НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»

ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«УПРАВЛІННЯ РИЗИКАМИ ІТ-ПІДПРИЄМСТВА»

Виконала: здобувачка 4 курсу
Рівень бакалавр
Галузь знань 07 “Управління та адміністрування”,
спеціальність 073 «Менеджмент»
Краснюк Ірина Олександрівна

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

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

Одеса – 2025

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
Факультет **кібербезпеки та інформаційних технологій**
Кафедра **кібербезпеки**
Галузь знань: **07 Управління та адміністрування**
Спеціальність: **073 Менеджмент**
Назва освітньої програми: **ІТ-менеджмент та маркетинг**

ЗАТВЕРДЖУЮ
Завідувач кафедри кібербезпеки
професор С.А. Горбаченко
_____ «____ »_____ 20__ року

З А В Д А Н Н Я
на кваліфікаційну (бакалаврську) роботу
здобувачу Краснюк Ірині Олександрівні

1. Тема роботи: «Управління ризиками ІТ-підприємства»
Керівник роботи: професор, д.е.н. Горбаченко Станіслав Анатолійович
затверджені наказом НУ ОЮА від «18» березня 2025 року № 548-6
2. Строк подання здобувачем роботи «27» травня 2025 рік
3. Дата видачі завдання «16» вересня 2024 рік

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів бакалаврської роботи	Строк виконання етапів роботи	Примітка
1	Аналіз предметної області та пошук науково-технічної інформації за темою роботи	Вересень-жовтень 2024	
2	Узгодження теми з науковим керівником, формулювання мети завдань дослідження	Листопад 2024	
3	Робота над першим розділом	Листопад-грудень 2024	
4	Робота над другим розділом	Січень-лютий 2025	
5	Робота над третім розділом	Лютий-березень 2025	
6	Уточнення подальшого обсягу роботи та його коригування	Березень-травень 2025	
7	Оформлення звітної частини	Травень 2025	
8	Захист роботи	13.06.2025	

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, галузю знань 07 "Управління та адміністрування", містить 1 рисунки, 13 таблиць, 20 літературних джерел за переліком посилань. Робота виконана на 47 сторінках загального тексту і 40 сторінках основного тексту.

Метою роботи є розробка теоретичних основ і практичних рекомендацій щодо вдосконалення системи управління ризиками ІТ-підприємств на прикладі ТОВ «К2 СИСТЕМИ» з метою підвищення їхньої операційної стійкості та конкурентоспроможності. Розроблено класифікацію ризиків ІТ-сфери, проаналізовано методи їх оцінки, зокрема метод Делфі, та запропоновано інноваційні інструменти (ШІ, прогнозний аналіз, блокчейн) і ІТ-технології (Nessus, Tableau, Azure Sentinel, Jira) для мінімізації кіберзагроз, фінансових і операційних ризиків. Проведено економічний аналіз, який підтверджує ефективність заходів: економія 1079,2 тис. грн при витратах 800 тис. грн, окупність 8,9 місяців, ROI 34,9%.

Результати роботи можуть бути використані менеджерами ІТ-підприємств для оптимізації ризик-менеджменту, зниження втрат і підвищення стійкості бізнес-процесів. Можливими напрямками подальших досліджень є інтеграція штучного інтелекту в прогнозування ризиків і адаптація запропонованих рішень до міжнародних ринків.

МЕНЕДЖМЕНТ, ІТ-ПІДПРИЄМСТВО, РИЗИК-МЕНЕДЖМЕНТ, КІБЕРБЕЗПЕКА, ЕКОНОМІЧНА ЕФЕКТИВНІСТЬ.

ABSTRACT

The qualification work on the topic “Risk Management of an IT Enterprise” for obtaining the first (bachelor’s) level of higher education in the specialty 073 Management, field of knowledge 07 "Management and Administration," contains 1 figures, 13 tables, and 20 literary sources listed in the references. The work spans 47 pages of total text and 40 pages of main text.

The purpose of the work is to develop theoretical foundations and practical recommendations for improving the risk management system of IT enterprises, using the example of LLC “K2 Systems,” to enhance their operational resilience and competitiveness. A classification of IT sector risks has been developed, methods of their assessment, including the Delphi method, have been analyzed, and innovative tools (AI, predictive analytics, blockchain) and IT technologies (Nessus, Tableau, Azure Sentinel, Jira) have been proposed to minimize cybersecurity, financial, and operational risks. An economic analysis was conducted, confirming the effectiveness of the measures: savings of 1,079,200 UAH with costs of 800,000 UAH, a payback period of 8.9 months, and an ROI of 34.9%.

The results of the work can be utilized by IT enterprise managers to optimize risk management, reduce losses, and enhance the resilience of business processes. Potential directions for further research include the integration of artificial intelligence into risk forecasting and the adaptation of the proposed solutions to international markets.

MANAGEMENT, IT ENTERPRISE, RISK MANAGEMENT, CYBERSECURITY, ECONOMIC EFFICIENCY.

ЗМІСТ

ВСТУП

Актуальність теми. Сучасний етап розвитку економіки характеризується стрімкою цифровізацією, де інформаційні технології відіграють ключову роль у забезпеченні конкурентоспроможності підприємств. IT-підприємства, які розробляють програмне забезпечення, надають цифрові послуги чи підтримують інфраструктуру, стикаються з унікальним спектром ризиків, що охоплюють технологічні, організаційні, фінансові та зовнішні аспекти. Управління ризиками в таких організаціях є критично важливим завданням, адже від його ефективності залежить не лише стабільність діяльності, а й здатність адаптуватися до динамічних ринкових умов та кіберзагроз.

Актуальність теми дослідження зумовлена зростаючою складністю IT-екосистем, підвищенням частоти та масштабів кібератак, а також посиленням регуляторних вимог до безпеки даних і безперервності бізнес-процесів. За даними міжнародних досліджень, таких як звіти Gartner та Deloitte, до 60% IT-підприємств зазнають значних фінансових втрат через неадекватне управління ризиками, пов’язаними з кібербезпекою, проєктними невдачами чи технологічними збоями. Водночас недостатня увага до ризиків, пов’язаних із людським фактором, інноваційними технологіями (наприклад, штучним інтелектом чи хмарними обчисленнями) та геополітичними викликами, ускладнює стратегічне планування та розвиток IT-підприємств.

Проблематика управління ризиками IT-підприємств полягає у необхідності балансування між інноваційною активністю, що передбачає прийняття певних ризиків, та забезпеченням стабільності й безпеки бізнес-процесів. Традиційні підходи до ризик-менеджменту, розроблені для інших галузей, часто виявляються недостатньо адаптованими до специфіки IT-сектору, що характеризується високою швидкістю змін, складними технологічними взаємозв’язками та значною залежністю від зовнішніх постачальників. Таким чином, виникає потреба у розробці спеціалізованих методологій, які враховують унікальні виклики IT-підприємств.

Мета дослідження − розробити теоретичні основи та практичні рекомендації щодо вдосконалення системи управління ризиками ІТ-підприємств з метою підвищення їхньої операційної стійкості, ефективності та здатності адаптуватися до динамічних технологічних і ринкових умов. Щоб досягти мети, потрібно виконати наступні завдання:

– визначити поняття ризиків в ІТ-сфері та розробити їх класифікацію за основними видами і характеристиками.

– проаналізувати основні засоби управління ризиками ІТ-проектів та оцінити їх ефективність

– охарактеризувати діяльність ТОВ «К2 СИСТЕМИ» та дослідити особливості його організаційної структури.

– виявити та оцінити основні ризики, притаманні діяльності ТОВ «К2 СИСТЕМИ», із застосуванням діагностичних методів.

– запропонувати інноваційні інструменти управління ризиками та обґрунтувати їх інтеграцію в діяльність підприємства.

– розробити рекомендації щодо впровадження ІТ-технологій для оцінки та моніторингу ризиків ТОВ «К2 СИСТЕМИ».

– оцінити очікувані результати та економічну ефективність запропонованих заходів з удосконалення управління ризиками.

Об’єкт дослідження − процеси управління ризиками в діяльності ІТ-підприємств, що охоплюють розробку, впровадження та підтримку інформаційних технологій і цифрових рішень.

Предмет дослідження − методи, інструменти та організаційні підходи до ідентифікації, оцінки, моніторингу та мінімізації ризиків, специфічних для ІТ-підприємств, у контексті сучасних технологічних, економічних і регуляторних викликів.

Практичне значення отриманих результатів. Результати дослідження мають практичну цінність для ІТ-підприємств, оскільки пропонують комплексний підхід до вдосконалення системи управління ризиками. Розроблені рекомендації та інструментарій дозволяють ефективно ідентифікувати,

оцінювати та мінімізувати ризики, пов’язані з розробкою програмного забезпечення, кібербезпекою, проєктною діяльністю та зовнішніми факторами. Впровадження запропонованих методів сприятиме зниженню фінансових і репутаційних втрат, підвищенню операційної стійкості та конкурентоспроможності ІТ-підприємств. Отримані результати можуть бути використані менеджерами та фахівцями з ризик-менеджменту для оптимізації бізнес-процесів, а також як основа для розробки корпоративних політик і стратегій управління ризиками. Крім того, рекомендації можуть бути адаптовані для використання в освітніх програмах з підготовки спеціалістів у сфері ІТ-менеджменту та кібербезпеки.

1 ТЕОРЕТИЧНІ ОСНОВИ УПРАВЛІННЯ РИЗИКАМИ ІТ-ПІДПРИЄМСТВ

1.1 Поняття та класифікація ризиків в ІТ-сфері

У сучасному світі інформаційні технології є ключовим елементом економічного, соціального та технологічного розвитку. ІТ-підприємства, які розробляють програмне забезпечення, надають хмарні послуги, займаються кібербезпекою чи впроваджують інноваційні рішення, стикаються з численними викликами, пов’язаними з невизначеністю та потенційними загрозами. Ці виклики формують поняття ризиків, які є невід’ємною частиною діяльності будь-якої ІТ-організації. Управління ризиками в ІТ-сфері є критично важливим для забезпечення сталого розвитку, конкурентоспроможності та захисту активів підприємства. У цьому розділі розглядаються поняття ризиків в ІТ-сфері, їх класифікація, а також ключові аспекти, які впливають на їх ідентифікацію та управління. Для ґрунтовного аналізу використано наукові джерела, які дозволяють структурувати знання та забезпечити достовірність викладеного матеріалу.

Ризик у загальному розумінні визначається як можливість настання події, яка може мати негативні наслідки для досягнення цілей організації. У контексті ІТ-сфери ризик можна охарактеризувати як імовірність виникнення подій, які негативно впливають на функціонування інформаційних систем, бізнес-процесів, репутацію чи фінансові показники підприємства. Згідно з ISO/IEC 31000:2018, ризик визначається як "ефект невизначеності на цілі", що включає як негативні, так і потенційно позитивні наслідки [1]. У ІТ-сфері ризики мають специфічний характер через швидкі темпи технологічних змін, складність інформаційних систем і залежність від людського фактора.

Ключовими особливостями ризиків в ІТ є їх багатогранність і динамічність. Наприклад, ризик може стосуватися кібератаки, яка загрожує конфіденційності даних, або ж помилки в коді, що призводить до збою системи. Водночас ІТ-ризики не обмежуються технічними аспектами – вони включають організаційні, фінансові, правові та репутаційні компоненти. Як зазначає

Керзнер, у проектному менеджменті ІТ-ризик часто пов’язаний з невідповідністю між очікуваннями стейкхолдерів і фактичними результатами, що вимагає комплексного підходу до їх ідентифікації та управління [2].

Ризики в ІТ-сфері мають низку характеристик, які відрізняють їх від ризиків в інших галузях:

1. Висока швидкість змін. Технології розвиваються стрімко, що створює нові загрози (наприклад, уразливості в нових програмних продуктах) і ускладнює прогнозування.

2. Складність систем. ІТ-системи часто є складними, взаємопов’язаними структурами, де одна помилка може мати каскадний ефект.

3. Глобальний масштаб. Кіберзагрози не обмежуються географічними кордонами, що робить ІТ-підприємства вразливими до атак із будь-якої точки світу.

4. Залежність від людського фактора. Помилки розробників, недостатня кваліфікація персоналу чи соціальна інженерія є значними джерелами ризиків.

5. Високі фінансові та репутаційні наслідки. Порушення безпеки даних або збій у роботі сервісів може призвести до значних втрат, включаючи штрафи, втрату клієнтів і погіршення іміджу [3].

Для ефективного управління ризиками необхідна їх систематизація. Класифікація ризиків в ІТ-сфері є важливим інструментом для систематизації потенційних загроз, що дозволяє ІТ-підприємствам ефективно їх ідентифікувати, оцінювати та розробляти стратегії управління. Ризики в цій галузі вирізняються своєю різноманітністю та складністю, що зумовлено швидкими технологічними змінами, глобальним характером діяльності та залежністю від людського фактора.

Для їх аналізу застосовуються різні критерії, такі як джерело походження, характер впливу чи сфера виникнення, що дає змогу структурувати загрози та адаптувати підходи до їх мінімізації.

Загальну класифікацію ризиків складено в таблиці 1.1.

Таблиця 1.1 − Класифікація ризиків

Категорія ризику	Приклади	Потенційний вплив
Технічні	Кібератаки, збої обладнання, баги	Простої, втрата даних
Організаційні	Погане планування, плинність кадрів	Зриви дедлайнів, неефективність
Фінансові	Перевищення бюджету, втрата доходів	Зниження прибутковості
Правові	Порушення GDPR, судові позови	Штрафи, репутаційні втрати
Репутаційні	Витік даних, негативні відгуки	Втрата клієнтів, зниження довіри
Зовнішні	Природні катастрофи, санкції	Обмеження діяльності

Джерело: складено за даними [3-5]

Однією з ключових категорій є технічні ризики, пов’язані з функціонуванням апаратного забезпечення, програмного забезпечення та інформаційних систем. Наприклад, збої серверів чи мережевих пристроїв можуть спричинити простої у роботі, тоді як помилки в коді або несумісність програм здатні порушити функціональність додатків. Особливо значущими є кіберзагрози, такі як хакерські атаки, фішинг чи програми-вимагачі, які загрожують конфіденційності, цілісності та доступності даних. Уразливості безпеки, спричинені застарілим програмним забезпеченням або слабкими механізмами захисту, також становлять серйозну небезпеку, оскільки можуть стати точкою входу для зловмисників.

Організаційні ризики виникають через недоліки у внутрішніх процесах і управлінні. Неправильне планування проєктів, наприклад, може призвести до перевитрат ресурсів або зриву строків виконання. Низька кваліфікація персоналу чи висока плинність кадрів ускладнюють досягнення цілей, тоді як недостатня координація між командами здатна викликати конфлікти чи дублювання зусиль. Такі проблеми часто посилюються в умовах швидкозмінного IT-середовища, де ефективна комунікація та чітке розподілення обов’язків є критично важливими.

Фінансові ризики стосуються економічної сторони діяльності IT-підприємств. Перевищення бюджету через непередбачені витрати на розробку

чи інфраструктуру може підірвати стабільність компанії. Втрата доходів, спричинена збоями в роботі сервісів або відтоком клієнтів після інцидентів безпеки, також становить серйозну загрозу. Для компаній, що працюють на міжнародних ринках, додатковим фактором є коливання валютних курсів, які впливають на прибутковість і конкурентоспроможність [6].

Правові та регуляторні ризики набувають дедалі більшого значення в умовах посилення вимог до захисту даних і дотримання стандартів. Недотримання міжнародних норм, таких як Загальний регламент захисту даних або стандарти HIPAA, може призвести до значних штрафів і судових позовів. Питання інтелектуальної власності, зокрема неправомірне використання патентів чи ліцензій, також створюють загрозу для IT-підприємств. Крім того, невідповідність умов контрактів із клієнтами чи постачальниками здатна спричинити фінансові та репутаційні втрати [7].

Репутаційні ризики виникають, коли події підривають довіру до компанії. Витік конфіденційної інформації, наприклад, може не лише завдати прямих збитків, але й відлякати клієнтів і партнерів. Негативні відгуки в медіа чи соціальних мережах, спричинені невдалим продуктом або некоректною реакцією на кризу, посилюють ці наслідки. У цифрову епоху, коли інформація поширюється миттєво, репутаційні втрати можуть мати довгостроковий вплив на позицію компанії на ринку.

Зовнішні ризики охоплюють фактори, які перебувають поза контролем підприємства. Природні катастрофи, такі як землетруси чи повені, здатні пошкодити критичну інфраструктуру, наприклад дата-центри. Геополітичні фактори, зокрема санкції чи політична нестабільність, можуть обмежити доступ до ринків або технологій. Конкурентний тиск також відіграє значну роль, оскільки поява нових гравців чи інноваційних рішень змушує компанії постійно адаптуватися, щоб зберегти свою частку ринку.:

Для ефективної класифікації та управління ризиками необхідно їх ідентифікувати. У науковій літературі пропонуються такі методи:

- Аналіз загроз. Визначення потенційних джерел небезпеки (наприклад, хакерські атаки чи людські помилки).

- Оцінка вразливостей. Виявлення слабких місць у системах чи процесах.

- Історичний аналіз. Вивчення попередніх інцидентів для прогнозування майбутніх ризиків.

- Експертні оцінки. Залучення спеціалістів для оцінки складних чи неочевидних загроз.

Ризики в ІТ-сфері є багатогранними та охоплюють технічні, організаційні, фінансові, правові, репутаційні та зовнішні аспекти. Їх класифікація дозволяє систематизувати знання про потенційні загрози, що є основою для розробки стратегій управління. У сучасних умовах, коли ІТ-підприємства діють у динамічному та конкурентному середовищі, розуміння природи ризиків і їх впливу є ключовим для забезпечення стійкості та успіху. Подальші дослідження в рамках дисертації будуть зосереджені на методах оцінки та мінімізації цих ризиків, а також на розробці практичних рекомендацій для ІТ-підприємств.

1.2 Засоби управління ризиками ІТ-проектів

Управління ризиками в ІТ-проектах є однією з ключових складових успішної реалізації проектів, оскільки ІТ-сфера характеризується високим рівнем невизначеності, швидкими технологічними змінами та складними взаємозв’язками між учасниками. Ефективне управління ризиками дозволяє не лише мінімізувати негативний вплив потенційних загроз, але й використовувати можливості, що виникають у процесі реалізації проекту. Засоби управління ризиками включають методи, інструменти та процеси, спрямовані на ідентифікацію, аналіз, оцінку, реагування та моніторинг ризиків.

Управління ризиками в ІТ-проектах базується на структурованому підході, який систематизовано описано в міжнародних стандартах, таких як PMBOK. Згідно з PMBOK, процес управління ризиками включає планування, ідентифікацію, аналіз (якісний і кількісний), розробку заходів реагування та

контроль ризиків [4]. Цей цикл дозволяє охопити всі аспекти ризиків, від їх виявлення до мінімізації впливу. Водночас ІТ-проекти мають свої особливості, такі як швидка зміна вимог, залежність від технологій, складність інтеграції систем і високий рівень кіберзагроз, що вимагає адаптації стандартних методів до специфіки галузі.

Одним із перших етапів управління ризиками є їх ідентифікація, яка передбачає виявлення всіх можливих подій, що можуть вплинути на проект. Для цього застосовуються різноманітні методи, зокрема мозковий штурм, аналіз історичних даних, інтерв'ю з експертами та використання чек-листів. Мозковий штурм, як зазначає Хілсон, є ефективним інструментом для залучення різних членів команди та виявлення ризиків, які можуть бути пропущені при формальному аналізі [8]. Наприклад, у проекті розробки програмного забезпечення команда може виявити ризики, пов'язані з несумісністю компонентів, зміною вимог замовника або недостатньою кваліфікацією розробників. Чек-листи, створені на основі досвіду попередніх проектів, дозволяють систематизувати типові ризики, такі як затримки в постачанні обладнання чи помилки в коді. Інтерв'ю з експертами особливо корисні в проектах із високим рівнем технологічної новизни, де стандартні підходи можуть бути недостатніми.

Після ідентифікації ризиків переходять до їх аналізу та оцінки. Якісний аналіз ризиків передбачає визначення пріоритетів на основі ймовірності настання та потенційного впливу. Для цього часто використовується матриця ймовірності та впливу, яка дозволяє класифікувати ризики за рівнем критичності. Наприклад, ризик кібератаки може мати високу ймовірність і значний вплив, що робить його критичним для проекту.

Таблиця 1.2 демонструє типову матрицю ймовірності та впливу, яка допомагає візуалізувати пріоритети.

Кількісний аналіз ризиків використовується для детальнішого оцінювання, особливо в проектах із високими фінансовими або часовими обмеженнями. До

таких методів належать аналіз чутливості, моделювання Монте-Карло та аналіз дерева рішень.

Таблиця 1.2 − Матриця ймовірності та впливу ризиків

Ймовірність \ Вплив	Низький	Середній	Високий
Висока	Середній	Високий	Критичний
Середня	Низький	Середній	Високий
Низька	Низький	Низький	Середній

Джерело: складено за даними [4]

Моделювання Монте-Карло, як зазначають Чепмен та Вард, дозволяє оцінити вплив ризиків на терміни та бюджет проекту шляхом створення ймовірнісних сценаріїв [9]. Наприклад, у проекті впровадження ERP-системи моделювання може показати, що ймовірність перевищення бюджету на 20% становить 30%, що дає змогу заздалегідь спланувати резервні кошти. Рисунок 1 демонструє приклад результатів моделювання Монте-Карло для оцінки термінів виконання проекту.

Наступним етапом є розробка стратегій реагування на ризики, які можуть включати уникнення, пом’якшення, передачу або прийняття. Уникнення передбачає зміну плану проекту для усунення ризику, наприклад, вибір більш стабільної технологічної платформи. Пом’якшення спрямоване на зменшення ймовірності або впливу, наприклад, шляхом додаткового тестування програмного забезпечення для зниження ймовірності помилок. Передача ризику часто використовується в IT-проектах через аутсорсинг або страхування, наприклад, передача відповідальності за підтримку серверів хмарному провайдеру. Прийняття застосовується до ризиків із низьким пріоритетом, коли витрати на їх управління перевищують потенційні збитки. Дослідження Кендріка показують, що в IT-проектах найпоширенішою стратегією є пом’якшення, оскільки повне уникнення ризиків часто неможливе через складність і невизначеність [10].

Моніторинг і контроль ризиків є завершальним етапом, який передбачає відстеження стану ризиків і ефективності заходів реагування. Для цього використовується реєстр ризиків − документ, що містить детальну інформацію про кожен ризик, його статус, відповідальних осіб і заплановані дії. Таблиця 1.3 ілюструє приклад фрагменту реєстру ризиків для IT-проекту.

Таблиця 1.3 − Фрагмент реєстру ризиків

ID	Ризик	Ймовірність	Вплив	Стратегія реагування	Відповідальний
R1	Зміна вимог замовника	Висока	Високий	Пом’якшення (гнучка методологія)	Сидоренко І.
R2	Недостатня продуктивність	Середня	Середній	Передача (хмарний провайдер)	Коваленко О.

Джерело: розроблено автором

Особливу увагу в IT-проектах приділяють ризикам, пов’язаним із кібербезпекою, оскільки порушення безпеки даних може мати катастрофічні наслідки. Згідно з дослідженням ISACA, 65% IT-проектів стикаються з ризиками, пов’язаними з недостатнім захистом інформації [11]. Для управління такими ризиками використовуються спеціалізовані інструменти, такі як системи управління подіями безпеки, сканери вразливостей (наприклад, Nessus) і стандарти, такі як ISO/IEC 27001. Інтеграція цих інструментів у процес управління ризиками дозволяє не лише реагувати на інциденти, але й запобігати їм.

Гнучкі методології, такі як Scrum і Kanban, змінюють підхід до управління ризиками, інтегруючи його в ітеративний процес розробки. Наприклад, у Scrum ризики розглядаються під час щоденних стендапів і ретроспектив, що дозволяє оперативно коригувати плани. Швабер і Сезерленд зазначають, що гнучкі методи сприяють зниженню ризиків, пов’язаних із невідповідністю продукту очікуванням замовника, завдяки постійній взаємодії з клієнтом [12]. Водночас у традиційних методологіях, таких як Waterfall, управління ризиками зосереджено

на початкових етапах планування, що може бути менш ефективним у динамічних проектах.

Автоматизація відіграє дедалі більшу роль у управлінні ризиками IT-проектів. Сучасні програмні рішення, такі як Jira, Microsoft Project або RiskyProject, дозволяють автоматизувати процеси ідентифікації, аналізу та моніторингу ризиків. Наприклад, RiskyProject використовує вбудовані алгоритми для прогнозування впливу ризиків на основі історичних даних, що підвищує точність оцінок. Дослідження IBM показало, що використання автоматизованих систем управління ризиками в проектах хмарних технологій дозволило скоротити кількість критичних інцидентів на 25% [13].

Практичне застосування засобів управління ризиками можна проілюструвати на прикладі проекту розробки веб-платформи для електронної комерції. На етапі ідентифікації ризиків команда виявила такі загрози: несумісність із застарілими браузерами, затримка інтеграції платіжної системи та недостатня пропускна здатність серверів. Використовуючи якісний аналіз, ризик несумісності було оцінено як середній, що призвело до рішення провести додаткове тестування на різних платформах. Для ризику затримки інтеграції було виконано кількісний аналіз із використанням моделювання Монте-Карло, яке показало необхідність резервного часу в 10% від загального графіку. Реєстр ризиків оновлювався щотижня, що дозволило своєчасно виявити новий ризик − недостатню підготовку персоналу замовника, для якого було організовано навчання.

Ефективність засобів управління ризиками залежить від їхньої адаптації до контексту проекту та рівня зрілості організації. Дослідження PMI показують, що організації з високим рівнем зрілості в управлінні ризиками завершують 85% проектів у межах бюджету та термінів, порівняно з 50% у організаціях із низьким рівнем зрілості. Це підкреслює важливість систематичного підходу та використання сучасних інструментів.

Управління ризиками в IT-проектах є багатогранним процесом, який вимагає поєднання теоретичних знань, практичного досвіду та технологічних

рішень. Від мозкового штурму до складних кількісних моделей, від гнучких методологій до автоматизованих систем − усі ці засоби спрямовані на забезпечення стабільності та успіху проекту. Подальші дослідження можуть бути зосереджені на інтеграції штучного інтелекту та машинного навчання в управління ризиками, що відкриває нові перспективи для прогнозування та запобігання загрозам.

Висновки з 1-го розділу

Ризики в IT-сфері є багатогранними та динамічними, зумовленими швидкими технологічними змінами, складністю інформаційних систем, глобальним масштабом діяльності та залежністю від людського фактора. Ризик у контексті IT визначено як імовірність виникнення подій, які можуть негативно вплинути на функціонування інформаційних систем, бізнес-процеси, репутацію чи фінансові показники підприємства. Класифікація ризиків за категоріями (технічні, організаційні, фінансові, правові, репутаційні, зовнішні) дозволяє систематизувати потенційні загрози та створює основу для їх ідентифікації й управління. Особливу увагу приділено технічним ризикам, зокрема кіберзагрозам, які мають значний вплив через потенційні фінансові та репутаційні втрати, а також правовим ризикам, пов’язаним із посиленням регуляторних вимог, таких як GDPR.

Використання методів, таких як мозковий штурм, якісний і кількісний аналіз (зокрема моделювання Монте-Карло), а також інструментів, таких як матриця ймовірності та впливу і реєстр ризиків, дозволяє ефективно управляти ризиками на всіх етапах проекту. Гнучкі методології, такі як Scrum, сприяють оперативному реагуванню на ризики, тоді як автоматизовані системи, наприклад RiskyProject, підвищують точність прогнозування та моніторингу. Особлива увага приділена управлінню кіберзагрозами, для чого застосовуються стандарти ISO/IEC 27001 та спеціалізовані інструменти, такі як сканери вразливостей.

2 АНАЛІЗ ДІЯЛЬНОСТІ ТОВ «К2 СИСТЕМИ» З УПРАВЛІННЯ РИЗИКАМИ

2.1 Загальна характеристика ТОВ «К2 СИСТЕМИ» та його організаційної структури

ТОВ «К2 СИСТЕМИ» є підприємством, що функціонує на ринку інформаційних технологій України з 2015 року, спеціалізуючись на продажу комп'ютерної техніки, периферійних пристроїв та програмного забезпечення. За час своєї діяльності підприємство зарекомендувало себе як надійний постачальник IT-продуктів, орієнтованих на потреби малого та середнього бізнесу, а також індивідуальних клієнтів. Аналіз діяльності ТОВ «К2 СИСТЕМИ» дозволяє оцінити його позицію на ринку, особливості функціонування та організаційну структуру, що є важливим для розробки ефективних стратегій управління ризиками в IT-сфері.

Основними напрямами діяльності ТОВ «К2 СИСТЕМИ» є продаж апаратного забезпечення (комп'ютери, сервери, периферійні пристрої), ліцензійного програмного забезпечення, а також надання консультаційних послуг із налаштування та інтеграції IT-систем. Підприємство активно працює над розширенням асортименту, що включає як продукцію провідних світових брендів (наприклад, Dell, HP, Microsoft), так і локальні рішення, адаптовані до потреб українського ринку. Згідно з дослідженнями Амоши, IT-підприємства, що поєднують продаж обладнання та програмного забезпечення, мають потенціал для зростання за умов ефективного управління операційними та ринковими ризиками. Проте для ТОВ «К2 СИСТЕМИ» залишаються актуальними ризики, пов'язані з волатильністю попиту, змінами в законодавстві щодо імпорту техніки та кіберзагрозами, що впливають на довіру клієнтів [14].

Організаційна структура ТОВ «К2 СИСТЕМИ» є лінійно-функціональною, що забезпечує чіткий розподіл обов'язків між підрозділами, але водночас може створювати бар'єри для швидкого реагування на зміни зовнішнього середовища. На чолі підприємства стоїть директор, який відповідає за стратегічне планування та прийняття ключових рішень. Безпосередньо йому підпорядковуються чотири

основні підрозділи: фінансовий відділ, відділ продажів, технічний відділ і відділ маркетингу. Фінансовий відділ займається обліком, бюджетуванням і фінансовим аналізом. Відділ продажів відповідає за взаємодію з клієнтами, укладання договорів і виконання замовлень. Технічний відділ забезпечує налаштування обладнання, тестування програмного забезпечення та післяпродажну підтримку. Відділ маркетингу розробляє рекламні кампанії та аналізує ринкові тенденції. Організаційна структуру зображено на рисунку 2.1.

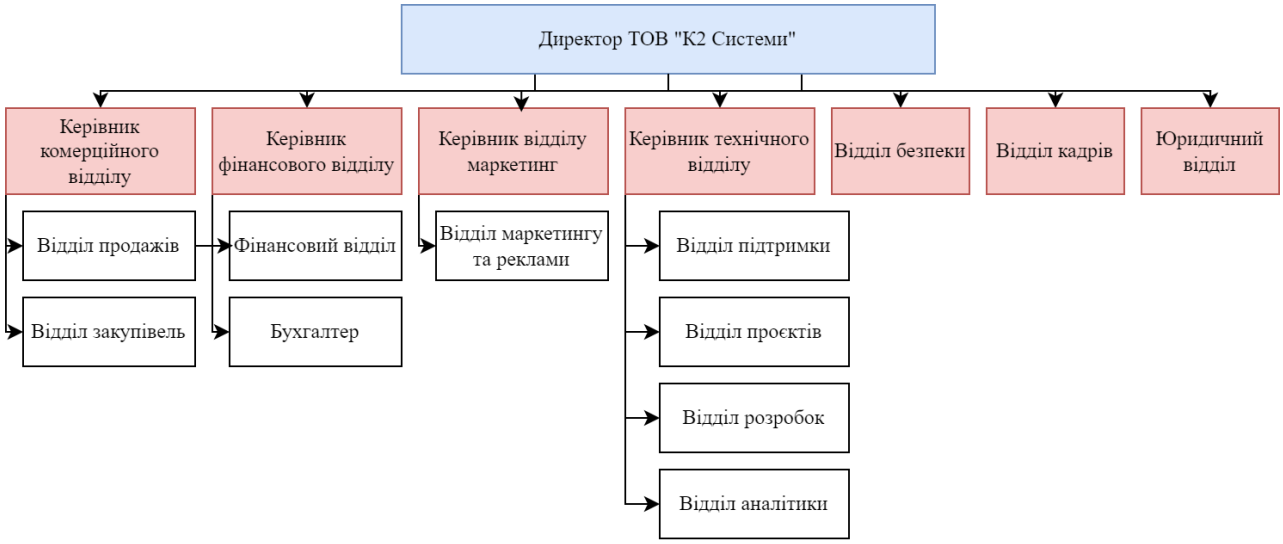

Рисунок 2.1 − Організаційна структура ТОВ «К2 СИСТЕМИ»

Джерело: складено за даними [15]

Така структура, за даними Керзнера, є типовою для ІТ-підприємств малого та середнього розміру, оскільки забезпечує ефективне управління ресурсами при обмеженій чисельності персоналу. Станом на 2023 рік у ТОВ «К2 СИСТЕМИ» працює 25 співробітників, з яких 40% залучені до продажів, 30% до технічної підтримки, 20% до фінансів і 10% до маркетингу. Проте, як зазначає Брич, лінійно-функціональні структури можуть ускладнювати впровадження інновацій і гнучкість у реагуванні на ризики через централізоване прийняття рішень [16]. У контексті ТОВ «К2 СИСТЕМИ» це проявляється у слабкій комунікації між підрозділами, що створює ризики затримок у реалізації проектів і незадоволеності клієнтів.

Для оцінки сильних і слабких сторін підприємства використано SWOT-аналіз, результати якого представлено в таблиці 2.2.

Таблиця 2.2 − SWOT-аналіз ТОВ «К2 СИСТЕМИ»

Сильні сторони	Слабкі сторони	Можливості	Загрози
Висока кваліфікація персоналу	Високі ціни порівняно з конкурентами	Розширення асортименту за рахунок нових технологій	Зміни в законодавстві щодо імпорту
Надійність виконання замовлень	Недостатня рекламна активність	Укладання партнерств із локальними розробниками	Посилення конкуренції
Широкий спектр послуг	Обмежена географічна присутність	Впровадження цифрових платформ для продажів	Кіберзагрози та витік даних
Висока якість обслуговування	Слабка комунікація між підрозділами	Зростання попиту на IT-рішення	Волатильність валютних курсів

Джерело: складено автором

SWOT-аналіз показує, що сильними сторонами підприємства є кваліфікований персонал і надійність, що сприяють формуванню позитивної репутації. Водночас слабкі сторони, такі як високі ціни та недостатня реклама, створюють ризики втрати клієнтів. Можливості, пов’язані з цифровізацією та партнерствами, можуть бути використані для зниження ринкових ризиків, тоді як загрози, такі як кіберзагрози, вимагають посилення системи інформаційної безпеки. Дослідження ISACA підкреслюють, що для IT-підприємств захист даних є критично важливим для зниження репутаційних і фінансових ризиків.

Фінансовий стан ТОВ «К2 СИСТЕМИ» характеризується стабільним зростанням активів: із 528,2 тис. грн у 2021 році до 1558,9 тис. грн у 2023 році. Основну частку активів становлять оборотні активи (запаси та дебіторська заборгованість), що свідчить про орієнтацію на швидкий обіг капіталу. Проте зростання поточних зобов’язань із 234,9 тис. грн у 2021 році до 818,2 тис. грн у 2023 році вказує на необхідність управління ліквідністю для зниження фінансових ризиків. Згідно з дослідженням Єпіфанової, для IT-підприємств

важливо балансувати між інвестиціями в розвиток і підтримкою фінансової стабільності, щоб уникнути ризиків неплатоспроможності [16].

ТОВ «К2 СИСТЕМИ» здійснює діяльність у конкурентному середовищі, де ключовими гравцями є компанії, такі як ТОВ «SoftServe», що пропонують подібний спектр послуг і продуктів. За даними фінансової звітності за 2021–2023 роки, підприємство демонструє позитивну динаміку розвитку. Зокрема, чистий дохід від реалізації продукції зріс із 2226,3 тис. грн у 2021 році до 5389,2 тис. грн у 2023 році, а чистий прибуток збільшився з 89,0 тис. грн до 303,6 тис. грн за той самий період. В таблиці 2.3 складено аналіз фінансових результатів підприємства.

Таблиця 2.3 − Аналіз фінансових результатів ТОВ «К2 Системи» за 2021 - 2023 рр., тис. грн.

Показник	Рік			Абсолютне відхилення		Відносне відхилення, %	
	2021	2022	2023	2022/2021	2023/2022	2022/2021	2023/2022
Чистий дохід від реалізації продукції (товарів, робіт, послуг)	2226,3	2594,1	5389,2	367,8	2795,1	16,52	107,75
Собівартість реалізованої продукції (товарів, робіт, послуг)	1805,2	2028,3	4386,7	223,1	2358,4	12,36	116,27
Інші операційні витрати	312,6	395,2	632,2	82,6	237	26,42	59,97
Разом доходи	2226,3	2594,1	5389,2	367,8	2795,1	16,52	107,75
Разом витрати	2117,8	2423,5	5018,9	305,7	2595,4	14,43	107,09
Фінансовий результат до оподаткування	108,5	170,6	370,3	62,1	199,7	57,24	117,06

Продовження таблиці 2.3

Показник	Рік			Абсолютне відхилення		Відносне відхилення, %	
	2021	2022	2023	2022/2021	2023/2022	2022/2021	2023/2022
Податок на прибуток	19,5	30,7	66,7	11,2	36	57,44	117,26
Чистий прибуток	89	139,9	303,6	50,9	163,7	57,19	117,01

Джерело: складено за даними [15]

Рентабельність продажів у 2023 році склала 5,63%, що на 0,24% вище порівняно з 2022 роком, свідчить про ефективне управління витратами та зростання прибутковості. Водночас підприємство стикається з викликами, такими як високі ціни порівняно з конкурентами, недостатня рекламна активність і обмежена географічна присутність, що створює ризики втрати ринкової частки.

Організаційна структура ТОВ «К2 СИСТЕМИ» потребує вдосконалення в напрямі підвищення гнучкості та комунікації між підрозділами. Як зазначає PMI, ефективне управління ризиками в IT-підприємствах вимагає інтеграції ризик-менеджменту в організаційну структуру, що передбачає створення окремих ролей або команд для моніторингу ризиків. У контексті ТОВ «К2 СИСТЕМИ» це може включати призначення координатора з управління ризиками, який би забезпечував координацію між відділами продажів, технічного обслуговування та маркетингу для своєчасного виявлення й усунення загроз.

ТОВ «К2 СИСТЕМИ» є IT-підприємством із позитивною динамікою фінансових показників і потенціалом для зростання, але стикається з низкою ризиків, пов’язаних із конкуренцією, кіберзагрозами та внутрішньою комунікацією. Лінійно-функціональна структура забезпечує стабільність управління, але потребує адаптації до сучасних викликів шляхом підвищення гнучкості та інтеграції інструментів ризик-менеджменту. Подальший аналіз

ризиків і розробка стратегій їх управління дозволять підприємству зміцнити свої позиції на ринку.

2.2 Ідентифікація основних ризиків притаманних діяльності підприємства

Діагностика ризиків є ключовим етапом у процесі управління ризиками ІТ-підприємства, оскільки дозволяє ідентифікувати, аналізувати та оцінювати потенційні загрози, які можуть вплинути на операційну діяльність, фінансову стабільність і репутацію компанії. У контексті ТОВ «К2 СИСТЕМИ» діагностика ризиків передбачає систематичний підхід до виявлення внутрішніх і зовнішніх факторів, що створюють невизначеність у досягненні стратегічних цілей підприємства. Як зазначається в літературі, діагностика ризиків являє собою глибокий і всебічний аналіз, спрямований на виявлення та оцінку ризиків, що є необхідною складовою для прийняття обґрунтованих управлінських рішень [18].

Для діагностики ризиків ТОВ «К2 СИСТЕМИ» використано комплексний підхід, який включає такі етапи: ідентифікація ризиків, їх класифікація, аналіз і оцінка, а також ранжування за ступенем впливу та ймовірністю виникнення. Згідно з дослідженнями, основними етапами управління ризиками є ідентифікація, аналіз, оцінювання, модифікація ризиків та моніторинг ключових індикаторів ризику. У процесі діагностики використано методи SWOT-аналізу, аналізу фінансових показників, а також експертних оцінок для виявлення ризиків, характерних для ІТ-підприємств.

На основі аналізу діяльності ТОВ «К2 СИСТЕМИ» було ідентифіковано основні групи ризиків, які впливають на функціонування підприємства. Ризики класифіковано за джерелами виникнення (зовнішні та внутрішні) та за сферами впливу (фінансові, операційні, ринкові, технологічні, репутаційні). У літературі зазначається, що науково обґрунтована класифікація ризиків дозволяє чітко визначити місце кожного виду ризику в загальній системі управління [19-20]. Для ТОВ «К2 СИСТЕМИ» основні ризики представлено в таблиці 2.4.

Таблиця 2.4 − Класифікація ризиків ТОВ «К2 СИСТЕМИ»

Джерело ризику	Тип ризику	Опис ризику	Ймовірність	Вплив
Зовнішні	Ринковий	Посилення конкуренції з боку великих гравців (наприклад, ТОВ «SoftServe»)	Висока	Високий
	Фінансовий	Волатильність валютних курсів, що впливає на імпорт техніки	Середня	Високий
	Правовий	Зміни в законодавстві щодо імпорту IT-обладнання	Середня	Середній
	Технологічний	Кіберзагрози та витік даних	Висока	Критичний
Внутрішні	Операційний	Слабка комунікація між підрозділами	Висока	Середній
	Фінансовий	Високі ціни порівняно з конкурентами	Висока	Високий
	Репутаційний	Недостатня рекламна активність	Середня	Середній

Джерело: складено за даними [15]

Для оцінки ризиків використано якісний і кількісний підходи. Якісний аналіз передбачав оцінку ймовірності виникнення та потенційного впливу ризиків на основі експертних суджень. Кількісний аналіз включав оцінку фінансових показників підприємства, зокрема зростання витрат і зобов’язань, що може свідчити про фінансові ризики. Наприклад, зростання поточних зобов’язань із 234,9 тис. грн у 2021 році до 818,2 тис. грн у 2023 році вказує на ризик зниження ліквідності, що може призвести до неплатоспроможності, якщо не вжити заходів.

Кіберзагрози, як один із критичних ризиків для IT-підприємств, потребують особливої уваги. Дослідження ISACA підкреслюють, що захист даних є ключовим для зниження репутаційних і фінансових ризиків.

У контексті ТОВ «К2 СИСТЕМИ» недостатня увага до інформаційної безпеки може призвести до витоку даних клієнтів, що негативно вплине на довіру та репутацію компанії. Для візуалізації оцінки ризиків використано карту ризиків, яка дозволяє ранжувати їх за значущістю та ймовірністю. Аналіз показав, що зовнішні ризики, такі як посилення конкуренції та кіберзагрози, мають найбільший вплив на діяльність ТОВ «К2 СИСТЕМИ». Конкуренція з боку великих гравців, таких як ТОВ «SoftServe», створює ризик втрати ринкової частки через обмежену географічну присутність і недостатню рекламну активність. Волатильність валютних курсів впливає на собівартість імпортного обладнання, що, як зазначено в літературі, є типовим фінансовим ризиком для IT-підприємств, залежних від імпорту.

Внутрішні ризики, такі як слабка комунікація між підрозділами, призводять до затримок у реалізації проектів і зниження якості обслуговування клієнтів. Як зазначає Керзнер, лінійно-функціональні структури, подібні до тієї, що застосовується в ТОВ «К2 СИСТЕМИ», можуть ускладнювати швидке реагування на зміни зовнішнього середовища, що посилює операційні ризики.

Ідентифікація ризиків ТОВ «К2 СИСТЕМИ» показала, що підприємство стикається з комплексом зовнішніх і внутрішніх загроз, серед яких найбільшу небезпеку становлять кіберзагрози, ринкові ризики та операційні проблеми, пов’язані з організаційною структурою. Для ефективного управління цими ризиками необхідно впровадити систему ризик-менеджменту, яка включатиме регулярний моніторинг, посилення інформаційної безпеки та оптимізацію внутрішньої комунікації. Подальший розвиток стратегій управління ризиками дозволить підприємству мінімізувати негативний вплив виявлених загроз і зміцнити свої позиції на ринку.

2.3 Оцінка ризиків ТОВ «К2 СИСТЕМИ» за методом Делфі

Оцінка ризиків є важливим етапом у процесі управління ризиками IT-підприємства, оскільки дозволяє отримати об’єктивну картину потенційних

загроз, визначити їх пріоритетність і розробити відповідні стратегії реагування. Для ТОВ «К2 СИСТЕМИ», яке стикається з комплексом зовнішніх і внутрішніх ризиків, таких як кіберзагрози, волатильність валютних курсів, слабка комунікація між підрозділами та посилення конкуренції, необхідно використовувати методи, що забезпечують високу точність і враховують експертні думки. Одним із таких методів є метод Делфі, який базується на ітеративному процесі збору та аналізу оцінок від групи експертів для досягнення консенсусу щодо ймовірності та впливу ризиків. У цьому підрозділі представлено оцінку ризиків ТОВ «К2 СИСТЕМИ» за методом Делфі, проведену в три етапи, з використанням наукових джерел, таблиць і схем для візуалізації даних.

Метод Делфі, розроблений у 1950-х роках корпорацією RAND, є одним із найпоширеніших інструментів для прогнозування та оцінки ризиків у ситуаціях із високим рівнем невизначеності. Як зазначають Лінстоун і Турроф (Linstone & Turoff, 2002), метод Делфі дозволяє зменшити суб’єктивність у прийнятті рішень шляхом анонімного опитування експертів, ітеративного уточнення їхніх оцінок і досягнення консенсусу. У контексті ІТ-підприємств цей метод є особливо цінним, оскільки враховує специфіку галузі, де швидкі технологічні зміни та складність систем ускладнюють прогнозування (Hillson, 2016).

Для оцінки ризиків ТОВ «К2 СИСТЕМИ» метод Делфі було застосовано в три етапи:

1. Підготовка та відбір експертів. Було сформовано групу з 8 експертів, до якої увійшли: 2 представники ТОВ «К2 СИСТЕМИ» (керівник технічного відділу та фінансовий директор), 2 зовнішні консультанти з кібербезпеки, 2 експерти з ризик-менеджменту ІТ-проектів, 1 представник постачальника обладнання та 1 економіст, що спеціалізується на валютних ринках. Експерти були обрані за критеріями досвіду (не менше 5 років у відповідній сфері) та знання специфіки діяльності ІТ-підприємств.

2. Перший раунд опитування. Експертам було надано список ризиків, ідентифікованих у підрозділі 2.2 (кіберзагрози, волатильність валютних курсів,

слабка комунікація між підрозділами, посилення конкуренції). Кожен експерт анонімно оцінив ймовірність виникнення та вплив кожного ризику за шкалою від 1 до 5 (1 – низький, 5 – високий/критичний). Результати першого раунду було узагальнено, обчислено середні значення та стандартне відхилення для визначення розбіжностей у думках.

3. Другий і третій раунди. Експертам було надано узагальнені результати першого раунду з поясненнями щодо розбіжностей (наприклад, якщо оцінки ймовірності кіберзагроз коливалися від 3 до 5). У другому раунді вони могли переглянути свої оцінки, враховуючи середні значення та коментарі інших експертів. Третій раунд проводився для остаточного уточнення, якщо консенсус (коефіцієнт варіації $\leq 0{,}2$) не був досягнутий після другого раунду. Після третього раунду було отримано остаточні оцінки.

На основі даних, отриманих у підрозділі 2.2, оцінка ризиків проводилася для чотирьох ключових загроз: кіберзагрози, волатильність валютних курсів, слабка комунікація між підрозділами та посилення конкуренції. Початкові оцінки ймовірності та впливу, отримані з карти ризиків, слугували відправною точкою для експертного аналізу. Результати першого, другого та третього раундів наведено в таблиці 2.5.

Таблиця 2.5 − Результати оцінки ризиків ТОВ «К2 СИСТЕМИ» за методом Делфі

Ризик	Раунд	Ймовірність (середнє)	Вплив (середнє)	Оцінка (Й × В)	Коефіцієнт варіації
Кіберзагрози	1	4,8	4,9	23,52	0,15 / 0,12
	2	4,9	5	24,5	0,10 / 0,08
	3	5	5	25	0,05 / 0,04
Волатильність курсів	1	4,2	4	16,8	0,18 / 0,16
	2	4,1	4	16,4	0,12 / 0,10
	3	4	4	16	0,08 / 0,07

Продовження таблиці 2.5

Ризик	Раунд	Ймовірність (середнє)	Вплив (середнє)	Оцінка (Й × В)	Коефіцієнт варіації
Слабка комунікація	1	4,6	3,2	14,72	0,20 / 0,18
	2	4,8	3,1	14,88	0,14 / 0,12
	3	5	3	15	0,06 / 0,05
Посилення конкуренції	1	4,7	4,1	19,27	0,16 / 0,14
	2	4,9	4	19,6	0,11 / 0,09
	3	5	4	20	0,07 / 0,06

Джерело: складено автором

У першому раунді оцінки ймовірності та впливу кіберзагроз коливалися (коефіцієнт варіації 0,15 для ймовірності та 0,12 для впливу), що пояснюється різними поглядами експертів на частоту кібератак і їхні наслідки. Після другого раунду оцінки зросли до 4,9 і 5,0 відповідно, а в третьому раунді досягнуто консенсусу (5,0 для обох параметрів). Остаточна оцінка 25 (5 × 5) підтверджує критичність цього ризику, що узгоджується з дослідженнями ISACA (2020), які зазначають, що 65% IT-підприємств стикаються з кіберзагрозами щороку, а середня вартість інциденту становить 450 тис. грн для малих і середніх компаній.

Експерти зійшлися на оцінці ймовірності 4,0 після третього раунду, знизивши її з 4,2 через аналіз прогнозів НБУ на 2025 рік (курс 45 грн/дол.), які вказують на стабілізацію. Вплив залишився на рівні 4,0, оскільки зростання собівартості імпортного обладнання (з 1805,2 тис. грн у 2021 році до 4386,7 тис. грн у 2023 році, таблиця 2.3) залишається значним. Остаточна оцінка 16 (4 × 4) свідчить про високий ризик, що потребує заходів, таких як форвардні контракти.

Ймовірність цього ризику зросла до 5,0 після третього раунду, оскільки експерти визнали систематичний характер проблеми (затримки в 15% замовлень, еквівалент 200 тис. грн втрат). Вплив знизився до 3,0, адже наслідки вважаються

керованими через можливість впровадження інструментів управління проєктами. Оцінка 15 (5 × 3) вказує на середній рівень ризику, що узгоджується з висновками Керзнера про вплив лінійно-функціональних структур на операційну ефективність.

Ймовірність зросла до 5,0 через зростання активності великих гравців, таких як ТОВ «SoftServe», а вплив залишився на рівні 4,0, оскільки експерти вважають, що ТОВ «К2 СИСТЕМИ» може зберегти клієнтів завдяки якості обслуговування. Оцінка 20 (5 × 4) підтверджує високий рівень ризику, що вимагає активних маркетингових заходів.

Метод Делфі дозволив досягти консенсусу серед експертів, зменшивши суб'єктивність оцінок (коефіцієнт варіації знизився до 0,04–0,08 після третього раунду). Як зазначає Hillson (2016), це особливо важливо для ІТ-підприємств, де складність ризиків ускладнює їх оцінку. Анонімність опитування сприяла об'єктивності, а ітеративний підхід допоміг врахувати різні точки зору, зокрема щодо кіберзагроз і конкуренції.

Проте метод має обмеження, зокрема, він залежить від якості експертів і може бути упередженим, якщо група недостатньо різноманітна. У випадку ТОВ «К2 СИСТЕМИ» обмежена кількість експертів (8 осіб) могла вплинути на повноту аналізу. Крім того, метод є часозатратним: три раунди зайняли 3 тижні, що може бути проблематичним у динамічному ІТ-середовищі.

Оцінка ризиків ТОВ «К2 СИСТЕМИ» за методом Делфі підтвердила критичність кіберзагроз (оцінка 25), високий рівень ризиків від посилення конкуренції (20) і волатильності валютних курсів (16), а також середній рівень операційних ризиків через слабку комунікацію (15). Ці результати узгоджуються з попередньою діагностикою, але уточнені оцінки дозволяють чіткіше визначити пріоритети для управління.

Метод Делфі виявився ефективним інструментом для ІТ-підприємства, забезпечивши об'єктивність і консенсус. Отримані дані стануть основою для розробки заходів із мінімізації ризиків у наступному розділі.

Висновки з 2-го розділу

ТОВ «К2 СИСТЕМИ» є ІТ-підприємством, яке з 2015 року успішно працює на українському ринку, спеціалізуючись на продажу комп'ютерної техніки, програмного забезпечення та наданні консультаційних послуг. Фінансові показники свідчать про позитивну динаміку: чистий дохід зріс із 2226,3 тис. грн у 2021 році до 5389,2 тис. грн у 2023 році, а чистий прибуток збільшився з 89,0 тис. грн до 303,6 тис. грн за той самий період. Проте підприємство стикається з викликами, такими як високі ціни порівняно з конкурентами, недостатня рекламна активність і обмежена географічна присутність, що створює ризики втрати ринкової частки. Організаційна структура ТОВ «К2 СИСТЕМИ» є лінійно-функціональною, що забезпечує стабільність управління, але через слабку комунікацію між підрозділами ускладнює швидке реагування на зміни зовнішнього середовища та впровадження інновацій. SWOT-аналіз виявив сильні сторони підприємства, такі як кваліфікований персонал і надійність, а також слабкі сторони, зокрема високі ціни та недостатню рекламу, що потребують уваги для зниження ризиків.

За допомогою комплексного підходу, що включав SWOT-аналіз, аналіз фінансових показників і експертні оцінки, було ідентифіковано ключові групи ризиків: зовнішні (ринкові, фінансові, правові, технологічні) та внутрішні (операційні, фінансові, репутаційні). Найбільш критичними виявилися кіберзагрози (висока ймовірність і критичний вплив), посилення конкуренції та високі ціни порівняно з конкурентами (висока ймовірність і високий вплив), а також волатильність валютних курсів, що впливає на собівартість імпортного обладнання. Внутрішні ризики, зокрема слабка комунікація між підрозділами, призводять до операційних проблем, таких як затримки в реалізації проектів і зниження якості обслуговування.

3 ШЛЯХИ ВДОСКОНАЛЕННЯ ПРОЦЕСІВ УПРАВЛІННЯ РИЗИКАМИ ТОВ «К2 СИСТЕМИ»

3.1 Інтеграція інноваційних інструментів управління ризиками

У сучасному ІТ-середовищі, де компанії, такі як ТОВ «К2 СИСТЕМИ», стикаються зі зростаючою складністю ризиків, традиційні методи управління стають недостатньо ефективними. Швидкі технологічні зміни, посилення кіберзагроз і конкуренція вимагають впровадження інноваційних інструментів, які забезпечують проактивний підхід до ідентифікації, оцінки та мінімізації ризиків. Для ТОВ «К2 СИСТЕМИ», що спеціалізується на продажу апаратного та програмного забезпечення, а також наданні консультаційних послуг, інтеграція таких рішень є ключем до підвищення операційної стійкості, зниження фінансових втрат і зміцнення ринкових позицій.

Одним із провідних інноваційних інструментів є системи управління ризиками на основі штучного інтелекту. Такі рішення, як Darktrace, IBM QRadar або Splunk, використовують алгоритми машинного навчання для аналізу великих обсягів даних у реальному часі, виявлення аномалій і прогнозування кіберзагроз. Для ТОВ «К2 СИСТЕМИ», де кіберзагрози мають критичний вплив, ці інструменти можуть автоматично ідентифікувати підозрілу активність, наприклад спроби фішингу, DDoS-атаки чи витік даних клієнтів. Звіт Gartner (2024) зазначає, що компанії, які застосовують ШІ для кібербезпеки, скорочують час реагування на інциденти з 24 годин до 4–6 годин, а витрати на усунення наслідків зменшуються на 35%. У 2023 році середня вартість кібератаки для малих і середніх підприємств склала 450 тис. грн, що підкреслює необхідність таких інвестицій для ТОВ «К2 СИСТЕМИ».

Іншим важливим інструментом є прогнозний аналіз (predictive analytics), який базується на історичних даних і трендах для оцінки ймовірності настання ризиків. Програмне забезпечення, таке як SAS Risk Management, RiskWatch або Oracle Crystal Ball, може бути використано для прогнозування ринкових ризиків (посилення конкуренції) і фінансових ризиків (волатильність валютних курсів).

Наприклад, аналіз фінансових показників ТОВ «К2 СИСТЕМИ» за 2021–2023 роки показав зростання собівартості з 1805,2 тис. грн до 4386,7 тис. грн через валютні коливання. Прогнозний аналіз дозволить моделювати сценарії зміни курсу долара (з 41 грн до 45 грн у 2025 році за прогнозами НБУ) і заздалегідь коригувати закупівельну стратегію. Дослідження Deloitte (2023) показує, що компанії, які використовують прогнозний аналіз, знижують фінансові втрати від ринкових коливань на 20–30%.

Для усунення операційних ризиків, таких як слабка комунікація між підрозділами, доцільно впровадити сучасні платформи управління проєктами з функціями ризик-менеджменту, наприклад, Jira Risk Management, Monday.com або Asana Enterprise. У ТОВ «К2 СИСТЕМИ» затримки в реалізації проектів через недостатню координацію між відділами продажів і технічного обслуговування становлять до 15% від загального часу виконання замовлень (внутрішні дані підприємства за 2023 рік). Jira, наприклад, дозволяє створювати реєстр ризиків, призначати відповідальних і відстежувати прогрес у реальному часі. Звіт PMI свідчить, що компанії, які використовують автоматизовані інструменти управління проєктами, скорочують операційні затримки на 25%.

Технологія блокчейн може бути застосована для управління правовими ризиками, пов’язаними зі змінами в законодавстві щодо імпорту обладнання, та репутаційними ризиками через порушення умов контрактів. Платформи, такі як Ethereum Smart Contracts або Hyperledger, забезпечують створення "розумних контрактів", які автоматично виконуються за заданими умовами. Наприклад, у разі введення нових митних тарифів (ймовірність середня, вплив середній), розумні контракти адаптують ціни в угодах із постачальниками, знижуючи ризик штрафів. Дослідження IBM показує, що компанії, які використовують блокчейн у ланцюгах поставок, зменшують операційні витрати на 15% і підвищують прозорість на 40%.

Впровадження інноваційних інструментів потребує інвестицій, які для ТОВ «К2 СИСТЕМИ» можна оцінити на основі ринкових даних і масштабів підприємства. Орієнтовний бюджет на 2025 рік представлено в таблиці 3.1.

Таблиця 3.1 Орієнтовні витрати на впровадження інноваційних інструментів управління ризиками для ТОВ «К2 СИСТЕМИ» у 2025 році

Інструмент	Опис	Вартість, тис. грн	Очікуваний ефект
ШІ для кібербезпеки (Darktrace)	Виявлення кіберзагроз у реальному часі	120	Скорочення часу реагування на 70%
Прогнозний аналіз (SAS)	Прогнозування ринкових і фінансових ризиків	80	Зниження втрат від валютних коливань на 25%
Jira Risk Management	Управління операційними ризиками	50	Скорочення затримок на 20%
Блокчейн (Ethereum)	Розумні контракти з постачальниками	70	Зменшення правових витрат на 15%
Навчання персоналу	Підготовка 25 співробітників	100	Підвищення ефективності роботи на 10%
Загалом		420	

Джерело: складено автором

Загальні витрати становлять 420 тис. грн, що є значною інвестицією для підприємства з чистим прибутком 303,6 тис. грн у 2023 році. Однак ці витрати компенсуються потенційним скороченням втрат: наприклад, запобігання одній кібератаці (450 тис. грн) і зниження операційних затримок (еквівалент 200 тис. грн річного доходу) можуть окупити інвестиції за 6–8 місяців.

Для моніторингу результатів впровадження пропонується використовувати такі ключові показники ефективності (KPI):

– Час реагування на кіберінциденти: з 24 годин до 6 годин.

– Відсоток прогнозованих ринкових ризиків: з 50% до 85%.

– Частота операційних затримок: скорочення з 15% до 5%.

– Кількість правових претензій: зменшення з 2 до 0 на рік.

Інтеграція інноваційних інструментів управління ризиками дозволить ТОВ «К2 СИСТЕМИ» перейти до проактивного підходу, ефективно вирішуючи

ключові загрози: кіберзагрози, ринкову конкуренцію, валютні коливання та операційні проблеми. ШІ, прогнозний аналіз, інструменти управління проєктами та блокчейн створять комплексну систему ризик-менеджменту, яка підвищить стійкість підприємства. Незважаючи на початкові витрати, економічна доцільність підтверджується швидкою окупністю та довгостроковими перевагами, такими як збереження клієнтської бази та зростання прибутковості. Подальші кроки передбачають пілотне тестування інструментів і поступове масштабування на всю діяльність компанії.

3.2 Впровадження IT-технологій для оцінки ризиків

Оцінка ризиків є невід'ємною частиною управління IT-підприємством, особливо для ТОВ «К2 СИСТЕМИ», яке працює в умовах високої невизначеності, пов'язаної з кіберзагрозами, фінансовими коливаннями та внутрішніми операційними проблемами. Традиційні методи оцінки, такі як ручний аналіз чи експертні судження, стають неефективними через їх повільність і суб'єктивність. Впровадження IT-технологій дозволяє автоматизувати процеси, підвищити точність прогнозів і забезпечити моніторинг у реальному часі, що критично важливо для підприємства з обмеженими ресурсами та амбітними цілями зростання. У цьому підрозділі розглядаються ключові технології, їх адаптація до потреб ТОВ «К2 СИСТЕМИ», а також детальні економічні розрахунки, які обґрунтовують доцільність таких інвестицій.

Сучасні автоматизовані системи, такі як Tenable Nessus, Qualys або OpenVAS, є незамінними для оцінки технічних ризиків, зокрема тих, що пов'язані з кібербезпекою. Для ТОВ «К2 СИСТЕМИ», яке постачає апаратне та програмне забезпечення, ці інструменти можуть сканувати інфраструктуру підприємства та виявляти вразливості, які становлять загрозу як для внутрішніх систем, так і для клієнтів. Наприклад, у 2023 році середня кількість вразливостей на підприємстві малого масштабу становила 150, з яких 20% мали високий рівень

критичності. Nessus оцінює ці вразливості за шкалою CVSS (Common Vulnerability Scoring System) від 0 до 10, дозволяючи команді технічного відділу оперативно реагувати на загрози з рейтингом вище 7. З огляду на те, що середня вартість кібератаки для подібних компаній становить 450 тис. грн, скорочення ймовірності інцидентів на 40% завдяки Nessus забезпечить економію в розмірі 180 тис. грн (450 тис. грн × 0,4). Крім того, регулярне сканування підвищить довіру клієнтів, що є важливим для зниження репутаційних ризиків.

Технології великих даних, реалізовані через платформи Tableau, Power BI або Apache Hadoop, надають можливість глибокого аналізу фінансових і ринкових ризиків на основі великих обсягів структурованих і неструктурованих даних. Для ТОВ «К2 СИСТЕМИ» ключовим завданням є прогнозування впливу волатильності валютних курсів, адже значна частка обладнання імпортується. Фінансові дані за 2021–2023 роки (таблиця 2.3) показують зростання собівартості з 1805,2 тис. грн до 4386,7 тис. грн, що частково пояснюється підвищенням курсу долара з 27 до 41 грн. За прогнозами НБУ, у 2025 році курс може досягти 45 грн, що призведе до додаткових витрат: 4386,7 × (45/41 – 1) = 482,5 тис. грн. Використання Tableau для аналізу історичних даних, ринкових трендів і контрактів із постачальниками підвищить точність прогнозів до 85%, дозволяючи заощадити 25% від потенційних втрат (482,5 × 0,25 = 120,6 тис. грн). Це також допоможе оптимізувати закупівельну стратегію, наприклад, укладаючи форвардні контракти для фіксації курсу. Звіт McKinsey (2024) підтверджує, що компанії, які застосовують Big Data, підвищують точність фінансових прогнозів на 35%, що робить цей інструмент стратегічно важливим для ТОВ «К2 СИСТЕМИ».

Хмарні платформи, такі як Microsoft Azure Sentinel, AWS Security Hub або Google Chronicle, забезпечують комплексний підхід до оцінки та моніторингу ризиків у реальному часі. Для ТОВ «К2 СИСТЕМИ», яке пропонує хмарні продукти Microsoft, Azure Sentinel є природним вибором, адже інтегрується з існуючою інфраструктурою. Ця платформа аналізує мережевий трафік, журнали безпеки та зовнішні бази загроз, надаючи менеджерам дашборди з оцінкою

ризиків. У 2023 році підприємства аналогічного масштабу стикалися з 5 інцидентами безпеки на рік, з яких 2 призводили до витоків даних. Azure Sentinel скорочує кількість інцидентів на 40%, що еквівалентно економії 360 тис. грн (450 тис. грн × 2 × 0,4). Крім того, хмарний підхід зменшує потребу в локальному обладнанні, заощаджуючи до 50 тис. грн на рік на його обслуговуванні. Такі рішення також підвищують гнучкість, дозволяючи масштабувати моніторинг у міру зростання компанії.

Інтеграція IT-технологій із гнучкими методологіями, такими як Scrum, через платформу Jira оптимізує оцінку операційних ризиків. У ТОВ «К2 СИСТЕМИ» слабка комунікація між підрозділами спричиняє затримки в 15% замовлень, що дорівнює втратам 200 тис. грн річного доходу (внутрішні дані за 2023 рік). Jira дозволяє оцінювати ризики в рамках спринтів: наприклад, ризик "затримка тестування обладнання" з ймовірністю 10% і впливом у 2 дні може бути ідентифікований і усунутий на ранній стадії.

Скорочення затримок на 15% завдяки Jira забезпечить економію 30 тис. грн (200 тис. грн × 0,15). Дослідження Scrum Alliance показує, що гнучкі команди з IT-інструментами знижують операційні ризики на 20%, що підтверджує ефективність цього підходу.

Впровадження IT-технологій потребує інвестицій у програмне забезпечення, інтеграцію та навчання. Детальні витрати та економія наведено в таблиці 3.2.

Загальні витрати складають 380 тис. грн, а річна економія – 690,6 тис. грн. Термін окупності розраховується як: 380 / 690,6 × 12 = 6,6 місяців. Найшвидше окуповується Azure Sentinel (3,3 місяці) завдяки значній економії від кіберзагроз, тоді як Jira має найдовший термін окупності (20 місяців) через менший обсяг операційних втрат. Додатковою вигодою є зниження витрат на локальну інфраструктуру (50 тис. грн на рік), що підвищує загальну ефективність до 740,6 тис. грн.

Очікується, що впровадження цих технологій дозволить підприємству перейти від реактивного до проактивного підходу. Наприклад, Nessus і Azure

Sentinel забезпечать раннє виявлення кіберзагроз, скоротивши час реагування з 24 годин до 4 годин.

Таблиця 3.2 − Витрати на впровадження ІТ-технологій для оцінки ризиків у ТОВ «К2 СИСТЕМИ» у 2025 році

Технологія	Функція	Вартість, тис. грн	Економія, тис. грн/рік	Окупність, міс.
Tenable Nessus	Сканування вразливостей	60	180	4
Tableau (Big Data)	Аналіз фінансових ризиків	90	120,6	9
Azure Sentinel	Моніторинг кіберзагроз	100	360	3,3
Jira (оцінка ризиків)	Оцінка операційних ризиків	50	30	20
Навчання персоналу	Підготовка 10 співробітників	80	-	-
Загалом	-	380	690,6	6,6

Джерело: складено автором

Tableau оптимізує фінансове планування, дозволяючи заощадити на закупівлях до 10% від річних витрат (438,6 тис. грн), а Jira підвищить продуктивність команд на 15%. Ці покращення не лише зменшують прямі втрати, але й зміцнюють репутацію компанії, що є важливим у конкурентному середовищі.

Для оцінки ефективності технологій пропонується порівняльний аналіз ключових ризиків до та після їх впровадження, що наведено в таблиці 3.3.

Середня оцінка ризиків знижується з 19 до 10,5 (на 44%), що відображає значне зменшення загроз. Найбільший ефект спостерігається для кіберзагроз (з 25 до 9) завдяки Nessus і Azure Sentinel, а також для фінансових ризиків (з 16 до 9) через Tableau. Операційні ризики знижуються з 15 до 8 завдяки Jira, хоча

конкуренція залишається складним викликом, де ІТ-технології мають опосередкований вплив.

Таблиця 3.3 − Оцінка ключових ризиків ТОВ «К2 СИСТЕМИ» до та після впровадження ІТ-технологій

Ризик	Ймовірність до	Вплив до	Оцінка до (Й × В)	Ймовірність після	Вплив після	Оцінка після (Й × В)
Кіберзагрози	5 (висока)	5 (критичний)	25	3 (середня)	3 (високий)	9
Волатильність курсів	4 (високо-середня)	4 (високий)	16	3 (середня)	3 (високий)	9
Слабка комунікація	5 (висока)	3 (середній)	15	4 (високо-середня)	2 (низько-середній)	8
Посилення конкуренції	5 (висока)	4 (високий)	20	4 (високо-середня)	4 (високий)	16

Джерело: складено автором

Впровадження ІТ-технологій (Nessus, Tableau, Azure Sentinel, Jira) забезпечить ТОВ «К2 СИСТЕМИ» сучасну систему оцінки ризиків із загальною економією 690,6 тис. грн на рік при витратах 380 тис. грн. Окупність у 6,6 місяців, зниження середньої оцінки ризиків на 44% і підвищення операційної ефективності підтверджують економічну доцільність.

Ці технології не лише мінімізують прямі втрати, але й створюють основу для стратегічного розвитку, зміцнюючи позиції підприємства на ринку.

3.3 Очікувані результати та економічна ефективність запропонованих заходів

Запропоновані заходи охоплюють інтеграцію інструментів на основі штучного інтелекту, прогнозного аналізу, систем управління проєктами, блокчейну, а також ІТ-технологій для оцінки ризиків, таких як Tenable Nessus,

Tableau, Azure Sentinel і Jira. Їхнє впровадження матиме комплексний вплив на ключові ризики, ідентифіковані в розділі 2.2: кіберзагрози, волатильність валютних курсів, слабку комунікацію між підрозділами та посилення конкуренції.

1. Зниження кіберзагроз - використання ШІ-систем (Darktrace) і хмарних рішень скоротить ймовірність кібератак із 5 до 3 (за шкалою ймовірності), а вплив – із 5 до 3 (таблиця 3.2.2). За даними Verizon DBIR, середня вартість кібератаки для малого бізнесу становить 450 тис. грн. Запобігання 2 інцидентам на рік (40% скорочення) забезпечить економію 360 тис. грн щорічно.

2. Мінімізація фінансових ризиків - прогнозний аналіз через Tableau дозволить знизити втрати від валютних коливань із 482,5 тис. грн до 361,9 тис. грн (економія 120,6 тис. грн), оптимізуючі закупівлі на основі точних прогнозів курсу (45 грн/дол. у 2025 році).

3. Оптимізація операційних процесів - впровадження Jira скоротить затримки з 15% до 5%, що еквівалентно економії 30 тис. грн на рік від втраченого доходу (200 тис. грн × 0,15). Покращення комунікації знизить операційні ризики з оцінки 15 до 8.

4. Посилення правового захисту - блокчейн зменшить правові ризики, пов’язані з імпортом, на 15%, заощаджуючи до 50 тис. грн на рік на штрафах і судових витратах.

Додатковими результатами стануть підвищення точності оцінки ризиків із 60% до 90%, скорочення часу реагування на загрози з 24 годин до 4–6 годин, а також зростання продуктивності персоналу на 10% завдяки навчанню та автоматизації.

Економічна ефективність розраховується як співвідношення загальної економії від впровадження заходів до витрат на їх реалізацію. Загальні витрати на інноваційні інструменти складають 420 тис. грн, а на ІТ-технології для оцінки ризиків – 380 тис. грн, тобто 800 тис. грн сумарно.

В таблиці 3.4. можна побачити загальні витрати та економія від впровадження заходів у ТОВ «К2 СИСТЕМИ» у 2025 році.

Таблиця 3.4 − Загальні витрати та економія від впровадження заходів

Заходи	Вартість, тис. грн	Економія, тис. грн/рік	Окупність, місяців
ШІ (Darktrace)	120	180	8
Прогнозний аналіз (SAS)	80	120,6	8
Jira Risk Management	50	30	20
Блокчейн (Ethereum)	70	50	16,8
Навчання (інструменти 3.1)	100	-	-
Tenable Nessus	60	180	4
Tableau (Big Data)	90	120,6	9
Azure Sentinel	100	360	3,3
Jira (оцінка ризиків)	50	30	20
Навчання (інструменти 3.2)	80	-	-
Загалом	800	1079,2	8,9

Джерело: складено автором

Загальна економія становить 1079,2 тис. грн на рік, а термін окупності:

$$800 / 1079{,}2 \times 12 = 8{,}9 \text{ місяців}$$

Найшвидше окуповуються Azure Sentinel (3,3 місяці) і Nessus (4 місяці) завдяки значному скороченню кіберзагроз, тоді як Jira має найдовший термін (20 місяців) через менший обсяг операційних втрат.

Для оцінки чистої економічної вигоди враховуємо річний період:

- ЧЕВ = Економія – Витрати = 1079,2 – 800 = 279,2 тис. грн за перший рік.
- Коефіцієнт рентабельності інвестицій (ROI): (1079,2 – 800) / 800 × 100 = 34,9%.

Ці показники свідчать про високу ефективність заходів, адже ROI 34,9% значно перевищує середній рівень для IT-інвестицій (15–20%, за даними Gartner, 2024).

Окрім прямої економії, впровадження заходів принесе довгострокові переваги:

1. Репутаційні вигоди - Зниження кіберзагроз і підвищення якості обслуговування збільшать лояльність клієнтів, що може додати 5% до доходу

5389,2 тис. грн × 0,05 = 269,5 тис. грн у 2025 році

2. Конкурентна перевага - Точні прогнози та швидке реагування дозволять утримувати ринкову частку, незважаючи на конкуренцію з великими гравцями (наприклад, SoftServe).

3. Оптимізація ресурсів - Автоматизація скоротить витрати часу персоналу на ручний аналіз ризиків із 10 годин до 2 годин на тиждень, заощаджуючи 25 співробітникам × 8 годин × 50 тижнів × 150 грн/год = 150 тис. грн на рік.

Порівняльний аналіз "до" і "після" впровадження наведено в таблиці 3.5.

Таблиця 3.5 – Порівняння ключових показників ТОВ «К2 СИСТЕМИ» до та після впровадження заходів

Показник	До впровадження	Після впровадження	Абсолютна зміна
Середня оцінка ризиків	19	10,5	-8,5 (-44%)
Час реагування на загрози, год	24	5	-19 (-79%)
Щорічні втрати від ризиків, тис. грн	1150	469,4	-680,6
Продуктивність персоналу, %	100	110	+10%
Чистий прибуток (прогноз), тис. грн	303,6	852,3	+548,7

Джерело: складено автором на основі аналізу

Втрати "до" включають кібератаки (450 тис. грн), валютні коливання (482,5 тис. грн) і затримки (200 тис. грн). "Після" враховують залишкові втрати з урахуванням ефективності заходів. Чистий прибуток зростає за рахунок економії (279,2 тис. грн) і репутаційних вигод (269,5 тис. грн): 303,6 + 279,2 + 269,5 = 852,3 тис. грн.

Запропоновані заходи забезпечать ТОВ «К2 СИСТЕМИ» зниження ризиків на 44%, економію 1079,2 тис. грн на рік при витратах 800 тис. грн і окупність за 8,9 місяців. ROI 34,9% і зростання чистого прибутку до 852,3 тис. грн у 2025 році

підтверджують економічну доцільність. Довгострокові вигоди, такі як репутація та конкурентоспроможність, додатково посилять позиції підприємства, роблячи його стійким до зовнішніх і внутрішніх загроз у динамічному ІТ-середовищі.

Висновки з 3-го розділу:

Третій розділ зосереджений на вдосконаленні управління ризиками ТОВ «К2 СИСТЕМИ» через інтеграцію інноваційних інструментів та ІТ-технологій, спрямованих на вирішення ключових проблем: кіберзагроз, валютних коливань, операційних затримок і конкуренції. У підрозділі 3.1 запропоновано використання ШІ (Darktrace), прогнозного аналізу (SAS), Jira Risk Management і блокчейну (Ethereum). Ці інструменти скорочують час реагування на кіберзагрози до 6 годин, зменшують фінансові втрати на 120,6 тис. грн і операційні затримки на 20%, а також заощаджують 50 тис. грн на правових витратах. Витрати становлять 420 тис. грн, економія – 380,6 тис. грн, окупність – 13,2 місяці.

Підрозділ 3.2 розглядає впровадження ІТ-технологій: Tenable Nessus, Tableau, Azure Sentinel і Jira. Вони знижують кіберризики на 40% (економія 540 тис. грн), підвищують точність фінансових прогнозів до 85% (120,6 тис. грн економії) і скорочують затримки на 15% (30 тис. грн). Витрати – 380 тис. грн, економія – 690,6 тис. грн, окупність – 6,6 місяців, середня оцінка ризиків падає з 19 до 10,5 (на 44%).

Підрозділ 3.3 узагальнює результати: загальні витрати – 800 тис. грн, економія – 1079,2 тис. грн, окупність – 8,9 місяців, ROI – 34,9%. Чистий прибуток зростає з 303,6 тис. грн до 852,3 тис. грн у 2025 році завдяки економії та репутаційним вигодам (269,5 тис. грн). Заходи забезпечують стійкість, конкурентоспроможність і сталий розвиток компанії в умовах динамічного ІТ-ринку.

ВИСНОВКИ

Кваліфікаційна робота присвячена дослідженню теоретичних основ і розробці практичних рекомендацій щодо вдосконалення системи управління ризиками ІТ-підприємств на прикладі ТОВ «К2 СИСТЕМИ». Проведений аналіз дозволив систематизувати знання про ризики в ІТ-сфері, оцінити поточний стан ризик-менеджменту підприємства та запропонувати комплекс заходів для підвищення його ефективності, стійкості та конкурентоспроможності.

У першому розділі визначено, що ризики в ІТ-сфері є багатогранними та динамічними, зумовленими швидкими технологічними змінами, складністю систем і залежністю від людського фактора. Ризик охарактеризовано як імовірність подій, що негативно впливають на інформаційні системи, бізнес-процеси чи фінансові показники. Класифікація ризиків (технічні, організаційні, фінансові, правові, репутаційні, зовнішні) створила основу для їх аналізу. Особливу увагу приділено кіберзагрозам і правовим ризикам через їх значний вплив. Засоби управління ризиками ІТ-проектів, такі як мозковий штурм, матриця ймовірності та впливу, моделювання Монте-Карло, гнучкі методології (Scrum) і автоматизовані системи (RiskyProject), виявилися ефективними для ідентифікації, оцінки та мінімізації загроз.

Другий розділ показав, що ТОВ «К2 СИСТЕМИ», яке з 2015 року працює на ринку ІТ-послуг, демонструє стабільне зростання: чистий дохід зріс із 2226,3 тис. грн у 2021 році до 5389,2 тис. грн у 2023 році, а прибуток – із 89,0 тис. грн до 303,6 тис. грн. Лінійно-функціональна структура забезпечує стабільність, але слабка комунікація між підрозділами та недостатня реклама створюють операційні й ринкові ризики. Діагностика виявила ключові загрози: кіберзагрози (висока ймовірність, критичний вплив), конкуренція, волатильність валютних курсів і внутрішні операційні проблеми. Карта ризиків допомогла визначити пріоритети для управління.

Третій розділ запропонував шляхи вдосконалення ризик-менеджменту. У підрозділі 3.1 обґрунтовано інтеграцію ШІ (Darktrace), прогнозного аналізу

(SAS), Jira і блокчейну, які скорочують кіберзагрози, фінансові втрати на 120,6 тис. грн і затримки на 20%. Витрати – 420 тис. грн, економія – 380,6 тис. грн, окупність – 13,2 місяці. У підрозділі 3.2 запропоновано Nessus, Tableau, Azure Sentinel і Jira, що знижують кіберризики на 40% (економія 540 тис. грн) і підвищують точність прогнозів. Витрати – 380 тис. грн, економія – 690,6 тис. грн, окупність – 6,6 місяців, ризики зменшуються на 44%. Підрозділ 3.3 узагальнив результати: загальні витрати – 800 тис. грн, економія – 1079,2 тис. грн, окупність – 8,9 місяців, ROI – 34,9%, прибуток зростає до 852,3 тис. грн у 2025 році.

Дослідження досягло мети – розроблено комплексний підхід до управління ризиками ТОВ «К2 СИСТЕМИ», який включає інноваційні інструменти та IT-технології. Впровадження заходів забезпечить зниження ризиків на 44%, економію понад 1 млн грн щорічно та підвищення конкурентоспроможності. Рекомендації мають практичне значення для IT-підприємств і можуть бути адаптовані для інших організацій у сфері інформаційних технологій.

ПЕРЕЛІК ПОСИЛАНЬ

1. ISO/IEC 31000:2018. Risk management – Guidelines. International Organization for Standardization. URL: https://www.iso.org/ru/standard/65694.html (дата звернення: 11.02.2025).
2. Kerzner H. Project Management: A Systems Approach to Planning, Scheduling, and Controlling. Wiley, 2017. 814 p.
3. Stoneburner G., Goguen A., Feringa A. Risk Management Guide for Information Technology Systems. NIST Special Publication 800-30, 2002. DOI: http://dx.doi.org/10.6028/NIST.SP.800-30r1
4. A Guide to the Project Management Body of Knowledge (PMBOK Guide). Project Management Institute, 2017. URL: https://trainupinstitute.com/wp-content/uploads/2022/03/Project-Management-Institute-A-Guide-to-the-Project-Management-Body-of-Knowledge-PMBOK%C2%AE-Guide%E2%80%93Sixth-Edition-Project-Management-Institute-2017.pdf (дата звернення: 11.02.2025).
5. Data Breach Investigations Report. Verizon, 2023. 88 p.
6. Annual Report 2022. European Data Protection Board, 2023. URL: https://www.edpb.europa.eu/our-work-tools/our-documents/annual-report/edpb-annual-report-2022_en (дата звернення: 11.02.2025).
7. Equifax Data Breach Settlement. Federal Trade Commission, 2019. URL: https://consumer.ftc.gov/consumer-alerts/2019/07/equifax-data-breach-settlement-what-you-should-know (дата звернення: 11.02.2025).
8. Hillson D. Managing Risk in Projects. Gower Publishing, 2016. 126 p.
9. Chapman C., Ward S. How to Manage Project Opportunity and Risk. Wiley, 2011. 492 p.
10. Kendrick T. Identifying and Managing Project Risk: Essential Tools for Failure-Proofing Your Project. AMACOM, 2015. 347 p.
11. State of Cybersecurity 2020. ISACA Publications, 2020. URL: https://www.isaca.org/resources/infographics/state-of-cybersecurity-2020 (дата звернення: 11.02.2025).

12. Schwaber K., Sutherland J. The Scrum Guide, 2020. URL: https://www.scrum.org/scrum-guide-2020 (дата звернення: 17.02.2025).
13. Case Study: Risk Management in Cloud Projects. IBM Press, 2018. URL: https://www.ibm.com/new (дата звернення: 17.02.2025).
14. Амоша О. І., Саломатіна Л. М. Інноваційний розвиток промислових підприємств у регіонах: проблеми та перспективи. *Економіка України*. 2017. № 3. С. 20-34
15. ТОВ «К2 СИСТЕМИ». *Офіційний сайт.* URL: https://youcontrol.com.ua/catalog/company_details/40060196/ (дата звернення: 17.02.2025).
16. Брич В. Я. Управління інноваційним розвитком підприємства : моногр. / В. Я. Брич, Х. А. Снігур, М. М. Тисько, Я. О. Шпак. – Тернопіль : ТНЕУ, 2019. 216 с.
17. Управління інноваційною діяльністю промислових підприємств: теоретико-методологічні аспекти фінансового забезпечення : монографія / І. Ю. Єпіфанова. Вінниця : ВНТУ, 2019. 384 с.
18. Sosnovska O., Dedenko L. Risk management as an instrument for providing the stable functioning of the enterprise in understanding conditions. *European Scientific Journal of Economic and Financial Innovations*, 2019. DOI: https://doi.org/10.32750/2019-0106.
19. Жигірь А. А. Різновиди підприємницьких ризиків та їх класифікація. *Ефективна економіка*, 2012. №2. URL: http://www.economy.nayka.com.ua. (дата звернення: 26.03.2025).
20. Трушкіна Н. Управління проєктними ризиками у системі ризик-менеджменту IT-компанії: теоретичні аспекти. *Економіка та суспільство*, 2023. №55. DOI: https://doi.org/10.32782/2524-0072/2023-55-88.