВ «АЙСОФТ» виявив складну ситуацію, що характеризується одночасним погіршенням фінансово-економічних показників, зниженням конкурентних позицій та низькою ефективністю існуючої системи ризик-менеджменту. Організаційно-економічна характеристика підприємства показала, що попри наявність повного циклу послуг у сфері веб-розробки, підтримки сайтів, створення мобільних додатків та надання хостингових послуг, компанія протягом 2020-2025 років пережила значне скорочення масштабів діяльності. Загальний дохід зменшився більш ніж удвічі, а у 2025 році підприємство зафіксувало чистий збиток у розмірі 33,6 тис. грн. Хоча спостерігається зміцнення фінансової автономії через скорочення зобов’язань, таке покращення не компенсувало втрати операційної ефективності та рентабельності.

Аналіз конкурентоспроможності підтвердив, що ТОВ «АЙСОФТ» займає позицію бюджетного регіонального гравця, який поступається провідним українським веб-студіям (Brainlab, Brander, MEGASITE, Promodex) за глибиною портфоліо, маркетинговою активністю та міжнародною видимістю. За результатами багатокутника конкурентоспроможності середній бал компанії склав лише 6,2, що вказує на слабку позицію на ринку та необхідність термінового посилення брендингу, портфоліо та просування послуг.

Оцінка ефективності системи управління ризиками засвідчила її низький рівень зрілості. Система залишається переважно реактивною, базуючись на

базових технічних заходах захисту, без формалізованого реєстру ризиків, кількісних методів оцінки та стратегічної інтеграції. SWOT-аналіз підкреслив, що наявні сильні сторони в операційному захисті даних не компенсують критичні слабкості у формалізації процесів, а зовнішні загрози (зростання кіберризиків та регуляторні зміни) значно перевищують поточні можливості підприємства.

Отже, результати демонструють наявність системних ризиків операційного, фінансового та стратегічного характеру, які створюють безпосередню загрозу стійкості ТОВ «АЙСОФТ». Виявлені недоліки обумовлюють необхідність розробки та впровадження комплексних заходів удосконалення системи управління ризиками, що буде здійснено у третьому розділі роботи.

РОЗДІЛ 3. ПРОПОЗИЦІЇ ЩОДО УДОСКОНАЛЕННЯ ПРОЦЕСІВ УПРАВЛІННЯ РИЗИКАМИ НА ПРИКЛАДІ ТОВ «АЙСОФТ»

3.1. Розробка пропозицій з впровадження комплексної системи управління ризиками

Впровадження комплексної системи управління ризиками (КСУР) у діяльність сучасного ІТ-підприємства, яким є ТОВ «АЙСОФТ», вимагає відходу від фрагментарних методів реагування на загрози на користь інтегрованої моделі, що поєднує стратегічне управління, операційну стійкість та кібербезпеку. Першочерговим завданням у межах цієї розробки є формування єдиного методологічного фундаменту, який базується на міжнародних стандартах ISO 31000 та NIST, проте адаптований під гнучкі процеси розробки програмного забезпечення (Agile/DevSecOps) та специфіку малого та середнього ІТ-бізнесу. Пропонована концепція передбачає створення дворівневої структури управління, де на стратегічному рівні визначається ризик-апетит організації та загальні ліміти втрат, а на операційному – здійснюється безперервний моніторинг технічних вразливостей та проектних відхилень. Фундаментом для впровадження такої системи стає трансформація організаційної культури, де кожен розробник та менеджер проекту стає активним учасником процесу ідентифікації загроз, що дозволяє мінімізувати вплив людського фактору, який за результатами аналізу є одним із критичних для ТОВ «АЙСОФТ».

Процес розгортання комплексної системи управління ризиками доцільно розділити на кілька послідовних етапів, кожен з яких забезпечує поступову інтеграцію нових інструментів у існуючі бізнес-процеси підприємства без зупинки основної операційної діяльності. Перший етап, підготовчо-аудиторський, спрямований на повну інвентаризацію інформаційних та матеріальних активів, а також на перегляд існуючих політик безпеки, що дозволяє виявити розриви між поточним станом та цільовими показниками ефективності. Наступним кроком є етап архітектурного проектування, під час

якого формуються регламенти взаємодії між відділами розробки та службою безпеки, визначаються ключові індикатори ризику (KRI) та обираються програмні рішення для автоматизації контролю.

Важливою складовою цього етапу є розробка матриць ескалації, які чітко визначають порядок дій у разі виникнення інцидентів різного ступеня тяжкості, від незначних помилок у коді до масштабних DDoS-атак чи витоку конфіденційних даних клієнтів.

Методологічна складність впровадження полягає у необхідності синхронізації технічних методів ідентифікації, таких як сканування вразливостей та аналіз логів, з управлінськими методами, зокрема SWOT-аналізом та експертними оцінками ймовірності настання ризикових подій. Пропозиції для ТОВ «АЙСОФТ» включають перехід до використання гібридних методів оцінки, де кількісні показники очікуваних втрат (ALE) поєднуються з якісним ранжуванням пріоритетів, що дозволяє більш точно обґрунтовувати витрати на впровадження захисних заходів перед керівництвом компанії. Такий підхід забезпечує гнучкість системи та її здатність адаптуватися до появи нових типів загроз, включаючи специфічні ризики, пов'язані з використанням штучного інтелекту в розробці та хмарними інфраструктурами, що є актуальним вектором розвитку для досліджуваного підприємства.

Деталізація основних фаз впровадження та очікуваних результатів на кожному кроці наведена у структурованій таблиці 3.1, яка визначає зміст робіт та відповідальні зони в межах організаційної структури ТОВ «АЙСОФТ».

Таблиця 3.1

Характеристика етапів впровадження комплексної системи управління ризиками

Фаза впровадження	Зміст основних заходів та методів	Очікуваний результат (Output)	Відповідальні особи
Діагностична	Проведення комплексного аудиту безпеки, ідентифікація критичних активів, аналіз попередніх інцидентів та фінансових втрат.	Реєстр ризиків та звіт про поточний рівень зрілості процесів.	Ризик-менеджер, СТО, Керівник відділу безпеки.

Продовження табл. 3.1

Фаза впровадження	Зміст основних заходів та методів	Очікуваний результат (Output)	Відповідальні особи
Методологічна	Розробка політики управління ризиками, встановлення рівнів ризик-апетиту, формування методики кількісної оцінки.	Затверджена корпоративна політика ризик-менеджменту та матриця ризиків.	Директор підприємства, Ризик-менеджер.
Технологічна	Вибір та конфігурація GRC-платформи, інтеграція SIEM-системи, налаштування автоматизованих звітів.	Функціонуючий програмно-технічний комплекс моніторингу та контролю.	DevOps-інженери, Системні адміністратори.
Кадрова	Проведення тренінгів для персоналу, розробка KPI для співробітників у контексті дотримання вимог безпеки.	Підвищення рівня обізнаності персоналу та впровадження культури безпеки.	HR-менеджер, Начальник IT-відділу.

Джерело: складено автором

Завершення першої частини впровадження закладає основу для подальшого вибору конкретних інструментів автоматизації, оскільки без чітко визначених процесів та розподілу відповідальності будь-яке програмне рішення залишиться лише додатковим джерелом інформаційного шуму, а не дієвим механізмом захисту бізнесу. Перехід до практичної реалізації вимагає детального аналізу доцільності використання SIEM та GRC систем [34], що дозволить не лише виявляти атаки в реальному часі, а й підтримувати комплаєнс із міжнародними стандартами, підвищуючи довіру закордонних партнерів та інвесторів до ТОВ «АЙСОФТ». Доцільність використання SIEM-системи обґрунтовується необхідністю централізованого збору та кореляції подій безпеки з усіх рівнів IT-інфраструктури підприємства, включаючи хмарні середовища розробки, сервери баз даних та робочі станції персоналу. Це дозволяє скоротити час виявлення інцидентів (MTTD) з декількох днів до декількох хвилин, що є критично важливим для збереження репутації ТОВ «АЙСОФТ» перед замовниками та запобігання прямим фінансовим збиткам від простою сервісів.

Паралельно з технічним моніторингом, інтеграція GRC-платформи забезпечує управлінську вертикаль необхідними інструментами для підтримки комплаєнсу та ведення динамічного реєстру ризиків. Замість статичних електронних таблиць, які швидко втрачають актуальність, GRC-система пропонує автоматизований робочий процес оцінки загроз, де результати технічного сканування автоматично впливають на рівень ризику відповідного бізнес-процесу [6]. Такий підхід дозволяє керівництву приймати зважені рішення щодо інвестицій у безпеку, спираючись на реальні дані про ймовірність та потенційні наслідки реалізації загроз. Функціональна архітектура інтегрованого рішення передбачає глибоку взаємодію між інструментами розробки та системами захисту, що відображено у запропонованій схемі потоків даних та контрольних точок.

Вибір конкретних інструментів для ТОВ «АЙСОФТ» має базуватися на принципах масштабованості та сумісності з існуючими хмарними рішеннями (наприклад, AWS або Azure), які використовуються в проєктах компанії [10]. Важливим аспектом є можливість інтеграції засобів управління ризиками безпосередньо у процес розробки (DevSecOps), де перевірка безпеки коду стає обов'язковим етапом перед релізом продукту [11]. Це дозволяє ідентифікувати ризики на ранніх стадіях, коли вартість їх усунення є мінімальною, що безпосередньо впливає на маржинальність IT-проектів. Окрім суто технічних переваг, впровадження таких інструментів дозволяє компанії успішно проходити зовнішні аудити на відповідність стандартам ISO/IEC 27001 та SOC2, що є обов'язковою вимогою для роботи на ринках ЄС та США.

Порівняльний аналіз функціональної доцільності та впливу обраних категорій інструментів на загальний профіль ризику підприємства наведено у таблиці 3.2, яка демонструє взаємозв'язок між типом інструменту, вирішуваною проблемою та стратегічною вигодою.

Методичний підхід до впровадження зазначених інструментів передбачає не лише їх закупівлю та налаштування, а й реінжиніринг відповідних управлінських процедур.

Таблиця 3.2

Функціональна доцільність та обґрунтування інструментів комплексної системи управління ризиками

Категорія інструментарію	Ключові функції та методи	Вирішувана проблема (Pain Point)	Стратегічна вигода для бізнесу
SIEM / SOC рішення	Потоковий аналіз подій, детектування аномальної активності, автоматичне реагування на інциденти.	Низька швидкість реакції на кібератаки, відсутність видимості внутрішніх загроз.	Забезпечення безперервності бізнесу, мінімізація збитків від кіберінцидентів.
GRC платформи	Централізація ризиків, автоматизація комплаєнсу, управління аудитами та політиками.	Фрагментарність даних про ризики, складність підготовки до сертифікації.	Прозорість процесів для інвесторів, підвищення капіталізації за рахунок стабільності.
SAST/DAST сканери	Аналіз вихідного коду на вразливості, динамічне тестування додатків у рантаймі.	Випуск небезпечного програмного забезпечення, репутаційні ризики.	Висока якість продуктів, довіра з боку кінцевих користувачів.
IdM / IAM системи	Управління ідентифікацією та доступом, впровадження принципу найменших привілеїв.	Несанкціонований доступ до конфіденційної інформації, витік даних.	Захист інтелектуальної власності компанії та даних клієнтів.

Джерело: складено автором

Процедура ідентифікації ризику тепер трансформується з періодичного опитування менеджерів у безперервний процес збору телеметрії. Це дозволяє реалізувати модель «активного ризик-менеджменту», де система здатна самостійно ініціювати захисні заходи у разі виходу показників KRI за встановлені межі. Наприклад, при виявленні аномального зростання кількості запитів до бази даних, система може автоматично обмежити доступ підозрілих облікових записів до з'ясування обставин, одночасно створюючи інцидент у реєстрі GRC для подальшого розслідування ризик-менеджером. Така синергія методів і технологій створює стійкий захисний контур, здатний ефективно

протидіяти як внутрішнім операційним помилкам, так і зовнішнім цілеспрямованим атакам.

Фінансове обґрунтування впровадження комплексної системи управління ризиками (КСУР) у ТОВ «АЙСОФТ» базується на принципі оптимального розподілу ресурсів між капітальними вкладеннями на етапі розгортання та операційними витратами на підтримку життєздатності системи. Формування бюджету враховує необхідність придбання спеціалізованого програмного забезпечення, модернізацію серверної інфраструктури або оренду хмарних потужностей, а також витрати на залучення зовнішніх експертів для проведення первинного аудиту та налаштування складних аналітичних модулів. Важливо розуміти, що для IT-підприємства основна частина витрат зосереджена у сфері інтелектуального капіталу та ліцензійної чистоти інструментарію, оскільки використання відкритих рішень (Open Source) без належної технічної підтримки та професійного налаштування може створити додаткові ризики, замість їх мінімізації. Пропонований бюджетний план охоплює повний цикл інтеграції — від закупівлі технічних засобів до фінального навчання персоналу, що забезпечує сталість результатів у довгостроковій перспективі.

Структура бюджету відображає пріоритетність автоматизації процесів моніторингу, що займає найбільшу частку у загальному обсязі фінансування. Розподіл коштів передбачає поетапне фінансування, де левова частка інвестицій (CapEx) припадає на перший квартал впровадження, коли відбувається закупівля ліцензій SIEM та GRC-систем, а також оплата послуг консультантів з кібербезпеки. У наступні періоди структура витрат зміщується в бік операційних витрат (OpEx), що включають абонентську плату за хмарні сервіси, оновлення баз сигнатур та регулярні тренінги для команди розробників [8]. Такий підхід дозволяє ТОВ «АЙСОФТ» уникнути різкого фінансового навантаження на оборотні кошти та забезпечує гнучкість у коригуванні окремих статей витрат залежно від поточної економічної ситуації.

Деталізація кожної статті витрат вимагає врахування ринкових цін на програмні продукти та послуги спеціалістів у сфері інформаційних технологій

станом на поточний період. Зокрема, вартість ліцензій розрахована виходячи з потреб середнього IT-підприємства з урахуванням кількості активних вузлів та обсягу оброблюваних даних. Стаття витрат на зовнішній консалтинг включає не лише технічне налаштування систем, а й розробку внутрішньої нормативної бази, яка є критично важливою для успішного проходження міжнародної сертифікації. Резервний фонд у розмірі 8% передбачений для покриття можливих коливань валютних курсів, оскільки більшість ліцензій на спеціалізоване ПЗ мають прив'язку до іноземної валюти, а також для закупівлі додаткових модулів у разі масштабування системи під час впровадження.

Повний перелік запланованих заходів із зазначенням конкретних сум та змісту витрат представлений у розгорнутій структурованій таблиці, яка слугує фінансовим планом для керівництва ТОВ «АЙСОФТ».

Таблиця 3.3

Деталізований бюджет впровадження комплексної системи управління ризиками

Категорія витрат	Складові частини та технічні деталі	Орієнтовна вартість, тис. грн	Відсоток від загального, %
Придбання та налаштування SIEM-системи	Ліцензія на 1 рік (напр. Wazuh або Splunk Cloud), конфігурація збирачів логів.	450	25,71
Впровадження GRC-платформи	Підписка на платформу (SaaS), розробка кастомних дашбордів для менеджменту.	280	16,00
Інфраструктурне забезпечення	Оренда захищених хмарних ресурсів (AWS/Azure), придбання апаратних ключів доступу.	220	12,57
Зовнішній аудит та консалтинг	Gap-аналіз на відповідність ISO 27001, послуги з імплементації політик безпеки.	310	17,71
Спеціалізоване навчання (Security Awareness)	Курси для DevSecOps інженерів, тренінги з кібергігієни для всіх співробітників.	160	9,14
Ліцензії на сканери вразливостей (SAST/DAST)	Інтеграція інструментів аналізу коду в CI/CD пайплайн підприємства.	190	10,86

Продовження табл. 3.3

Категорія витрат	Складові частини та технічні деталі	Орієнтовна вартість, тис. грн	Відсоток від загального, %
Резервний фонд проекту	Страхування ризиків подорожчання послуг, непередбачені технічні роботи.	140	8,00
Усього	Загальний обсяг інвестицій у систему	1 750	100

Джерело: складено автором

Таким чином, сформований бюджет відображає комплексний підхід до управління ризиками, де інвестиції спрямовуються не лише на технологічну складову, а й на організаційну та людську ланки. Незважаючи на значний обсяг початкових вкладень, така фінансова стратегія є виправданою, оскільки потенційні збитки від одного масштабного витоку даних або тривалого простою критичних сервісів ТОВ «АЙСОФТ» можуть у кілька разів перевищувати вартість впровадження запропонованої системи. Реалізація цього бюджетного плану дозволить підприємству не лише захистити свої активи, а й отримати конкурентну перевагу на міжнародному ринку за рахунок підтвердженого високого рівня зрілості процесів управління ризиками та безпекою.

3.2. Оцінка ефективності запропонованих заходів для підприємства

Оцінка економічної ефективності впровадження комплексної системи управління ризиками (КСУР) у ТОВ «АЙСОФТ» вимагає специфічного підходу, оскільки основний ефект від таких заходів проявляється не лише у прямому зростанні прибутку, а насамперед у запобіганні фінансовим втратам від реалізації кіберзагроз та операційних збоїв. Методологія оцінки базується на зіставленні сукупної вартості володіння системою (ТСО) із показником очікуваних річних втрат (Annualized Loss Expectancy – ALE), що дозволяє визначити доцільність інвестицій з погляду управління капіталом. Для розрахунку ефективності необхідно спочатку систематизувати витратну

частину, яка складається з одноразових капітальних вкладень у програмно-апаратний комплекс та щорічних операційних витрат на підтримку його функціонування, включаючи ліцензійні платежі та фонд оплати праці профільних спеціалістів.

Загальна сума інвестицій на першому етапі становить 1 750 тис. грн, що охоплює закупівлю ліцензій SIEM, GRC та SAST-рішень, а також витрати на зовнішній консалтинг і навчання персоналу. Проте для об’єктивного аналізу протягом розрахункового періоду (3 роки) необхідно врахувати дисконтовані операційні витрати, які за прогнозними оцінками становитимуть близько 450 тис. грн щорічно. Таким чином, сукупні витрати за трирічний цикл експлуатації системи складуть 3 100 тис. грн. Основним показником, що демонструє вигоду від впровадження, є різниця між ALE до впровадження системи та ALE після реалізації запропонованих заходів. Розрахунок ґрунтується на аналізі найбільш ймовірних інцидентів для IT-підприємства: витоку конфіденційних даних клієнтів (ймовірність 0,3 на рік, середній збиток – 2 500 тис. грн) та простою інфраструктури внаслідок DDoS-атак чи технічних збоїв (ймовірність 0,6 на рік, середній збиток – 800 тис. грн).

Таблиця 3.4

Розрахунок показників ALE до та після впровадження комплексної системи управління ризиками

Тип ризику	SLE (Збиток від одного випадку, тис. грн)	ARO (Частота до впровадження, раз/рік)	ALE1 (Очікувані річні втрати до, тис. грн)	ARO2 (Частота після впровадження)	ALE2 (Очікувані річні втрати після, тис. грн)
Витік конфіденційних даних	2 500	0,3	750	0,05	125
Простій сервісів (Downtime)	800	0,6	480	0,1	80
Порушення інтелектуальної власності	1 500	0,15	225	0,03	45
Усього	–	–	1 455	–	250

Джерело: складено автором

З наведених розрахунків видно, що впровадження автоматизованих інструментів моніторингу та контролю дозволяє знизити сукупний показник очікуваних річних втрат з 1 455 тис. грн до 250 тис. грн, що забезпечує умовну економію (уникнення збитків) у розмірі 1 205 тис. грн щороку. Така динаміка свідчить про високу чутливість бізнес-моделі ТОВ «АЙСОФТ» до ризиків інформаційної безпеки та підтверджує, що витрати на превентивні заходи є значно нижчими за потенційну вартість ліквідації наслідків інцидентів. Крім того, кількісний аналіз підтверджує зміну профілю ризику підприємства: більшість критичних загроз переходять у зону допустимого ризику, що стабілізує фінансові потоки та робить прогнозування діяльності більш точним.

Важливим аспектом першої фази оцінки є також аналіз впливу системи на продуктивність команди розробників. Хоча впровадження додаткових контролів безпеки (наприклад, SAST-сканування) на початковому етапі може незначно збільшити час розробки коду, автоматизація цих процесів у межах CI/CD пайплайну в середньостроковій перспективі скорочує витрати на виправлення помилок на стадії релізу. Якщо вартість усунення вразливості на етапі експлуатації програмного продукту є у 10-15 разів вищою, ніж на етапі проектування, то впровадження методів ранньої ідентифікації ризиків генерує додатковий операційний ефект, який не відображається у прямих фінансових розрахунках, але суттєво впливає на рентабельність окремих проектів компанії.

Для остаточного підтвердження доцільності впровадження комплексної системи управління ризиками необхідно перейти від статичних показників уникнених збитків до динамічних індикаторів ефективності інвестицій. Ключовим метрикою в даному контексті виступає показник повернення інвестицій у безпеку (ROSI), який адаптує класичну формулу ROI під специфіку ризик-менеджменту [16]. Розрахунок базується на відношенні чистого ефекту від зниження ризиків (різниця між ALE до та після впровадження за вирахуванням щорічних витрат на підтримку) до обсягу початкових інвестицій. Враховуючи отримані раніше дані, де річна економія від запобігання інцидентам становить 1

205 тис. грн, а щорічні операційні витрати на систему складають 450 тис. грн, чистий річний вигода дорівнює 755 тис. грн.

При обсязі початкових капітальних вкладень у розмірі 1 750 тис. грн, термін окупності проекту складе приблизно 2,3 роки. Це є дуже позитивним показником для ІТ-галузі, де життєвий цикл програмних рішень зазвичай перевищує 3-5 років. Показник ROSI для першого повного року експлуатації системи (після етапу впровадження) розраховується як (1 205 000 - 450 000) / 1 750 000 * 100%, що становить 43%. Такий рівень рентабельності свідчить про те, що кожен вкладений у систему управління ризиками гривня приносить 43 копійки чистої економії понад витрати на її утримання, що значно перевищує середньоринкову вартість капіталу та альтернативні варіанти інвестування в пасивні методи захисту.

Таблиця 3.5

Динаміка фінансових показників ефективності проекту на трирічному горизонті

Показник ефективності	Рік 1 (Впровадження)	Рік 2 (Експлуатація)	Рік 3 (Оптимізація)
Капітальні витрати (CapEx), тис. грн	1 750	0	0
Операційні витрати (OpEx), тис. грн	450	450	450
Уникнені збитки (Економія), грн	602,5*	1 205	1 205
Чистий грошовий потік (NPV), тис. грн	-1 597,5	755	755
Кумулятивний ефект, тис. грн	-1 597,5	-842	-87**

Джерело: складено автором

* – *для 1-го року ефект розраховано за 6 місяців після завершення фази впровадження.*

** – *вихід на повну самоокупність та отримання чистого прибутку очікується в першому кварталі 4-го року.*

Окрім прямого фінансового ефекту, впровадження КСУР створює низку стратегічних переваг, які важко піддаються прямій кількісній оцінці, але мають вирішальне значення для капіталізації ТОВ «АЙСОФТ». По-перше, це суттєве

зміцнення репутаційного капіталу. Для ІТ-компанії, що працює на аутсорсинг або розробляє власні продукти, наявність сертифікованої та прозорої системи управління ризиками є критичним чинником при укладанні контрактів з великими західними партнерами. Це дозволяє претендувати на проекти з вищим чеком (high-ticket projects), де вимоги до безпеки та комплаєнсу є визначальними. По-друге, впровадження системи призводить до оптимізації страхових премій, якщо компанія використовує кібер-страхування, оскільки наявність дієвих засобів контролю знижує страхові ризики.

Додатковим фактором ефективності є підвищення інвестиційної привабливості підприємства. В очах потенційних інвесторів або кредиторів ТОВ «АЙСОФТ» перетворюється зі структури з високим рівнем невизначеності на керований бізнес із прогнозованими ризиками. Це знижує вартість залучення позикового капіталу та підвищує загальну оцінку вартості бізнесу у разі підготовки до M&A угод. Отже, запропоновані заходи з розробки та впровадження комплексної системи управління ризиками є не лише технічною необхідністю для захисту активів, а й потужним інструментом стратегічного розвитку, що забезпечує сталий розвиток компанії в умовах динамічного та агресивного цифрового середовища. Сукупний ефект від реалізації проекту підтверджує, що витрати на ризик-менеджмент є високорентабельною інвестицією, яка гарантує виживання та конкурентоспроможність ІТ-підприємства в довгостроковій перспективі.

Для остаточного прийняття рішення про доцільність впровадження комплексної системи управління ризиками в ТОВ «АЙСОФТ» необхідно провести розрахунок динамічних показників ефективності, які враховують часову вартість грошей та дозволяють порівняти даний проект із альтернативними варіантами використання капіталу. У сучасних умовах невизначеності на ІТ-ринку, просте зіставлення витрат і уникнених збитків є недостатнім, тому аналіз базується на методі дисконтування грошових потоків. Основним джерелом вхідних даних для розрахунку є чиста економія від зменшення ризиків, яка у попередніх розділах була визначена на рівні 1 205 000

грн на рік, за вирахуванням щорічних витрат на підтримку системи у розмірі 450 тис. грн. Розрахунковий період проекту прийнято за 3 роки, що відповідає середньому циклу морального застарівання програмного забезпечення та інструментів кібербезпеки. Ставка дисконтування встановлена на рівні 15%, що відображає середньозважену вартість капіталу для IT-сектору з урахуванням ризикової премії за інноваційність проекту.

Центральним показником ефективності є Чиста теперішня вартість (NPV), яка демонструє абсолютний приріст капіталу компанії в результаті реалізації проекту, приведений до поточного моменту часу [12]. Розрахунок NPV передбачає дисконтування чистих грошових потоків кожного року та віднімання від їхньої суми початкових інвестицій у розмірі 1 750 тис. грн. Враховуючи, що у перший рік система функціонує лише половину терміну в повному обсязі, грошовий потік першого року скориговано. Отримане позитивне значення NPV підтверджує, що проект не лише покриває витрати на своє впровадження та вартість капіталу, а й створює додаткову економічну додану вартість для ТОВ «АЙСОФТ». Паралельно розраховується індекс рентабельності інвестицій (PI), який показує відношення дисконтованих доходів до витрат; значення PI вище одиниці є прямим індикатором фінансової ефективності та стійкості запропонованої системи.

Результати розрахунків складено в таблиці 3.6.

Таблиця 3.6

Розрахунок показників фінансової ефективності впровадження системи (NPV, IRR, DPP)

Показник	Значення	Характеристика та висновок
Початкові інвестиції (I0), тис. грн	1 750	Капітальні витрати на ПЗ, ліцензії та аудит.
Чистий річний дохід (CF), тис. грн	755	Уникнені збитки мінус операційні витрати.
Ставка дисконтування (r)	15	Бар'єрна ставка з урахуванням ризиків.
Чиста теперішня вартість (NPV), тис. грн	284,35	Проект є прибутковим (NPV > 0).

Продовження табл. 3.6

Показник	Значення	Характеристика та висновок
Внутрішня норма доходності (IRR)	24,8	Вища за ставку дисконтування; проект стійкий.
Індекс рентабельності (PI)	1,16	На кожну вкладену гривню проект генерує 1.16 грн.
Простий термін окупності (PP)	2,32	Час повернення коштів без врахування дисконту.
Дисконтований термін окупності (DPP)	2,85	Термін повернення інвестицій з урахуванням часу.

Джерело: складено автором

Важливим індикатором є Внутрішня норма доходності (IRR), яка для даного проекту становить 24,8%. Цей показник демонструє граничний рівень вартості капіталу, при якому проект залишається беззбитковим. Оскільки IRR (24,8%) суттєво перевищує прийняту ставку дисконтування (15%), проект має значний «запас міцності» до можливого зростання вартості ресурсів або зниження ефективності інструментів захисту. Це робить систему управління ризиками привабливою не лише як засіб захисту, а й як ефективний інвестиційний інструмент. Дисконтований термін окупності (DPP) становить 2,85 роки, що вписується в межі трирічного горизонту планування і є прийнятним результатом для інфраструктурних IT-проектів, де основна вигода полягає в стабілізації операційної діяльності та запобіганні катастрофічним сценаріям.

Узагальнюючи результати фінансового аналізу, можна стверджувати, що впровадження комплексної системи управління ризиками в ТОВ «АЙСОФТ» є економічно обґрунтованим кроком. Високі значення NPV та IRR свідчать про те, що запропоновані заходи дозволяють трансформувати витрати на безпеку в стратегічний актив, який безпосередньо впливає на фінансову стійкість підприємства. Кількісні розрахунки підтверджують: автоматизація ризик-менеджменту, попри значні початкові витрати, забезпечує стабільний позитивний грошовий потік за рахунок радикального зниження частоти та

тяжкості наслідків від реалізації загроз. Таким чином, запропонована система є не просто технічним надбудовою, а фундаментом для довгострокового економічного зростання компанії в умовах сучасних кібервикликів.

Висновки за третім розділом

Узагальнюючи результати проведеного дослідження щодо розробки та впровадження комплексної системи управління ризиками в діяльність ТОВ «АЙСОФТ», можна констатувати, що в умовах сучасної цифрової економіки ризик-менеджмент перетворюється з допоміжної функції на стратегічний фундамент забезпечення життєздатності IT-підприємства. Спроектована система базується на глибокій інтеграції міжнародних стандартів безпеки у гнучкі процеси розробки програмного забезпечення, що дозволяє не лише оперативно реагувати на існуючі загрози, а й превентивно ідентифікувати потенційні вразливості на ранніх етапах життєвого циклу продуктів. Перехід до використання автоматизованих інструментів класу SIEM та GRC став ключовим технологічним рішенням, яке забезпечило трансформацію розрізнених технічних даних у зрозумілі бізнес-метрики, надаючи керівництву компанії об’єктивний інструментарій для прийняття управлінських рішень та точного визначення ризик-апетиту організації.

Запропонований триетапний план імплементації дозволив послідовно поєднати діагностику поточного стану, технологічне переоснащення та розвиток кадрового потенціалу, формуючи цілісний захисний контур навколо критичних активів підприємства. Важливим висновком розробки є те, що ефективність системи прямо залежить від синергії між технічними засобами контролю та організаційною культурою безпеки, де кожен співробітник усвідомлює свою роль у мінімізації впливу людського фактору. Впровадження методології DevSecOps у поєднанні з безперервним моніторингом подій дозволило ТОВ «АЙСОФТ» радикально скоротити середній час виявлення інцидентів та

мінімізувати ймовірність критичних збоїв, що безпосередньо впливає на рівень довіри з боку міжнародних партнерів та замовників.

Фінансово-економічна оцінка проєкту підтвердила високу доцільність інвестицій у запропоновані заходи, оскільки отримані показники чистої теперішньої вартості та внутрішньої норми доходності суттєво перевищують встановлені порогові значення для ІТ-галузі. Розрахунки продемонстрували, що превентивні витрати на підтримку комплексної системи управління ризиками є значно нижчими за потенційні збитки від реалізації кіберзагроз чи репутаційних втрат. Розроблена система не лише виконує функцію захисту, а й виступає каталізатором капіталізації компанії, підвищуючи її інвестиційну привабливість та забезпечуючи сталий розвиток у довгостроковій перспективі. Підсумком роботи є сформована модель адаптивного ризик-менеджменту, яка здатна гнучко масштабуватися разом із ростом бізнесу та ефективно протидіяти новим викликам глобального технологічного ринку.

ВИСНОВКИ

Проведене дослідження комплексно розв’язало проблему фрагментарного та переважно реактивного підходу до управління ризиками в діяльності українських ІТ-підприємств малого та середнього бізнесу, які в умовах прискореної цифрової трансформації стикаються з підвищеною вразливістю перед кіберзагрозами, технологічними збоями, регуляторними змінами та унікальними викликами, пов’язаними з інтеграцією штучного інтелекту та хмарних рішень. На конкретному прикладі ТОВ «АЙСОФТ» було продемонстровано, як обмежені внутрішні ресурси, відсутність системної інтеграції ризик-менеджменту в загальну стратегію розвитку та недостатня автоматизація процесів ідентифікації, оцінки й реагування на загрози призводять до зростання потенційних фінансових втрат, репутаційних ризиків та операційних перебоїв, що в підсумку підриває конкурентоспроможність компанії на ринку цифрових послуг. Такий стан речей є характерним для багатьох вітчизняних ІТ-організацій, де ризик-менеджмент часто сприймається як другорядна функція, а не як стратегічний елемент забезпечення стійкості бізнесу в динамічному середовищі.

Мета роботи була повністю досягнута шляхом послідовного виконання всіх завдань, сформульованих на початковому етапі. У теоретичній частині було розкрито сутність ризику в ІТ-сфері як комбінації ймовірності та наслідків, з акцентом на його еволюцію від простих ймовірнісних моделей до багатошарових фреймворків, що враховують технологічні, організаційні, людські та регуляторні аспекти. Детально досліджено методи ідентифікації та оцінки ризиків, включаючи якісні та кількісні підходи, які дозволяють формувати повний реєстр загроз і пріоритизувати їх за рівнем впливу на бізнес-процеси. Проаналізовано провідні моделі та інструменти управління ризиками, що демонструє можливості переходу до проактивного підходу з використанням автоматизованих систем і міжнародних стандартів, адаптованих до специфіки ІТ-галузі.

Практичний аналіз організаційно-економічної діяльності ТОВ «АЙСОФТ» виявив особливості компанії як типового представника малого IT-бізнесу, що спеціалізується на розробці веб- та мобільних рішень, наданні послуг хостингу та підтримці цифрової інфраструктури клієнтів. Було встановлено, що поточний стан ризиків у діяльності підприємства характеризується переважанням кіберзагроз, помилок у програмному забезпеченні, людських факторів та регуляторних викликів, а існуюча система управління ризиками є недостатньо структурованою, фрагментарною та позбавленою комплексного моніторингу, що знижує її ефективність і не дозволяє вчасно реагувати на потенційні інциденти. Оцінка конкурентоспроможності та ефективності наявних механізмів захисту підтвердила необхідність суттєвого вдосконалення, оскільки без системних змін компанія ризикує втратити ринкові позиції в умовах посилення конкуренції та зростання вимог до безпеки даних.

На основі отриманих результатів у заключній частині роботи розроблено конкретні пропозиції щодо вдосконалення процесів управління ризиками саме для ТОВ «АЙСОФТ», що дозволяє перейти від розрізненого реагування до цілісної, проактивної системи. Зокрема, рекомендовано впровадження комплексної системи управління ризиками, яка інтегрує сучасні технологічні інструменти для безперервного моніторингу подій безпеки в реальному часі та централізованого контролю процесів. Особливе місце в цих пропозиціях посідає впровадження SIEM-систем, що забезпечують автоматизований збір, аналіз і кореляцію даних про події в IT-інфраструктурі, дозволяючи оперативно виявляти аномалії та запобігати інцидентам до їхнього розвитку. Доповненням стає використання GRC-платформ, які поєднують управління ризиками, дотримання нормативних вимог та внутрішній контроль в єдиному цифровому середовищі, створюючи єдиний інформаційний простір для прийняття стратегічних рішень керівництвом. Ці заходи доповнено рекомендаціями щодо мінімізації ризиків через посилення політик доступу, регулярне навчання персоналу, удосконалення процесів тестування програмного забезпечення та впровадження додаткових технічних засобів захисту інформаційних активів.

Економічне обґрунтування запропонованих заходів, проведене з урахуванням специфіки діяльності ТОВ «АЙСОФТ», демонструє їхню високою доцільність: очікувані вигоди від суттєвого зниження ймовірності інцидентів, мінімізації потенційних втрат від кіберзагроз і операційних збоїв, а також підвищення загальної ефективності бізнес-процесів значно перевищують необхідні інвестиції в технологічні рішення, навчання та організаційні зміни. Для підприємства це означає не лише підвищення рівня захисту інформаційних активів і забезпечення відповідності регуляторним вимогам, але й посилення конкурентних позицій на ринку, створення надійного фундаменту для стійкого розвитку та можливості масштабування діяльності в умовах цифрової економіки. У загальнонауковому плані результати дослідження сприяють розвитку теорії та практики управління ризиками в ІТ-сфері в Україні, пропонуючи адаптовані рішення для підприємств з обмеженими ресурсами та сприяючи формуванню культури ризикоорієнтованого мислення як невід’ємної складової стратегічного менеджменту.

Отримані висновки підтверджують, що ефективне управління ризиками має стати стратегічним пріоритетом для кожного ІТ-підприємства, перетворюючи потенційні загрози на можливості для інновацій і зростання. Запропоновані заходи, апробовані на прикладі ТОВ «АЙСОФТ», можуть бути адаптовані іншими компаніями аналогічного профілю, забезпечуючи підвищення загальної стійкості галузі в умовах швидких технологічних трансформацій і посилення глобальних викликів. Таким чином, робота не лише розв’язала поставлену проблему, але й створила практичну базу для подальшого вдосконалення ризик-менеджменту в національному ІТ-секторі.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Горбаченко С. А. Штучний інтелект як інструмент сталого розвитку IT-бізнесу в Україні / Горбаченко С. А., Куклінова Т. В. // ГЕВ. Тернопіль : *ТНТУ*. 2025. Том 93. № 2. С. 66-72. DOI: https://doi.org/10.33108/galicianvisnyk_tntu2025.02.

2. Горбаченко С. А., Клєвцєвич Н. А. Роль кібербезпеки у впровадженні циркулярних економічних моделей: аналіз ризиків та можливостей. Вісник *Херсонського національного технічного університету*. 2024. № 1(88). С. 342-348. DOI: https://doi.org/10.35546/kntu2078-4481.2024.1.48.

3. Горбаченко С. А., Чепурна О. Є., Черевко Є. В. Математичне моделювання проєктних рішень на основі стохастичних процесів для аналізу ризиків. *Успіхи і досягнення у науці*. 2025. № 7 (17). С. 314-332. DOI: https://doi.org/10.52058/3041-1254-2025-7(17).

4. Горбаченко С.А., Саврацький О.О. Transformation of the innovative component of management processes in the context of digitalization. *Приазовський економічний вісник.* 2025. № 3 (43). С. 62-68. DOI: https://doi.org/10.32782/2522-4263/2025-3-11.

5. Захарова Я., Партика А. Еволюція управління кіберризиками крізь призму NIST CYBERSECURITY FRAMEWORK. *Кібербезпека: освіта, наука, техніка*. 2025. № 2(30). С. 333–347. DOI: https://doi.org/10.28925/2663-4023.2025.30.980

6. Здирко Н. Г., Мулик Т. О., Іщенко Я. П., Дриманова Л. М. Трансформація внутрішнього контролю підприємств у контексті цифровізації господарських процесів. *Економіка, фінанси, менеджмент: актуальні питання науки і практики*. 2025. № 2 (72). С. 23-46. DOI: http://dx.doi.org/10.37128/2411-4413-2025-2-2.

7. Копчак Ю., Лобунець Т., Луковський Р. SWOT-аналіз як важливий інструмент у розробці стратегії бізнесу. *Економіка та суспільство.* 2024. № 61. DOI: https://doi.org/10.32782/2524-0072/2024-61-146.

8. Котельникова Ю. М. Управління витратами в умовах цифрової економіки: сучасні моделі та інструменти оптимізації. *Економіка та суспільство.* 2025. № 73. DOI: https://doi.org/10.32782/2524-0072/2025-73-44.

9. Куклінова Т., Чепурна О., Мельник Є. Економіко-математичне моделювання: синергія аналітики, менеджменту та штучного інтелекту. *Сталий розвиток економіки*. 2025. №4 (55). С. 231-236. DOI: https://doi.org/10.32782/2308-1988/2025-55-31.

10. Кулаковська І. Ризики використання хмарних технологій. *Herald of Khmelnytskyi National University. Technical Sciences*. 2024. № 341(5). С. 45-52. https://doi.org/10.31891/2307-5732-2024-341-5-6.

11. Марценюк Є. В., Чорній В. В., Гарасимчук О. І. Автоматизоване управління ризиками витоку секретної інформації у програмному коді. *Телекомунікаційні та інформаційні технології*. 2025. № 3. С. 45-63. DOI: 10.31673/2412-4338.2025.038705.

12. Мисяк І. М., Діжак В. В., Степась М. В. Оцінка ефективності реальних інвестиційних проектів. *Scientific Notes of Lviv University of Business and Law.* 2023. № 37. С. 277-283. DOI: http://dx.doi.org/10.5281/zenodo.8074327.

13. ТОВ «АЙСОФТ». Opendata.bot. Офіційний веб-сайт. URL: https://opendatabot.ua/c/38266721 (дата звернення: 13.03.2026).

14. ТОВ «АЙСОФТ». VKURSI. Офіційний веб-сайт. URL: https://vkursi.pro/card/tov-aysoft-38266721 (дата звернення: 18.03.2026).

15. ТОВ «АЙСОФТ». You.Control. Офіційний веб-сайт. URL: https://youcontrol.com.ua/catalog/company_details/38266721/ (дата звернення: 13.03.2026).

16. Фукс М. А., Добринін І. С., Пшеничних С. В., Снігуров А. В., Чакрян В. Х. Методика побудови системи управління інформаційною безпекою на основі методів аналізу ієрархій, мережевого аналізу та теорії ігор в умовах обмежених ресурсів. *Вісник Херсонського національного технічного університету.* 2025. № 2(3 (94)). С. 484-496. DOI: https://doi.org/10.35546/kntu2078-4481.2025.3.2.62.

17. Хомка В. М. та ін. Інструменти ідентифікації фінансових ризиків на основі даних управлінського обліку. *Scientific Notes of Lviv University of Business and Law*. 2024. №40. С. 680-686. DOI: https://doi.org/10.5281/zenodo.10441307.

18. Черніков Д., Гришко С. Сучасні тенденції та стратегічні ризики впровадження технологій індустрії 4.0 та індустрії 5.0. *Економіка та суспільство.* 2023. № 54. DOI: https://doi.org/10.32782/2524-0072/2023-54-68.

19. A guide towards collaborative AI frameworks. ITU. URL: https://digitalregulation.org/a-guide-towards-collaborative-ai-frameworks/ (дата звернення: 12.03.2026).

20. AI N. Artificial intelligence risk management framework: Generative artificial intelligence profile. NIST Trustworthy and Responsible AI Gaithersburg, MD, USA. NIST AI 600-1. 2024. 63 p. DOI: https://doi.org/10.6028/NIST.AI.600-1

21. Ali T., Al-Khalidi M., Al-Zaidi R. Information Security Risk Assessment Methods in Cloud Computing: Comprehensive Review. *Journal of Computer Information Systems.* 2026. № 66(1). PP. 123–150. DOI: https://doi.org/10.1080/08874417.2024.2329985.

22. Barraza de la Paz J. V., Rodríguez-Picón L. A., Morales-Rocha V., Torres-Argüelles S. V. A Systematic Review of Risk Management Methodologies for Complex Organizations in Industry 4.0 and 5.0. *Systems.* 2023. № 11(5). PP. 218-237. DOI: https://doi.org/10.3390/systems11050218.

23. Barraza de la Paz J. V., Rodríguez-Picón L. A., Morales-Rocha V., Torres-Argüelles S. V. A systematic review of risk management methodologies for complex organizations in industry 4.0 and 5.0. *Systems*. 2023. № 11(5). DOI: https://doi.org/10.3390/systems11050218.

24. Dinu A. M. Tools and techniques for risk identification and assessment. Knowledge Horizons. *Economics*. 2015. № 7(2). PP. 139-141.

25. Fuchs D., Kuys B., Eisenbart B., Gericke K. A systematic literature review on emerging technology risks in Industry 4.0/5.0: identification, clustering and developing mitigation strategies. *Proceedings of the Design Society.* 2025. № 5. PP. 299–308. DOI: http://dx.doi.org/ 10.1017/pds.2025.10044.

26. Information security, cybersecurity and privacy protection – Privacy information management systems – Requirements and guidance. ISO/IEC 27701:2025. ISO. URL: https://www.iso.org/standard/27701 (дата звернення: 18.03.2026).

27. ISO 31000:2018. Risk management – Guidelines. ISO. URL: https://www.iso.org/ru/standard/65694.html (дата звернення: 18.03.2026).

28. iSoft Ukraine. IT-rating. URL: https://it-rating.ua/starsoft-ukraine

29. Kramarz K. The evolution of the concept of risk management in IT+ organizations. *Procedia Computer Science*. 2023. № 225. PP. 4843-4849. DOI: http://dx.doi.org/10.1016/j.procs.2023.10.484.

30. Lee M. C. Information security risk analysis methods and research trends: AHP and fuzzy comprehensive method. *International Journal of Computer Science & Information Technology*. 2014. № 6(1). DOI: http://dx.doi.org/10.5121/ijcsit.2014.6103.

31. Metin B., et al. IT Risk Management: Towards a System for Enhancing Objectivity in Asset Valuation That Engenders a Security Culture. *Information*. 2024. № 15(1). PP. 55-83. DOI: https://doi.org/10.3390/info15010055.

32. Mohsienuddin S., Sabri M. Risk management in information technology. *SSRN Electronic Journal*. 2020. №7. PP. 373-381.

33. NIST SP 800-30 Rev. 1. Guide for Conducting Risk Assessments. NIST. 2012. 95 p. DOI: https://doi.org/10.6028/NIST.SP.800-30r1 (дата звернення: 18.03.2026).

34. Orellano M., Gourc D. What typology of risks and methods for risk management in innovation projects?: A systematic literature review. *International Journal of Innovation Studies.* 2025. № 9(1). PP. 1-15. DOI: https://doi.org/10.1016/j.ijis.2024.10.001.

35. Podziņš O., Romānovs A. IT Risk Identification and Assessment Methodology. In Environment. Technology. Resources. *The International Scientific and Practical Conference.* 2017. № 2. PP. 124-127. DOI: https://doi.org/10.17770/etr2017vol2.2539

36. Rodríguez-Espíndola O., Chowdhury S., Dey P. K., Albores P., Emrouznejad A. Analysis of the adoption of emergent technologies for risk management in the era of

digital manufacturing. *Technological Forecasting and Social Change*. 2022. № 178. DOI: https://doi.org/10.1016/j.techfore.2022.121562.

37. Samimi A. Risk management in information technology. *Progress in Chemical and Biochemical Research.* 2020. № 3(2). PP. 130-134. DOI: http://dx.doi.org/ 10.33945/SAMI/PCBR.2020.2.6.

38. Stoneburner G., Goguen A., Feringa A. Risk management guide for information technology systems. National Institute of Standards and Technology. 2002. № 800(30). 55 p.

39. Tekinbaş C., Alpaslan F. N., Güçlü A. N.Risk Management Based on Machine Learning ASME. *Open J. Engineering ASME*. 2025. № 4(041022). P. 1-11. DOI: https://doi.org/10.1115/1.4069023.

40. Xu Y., Reniers G., Yang M. A Multidisciplinary Review into the Evolution of Risk Concepts and Their Assessment Methods. Processes. 2024. № 12(11). PP. 2449-24. DOI: https://doi.org/10.3390/pr12112449.