

Міністерство освіти і науки України  
Харківський національний університет радіоелектроніки

Факультет інформаційно-аналітичних технологій та менеджменту  
(повна назва)

Кафедра економічної кібернетики та управління економічною безпекою  
(повна назва)

## КВАЛІФІКАЦІЙНА РОБОТА Пояснювальна записка

рівень вищої освіти другий (магістерський)

Управління ризиками в контексті забезпечення економічної  
безпеки підприємства  
(тема)

Виконав:

студент 2 курсу, групи УФЕБм-22-1  
Кондрашов І.Є.  
(прізвище, ініціали)

Спеціальність 073 Менеджмент  
(код і повна назва спеціальності)

Тип програми освітньо-професійна  
(освітньо-професійна або освітньо-наукова)

Освітня програма Управління  
фінансово-економічною безпекою  
(повна назва освітньої програми)

Керівник проф. Полозова Т.В.  
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри

  
(підпис)

Полозова Т. В.  
(прізвище, ініціали)

2024 р.

Харківський національний університет радіоелектроніки

Факультет інформаційно-аналітичних технологій та менеджменту  
(повна назва)

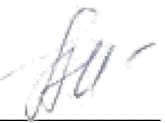
Кафедра економічної кібернетики та управління економічною безпекою  
(повна назва)

Рівень вищої освіти другий (магістерський)

Спеціальність 073 Менеджмент  
(код і повна назва)

Тип програми освітньо-професійна  
(освітньо-професійна або освітньо-наукова)

Освітня програма Управління фінансово-економічною безпекою  
(повна назва)

ЗАТВЕРДЖУЮ   
Зав. кафедри \_\_\_\_\_  
(підпис)  
« \_\_\_\_\_ » \_\_\_\_\_ 20 \_\_\_\_ р.

**ЗАВДАННЯ**  
НА КВАЛІФІКАЦІЙНУ РОБОТУ

студентові Кондрашову Ігорю Євгеновичу  
(прізвище, ім'я, по батькові)

1. Тема роботи Управління ризиками в контексті забезпечення економічної безпеки підприємства

затверджена наказом по університету від 03 листопада 2023 р. № 1292 Ст

2. Термін подання студентом роботи до екзаменаційної комісії 10 січня 2024 р.

3. Вихідні дані до роботи Наукові інформаційні джерела, періодичні видання, теоретичні та методичні розробки вчених в області забезпечення економічної безпеки підприємств, фінансова звітність досліджуваного підприємства

4. Перелік питань, що потрібно опрацювати в роботі \_\_\_\_\_

Вступ. 1 Теоретичні аспекти управління ризиками в контексті забезпечення економічної безпеки підприємства. 2 Аналіз фінансових результатів діяльності та практичних методів оцінки ризиків АТ «Інститут інформаційних технологій». 3 Напрями удосконалення управління ризиками в контексті забезпечення економічної безпеки підприємства. Висновки. Перелік джерел посилання. Додаток.

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій \_\_\_\_\_
1. Об'єкт, предмет, мета, завдання, основні наукові результати дослідження. \_\_\_\_\_
  2. Етапи процесу управління ризиками. \_\_\_\_\_
  3. Основні способи захоплення підприємства. \_\_\_\_\_
  4. Характеристика методів якісної оцінки рівня ризику. \_\_\_\_\_
  5. Характеристика методів кількісної оцінки ризиків. \_\_\_\_\_
  - 6-9. Аналіз діяльності підприємства. \_\_\_\_\_
  10. Структурно-логічна схема системи ризик-менеджменту. \_\_\_\_\_
  11. Схема процесу управління ризиками. \_\_\_\_\_
  12. Основні етапи формування системи ризик-менеджменту на підприємстві. \_\_\_\_\_
  13. Фактори, що сприяють виникненню ризику рейдерського захоплення підприємства. \_\_\_\_\_
  14. Заходи від ризику рейдерського захоплення для АТ «Інститут інформаційних технологій». \_\_\_\_\_
  15. Структурно-логічна характеристика результатів дослідження. \_\_\_\_\_

6. Консультанти розділів роботи (п.6 включається до завдання за наявності консультантів згідно з наказом, зазначеним у п.1)

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		підпис	дата

### КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Виконання першого розділу роботи	06.11.2023-16.11.2023	виконано
2	Виконання другого розділу роботи	17.11.2023-27.11.2023	виконано
3	Виконання третього розділу роботи	28.11.2023-18.12.2023	виконано
4	Оформлення роботи	19.12.2023-23.12.2023	виконано
5	Перевірка роботи на плагіат	24.12.2023-27.12.2023	виконано
6	Підготовка доповіді та ілюстративного матеріалу	28.12.2023-05.01.2024	виконано
7	Рецензування роботи	06.01.2024-09.01.2024	виконано
8	Подання роботи до екзаменаційної комісії	10.01.2024	

Дата видачі завдання 06 листопада 2023 р.

Студент \_\_\_\_\_  
(підпис)

Керівник роботи \_\_\_\_\_  
(підпис) проф. Полозова Т.В.  
(посада, прізвище, ініціали)

## РЕФЕРАТ

Кваліфікаційна робота: 93 с., 5 табл., 15 рис., 60 джерел, 1 додаток.

### УПРАВЛІННЯ, РИЗИК, СИСТЕМА РИЗИК-МЕНЕДЖМЕНТУ, ЕКОНОМІЧНА БЕЗПЕКА, РИЗИК, РЕЙДЕРСЬКОГО ЗАХОПЛЕННЯ.

Об'єктом дослідження є забезпечення економічної безпеки підприємства.

Метою дослідження є аналіз теоретичних підходів та удосконалення управління ризиками в контексті забезпечення економічної безпеки підприємства.

Розкрито економічний зміст та етапи управління ризиками в контексті забезпечення економічної безпеки підприємства. Розглянуто сутність ризику рейдерських захоплень підприємства. Здійснено огляд сучасних методів оцінки ризиків діяльності підприємства. Проаналізовано фінансові результати діяльності АТ «Інститут інформаційних технологій». Досліджено практичні методи оцінки ризиків, що використовуються в АТ «Інститут інформаційних технологій». Запропоновано концептуальний підхід до формування системи ризик-менеджменту на підприємстві. Розроблено практичні рекомендації щодо управління ризиком рейдерського захоплення для АТ «Інститут інформаційних технологій». Наведено структурно-логічну характеристику результатів дослідження.

## **ABSTRACT**

Master thesis: 93 p., 5 tables, 15 fig., 60 sources, 1 exhibit.

MANAGEMENT, RISK, RISK MANAGEMENT SYSTEM, ECONOMIC SECURITY, RISK, RAIDER CAPTURE.

The object of the research is to ensure the economic security of the enterprise.

The purpose of the research is the analysis of theoretical approaches and improvement of risk management in the context of ensuring the economic security of the enterprise.

The economic meaning and stages of risk management in the context of ensuring the economic security of the enterprise are disclosed. The essence of the risk of raiding of the enterprise was considered. An overview of modern methods of risk assessment of enterprise activity was carried out. The financial results of JSC «Institute of Information Technologies» were analyzed. The practical methods of risk assessment used in JSC «Institute of Information Technologies» are studied. A conceptual approach to the formation of a risk management system at the enterprise is proposed. Practical recommendations on the management of the risk of raiding have been developed for JSC «Institute of Information Technologies». The structural and logical characteristics of the research results are given.

## ЗМІСТ

Вступ.....	6
1 Теоретичні аспекти управління ризиками в контексті забезпечення економічної безпеки підприємства.....	9
1.1 Економічний зміст та етапи управління ризиками в контексті забезпечення економічної безпеки підприємства.....	9
1.2 Сутність ризику рейдерських захоплень підприємства.....	14
1.3 Огляд сучасних методів оцінки ризиків діяльності підприємства.....	25
2 Аналіз фінансових результатів діяльності та практичних методів оцінки ризиків АТ «Інститут інформаційних технологій».....	35
2.1 Загальна характеристика підприємства.....	35
2.2 Аналіз фінансових результатів діяльності підприємства.....	38
2.3 Практичні методи оцінки ризиків на підприємстві.....	46
3 Напрями удосконалення управління ризиками в контексті забезпечення економічної безпеки підприємства.....	57
3.1 Концептуальний підхід до формування системи ризик-менеджменту на підприємстві.....	57
3.2 Рекомендації щодо управління ризиком рейдерського захоплення для АТ «Інститут інформаційних технологій».....	68
3.3 Структурно-логічна характеристика результатів дослідження.....	75
Висновки.....	78
Перелік джерел посилання.....	86
Додаток А Копії публікацій.....	94

## ВСТУП

У сфері економічної безпеки підприємств, ризики володіють як теоретичним, так і практичним значенням, становлячи важливу складову системи управління. Розвиток ринкових відносин підсилює невизначеність і невпевненість у досягненні очікуваного кінцевого результату, що призводить до зростання ризиків. Тому виникає потреба в застосуванні відповідних методів оцінки та мінімізації можливих втрат для різних видів діяльності підприємств.

Різні види організацій можуть стикатися з різноманітними видами ризиків: комерційними, фінансовими, інформаційними, інвестиційними, екологічними тощо. На сьогоднішній день існуючі системи класифікації ризиків дозволяють обрати відповідні стратегії управління ризиками, підвищуючи тим самим безпеку організації як системи. Однак кожна з відомих стратегій управління ризиками, як правило, забезпечує максимальний ефект лише для конкретного виду ризику, що вимагає комплексного застосування всіх стратегій або їх використання різною мірою в поєднаннях, а також зміни управлінської поведінки в цій ситуації.

Основні напрями підвищення безпеки організації як системи вимагають певних витрат на наукове і методичне забезпечення. Зміна управлінської поведінки передбачає оцінку «особистої прийнятності» ризикової ситуації для конкретного керівника і можливості визначення ним ступеня ризику. Ризиками можна управляти за допомогою різних заходів, які дозволяють до певної міри прогнозувати настання ризикової події та знижувати ступінь ризику. Все вищезазначене свідчить про необхідність глибшого вивчення теоретичних основ управління ризиками в системі економічної безпеки підприємства та можливостей їх оцінки при різних видах ризиків.

Вагомий внесок у дослідження теоретичних і практичних аспектів управління підприємствами в умовах невизначеності та ризику внесли такі науковці: І. Балабанова, І. Бланк, П. Верченко, В. Вітлінський, І. Отенко, О. Перепелюкова, Т. Полозова, Ю. Романенков, Л. Соколова, С. Степаненко, О. Мурзабулатова, І. Шейко та інші.

Об'єктом дослідження є забезпечення економічної безпеки підприємства.

Предметом дослідження є методи управління ризиками в контексті забезпечення економічної безпеки підприємства.

Метою дослідження є аналіз теоретичних підходів та удосконалення управління ризиками в контексті забезпечення економічної безпеки підприємства.

Завдання дослідження:

- розкрити економічний зміст та етапи управління ризиками в контексті забезпечення економічної безпеки підприємства;
- розглянути сутність ризику рейдерських захоплень підприємства;
- здійснити огляд сучасних методів оцінки ризиків діяльності підприємства;
- проаналізувати фінансові результати діяльності АТ «Інститут інформаційних технологій»;
- дослідити практичні методи оцінки ризиків, що використовуються в АТ «Інститут інформаційних технологій»;
- запропонувати концептуальний підхід до формування системи ризик-менеджменту на підприємстві;
- розробити практичні рекомендації щодо управління ризиком рейдерського захоплення для АТ «Інститут інформаційних технологій»;
- навести структурно-логічну характеристику результатів дослідження.



Інформаційною базою для проведення дослідження були періодичні наукові видання, законодавство України, фінансова звітність підприємства, що досліджується.

Під час дослідження були використані такі методи аналізу, синтезу, порівняння, зіставлення, системного підходу, графічний.

Основні наукові результати дослідження:

– запропоновано концептуальний підхід до формування системи ризик-менеджменту на підприємстві;

– удосконалено основні етапи формування системи ризик-менеджменту на підприємстві.

Практична значущість отриманих результатів полягає у тому, що запропоноване організаційне забезпечення дозволить впровадити на підприємстві ефективну систему управління ризиком рейдерського захоплення, перевагою якої є врахування реального рівня ризику та характеристик діяльності в умовах конкретного підприємства.

Апробація результатів дослідження. Основні теоретичні положення і практичні результати проведених досліджень, висновки і рекомендації, які викладені в роботі, доповідались на IV Міжнародній науково-практичній конференції «Сучасні стратегії економічного розвитку: наука, інновації та бізнес-освіта» (Харків, 2023).

Публікації. Результати досліджень, проведених у роботі, опубліковано у 2 наукових працях, у тому числі 1 стаття у колективній монографії та 1 тези конференції.

# **1 ТЕОРЕТИЧНІ АСПЕКТИ УПРАВЛІННЯ РИЗИКАМИ В КОНТЕКСТІ ЗАБЕЗПЕЧЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА**

## **1.1 Економічний зміст та етапи управління ризиками в контексті забезпечення економічної безпеки підприємства**

Управління бізнесом – це складний процес, який включає в себе розробку та прийняття рішень, від результатів яких залежить загальна продуктивність діяльності економічного суб'єкта на ринку. Це вимагає врахування умов зовнішнього оточення, які складаються з факторів, що впливають на роботу підприємства і, відповідно, на його економічну безпеку. Ці фактори можуть бути як позитивними, так і негативними для учасника ринку. Негативний вплив зовнішніх факторів може призвести до нестабільності позиції підприємства, зниження його економічної безпеки та виникнення кризи в його діяльності [1-4].

Сутність поняття «економічна безпека» розглядається різними науковцями індивідуально. Вона може бути визначена як стан підприємства, що забезпечує йому здатність протидіяти несприятливим зовнішнім впливам. Економічна безпека також охоплює корпоративні ресурси та підприємницькі можливості, гарантуючи їхнє ефективне використання для стабільного функціонування та розвитку [2].

Управління ризиками на підприємстві полягає у передбаченні та управлінні можливістю виникнення ризику, визначенні ймовірних масштабів його прояву та розробці заходів для попередження або мінімізації втрат, пов'язаних із його реалізацією. Управління ризиками можна вважати одним із інструментів забезпечення економічної безпеки підприємства. Процес управління ризиками передбачає послідовність дій, що складаються з певних етапів. З урахуванням рекомендацій [3-6] можна виокремити ці етапи в контексті забезпечення економічної безпеки (рис. 1.1).

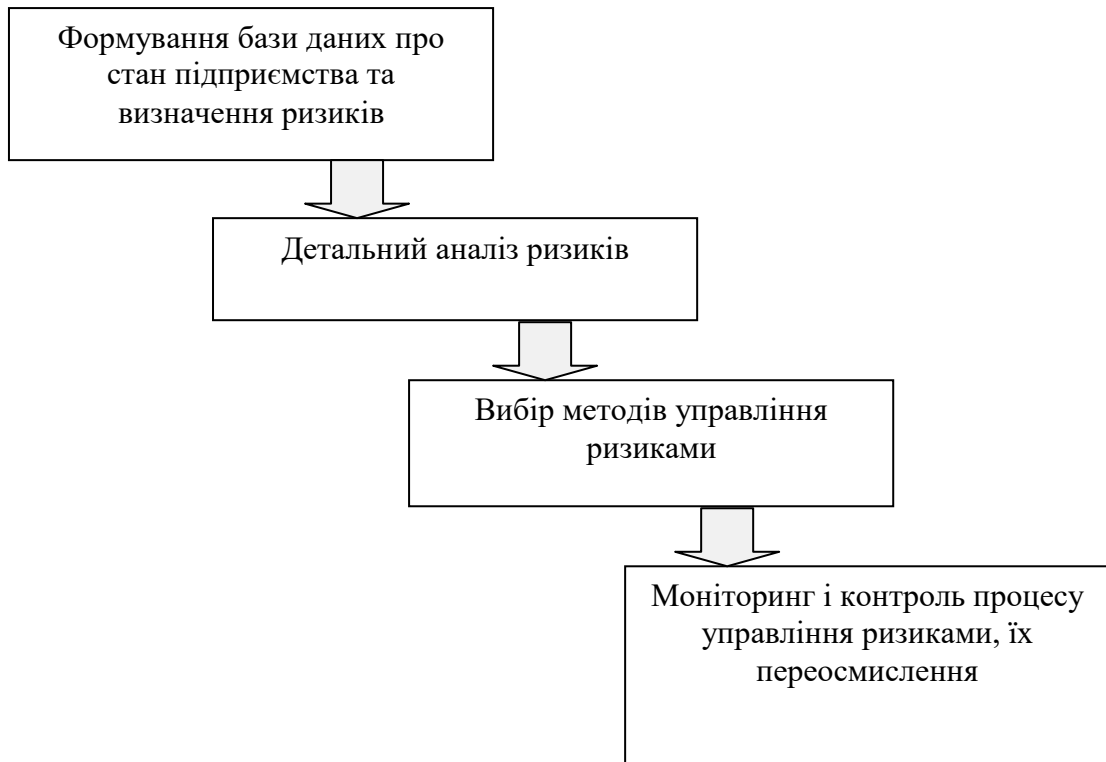


Рисунок 1.1 – Етапи процесу управління ризиками в контексті забезпечення економічної безпеки

Етап 1. Формування бази даних та ідентифікація ризиків. На цьому етапі створюється інформаційна база даних, що містить повну інформацію про стан підприємства. Це дозволяє дослідникові визначити основні джерела ризику, які можуть бути як очевидними, так і потенційними загрозами для діяльності підприємства.

Етап 2. Детальний аналіз ризиків. На даному етапі проводиться дослідження існуючих ризиків та визначення ймовірності їх реалізації у процесі підприємницької діяльності суб'єкта ринку. Для кількісної оцінки ризику використовуються дві основні характеристики: величина можливих втрат у разі небажаної події та ймовірність виникнення такої події.

Етап 3. Вибір методів управління ризиками. Методи управління ризиками поділяють на профілактичні та страхувальні. Профілактичні заходи включають відмову від ризику, мінімізацію ризику, диверсифікацію,

лімітування та передачу ризику іншим особам чи організаціям. Страхування ризиків може бути внутрішнім або зовнішнім.

Етап 4. Моніторинг і контроль процесу управління ризиками, їх переосмислення. Цей етап передбачає дослідження доцільності реалізованих заходів управління ризиками на підприємстві. Важливо визначити ефективність вжитих заходів, їх очікувану ефективність та практичну можливість реалізації протягом визначених термінових рамок.

Управління ризиками в контексті забезпечення економічної безпеки підприємства є важливою складовою стратегічного управління і включає в себе ряд економічних аспектів. Основний економічний зміст управління ризиками може бути визначений такими напрямками [7-10]:

- мінімізація втрат. Один з центральних аспектів управління ризиками – це зменшення можливих втрат для підприємства. Це може включати в себе ризики фінансові, операційні, репутаційні тощо. Шляхи мінімізації втрат включають в себе ретельний аналіз ризиків, їх ідентифікацію та розробку стратегій для їх управління;

- оптимізація фінансових ресурсів. Ефективне управління ризиками дозволяє підприємству економічно розподіляти свої фінансові ресурси. Вирішення проблем, пов'язаних із збитками та фінансовими втратами, дозволяє зберігати та використовувати ресурси для стратегічного розвитку;

- забезпечення стійкості підприємства. Управління ризиками спрямоване на створення стійкості та витривалості підприємства перед різноманітними зовнішніми та внутрішніми загрозами. Це важливо для забезпечення економічної безпеки та надійності підприємства в умовах невизначеності;

- збереження репутації. Ефективне управління ризиками включає в себе заходи для запобігання можливим загрозам для репутації підприємства.

Репутаційні ризики можуть серйозно вплинути на ставлення клієнтів, інвесторів та партнерів до підприємства;

– сприяння інноваціям та розвитку. Управління ризиками може стимулювати інновації та розвиток. Ретельне вивчення ризиків, пов'язаних з новими проектами чи напрямками, дозволяє підприємству приймати обґрунтовані рішення та забезпечує стійке зростання;

– відповідність законодавчим вимогам. Управління ризиками включає в себе відстеження та виконання законодавчих вимог. Відповідність правовим стандартам сприяє зменшенню ризиків правопорушень та відповідних фінансових санкцій.

Економічне управління ризиками покликане не лише захищати підприємство від потенційних загроз, але й створювати фундамент для стабільності, розвитку та конкурентоспроможності в економічному середовищі.

Зв'язок між управлінням ризиками та економічною безпекою підприємства полягає в тісному взаємозв'язку між стратегічними рішеннями, фінансовою стійкістю та здатністю підприємства впоратися з потенційними невдачами чи негативними впливами зовнішнього середовища. Основні аспекти цього зв'язку включають [11-19]:

– превентивна орієнтованість. Управління ризиками передбачає превентивні заходи, спрямовані на уникнення можливих проблем. Це дозволяє підприємству попереджувати або пом'якшувати негативні економічні наслідки, що можуть виникнути внаслідок непередбачуваних обставин;

– фінансова стійкість. Ефективне управління ризиками забезпечує збереження фінансової стійкості підприємства. Зменшення фінансових ризиків та витрат дозволяє утримати необхідні ресурси для ефективної діяльності та розвитку;

– стабільність виробничих процесів. Управління ризиками сприяє стабільності виробничих процесів та допомагає уникнути непередбачуваних перерв у виробництві. Це забезпечує економічну безпеку шляхом забезпечення плавності операцій;

– репутаційний аспект. Негативні події, які можуть виникнути через недоуправління ризиками, можуть впливати на репутацію підприємства. Репутаційні ризики можуть мати прямий вплив на довіру клієнтів, інвесторів та партнерів, а це безпосередньо пов'язано з економічною безпекою;

– адаптація до змін в зовнішньому середовищі. Управління ризиками надає підприємству інструменти для ефективної адаптації до змін у зовнішньому середовищі. Це особливо важливо в умовах швидких змін на ринку та інших економічних умовах;

– стратегічне планування. Управління ризиками включає в себе стратегічне планування, що враховує можливі загрози та можливості. Це допомагає підприємству розробляти ефективні стратегії, які сприяють економічній безпеці та конкурентоспроможності;

– ефективна внутрішня контрольна система. Управління ризиками включає в себе встановлення ефективної внутрішньої контрольної системи, що дозволяє вчасно виявляти та вирішувати можливі проблеми, забезпечуючи економічну безпеку.

У цілому, управління ризиками та економічна безпека взаємодіють, формуючи цілісний підхід до забезпечення стійкості та процвітання підприємства в динамічному економічному середовищі.

Таким чином, управління ризиками на підприємстві є складним процесом, що базується на виваженому визначенні джерел ризику та включає чотири основні етапи, які виконуються в певній послідовності. Майбутні дослідження можуть фокусуватися на визначенні найбільш актуальних ризиків для швейних підприємств і обґрунтуванні вибору методів для їх зменшення.

## 1.2 Сутність ризику рейдерських захоплень підприємства

Загалом рейдерство розглядається як прояв недоліків у політичних та правових структурах влади в країні, недосконалості чинного законодавства, відсутності належних умов для захисту бізнесу, прав власників та рівноправної конкуренції. Існування явища рейдерства в Україні ще раз підкреслює глибокі системні проблеми нашої держави [20, 21].

Основною причиною попиту на рейдерські послуги вважається початок переходу України до ринкових відносин та активний процес «глобального» перерозподілу власності.

Згідно з оцінками експертів, на сьогоднішній день рейдери використовують різноманітні методи, такі як психологічний тиск, шантаж, фальсифікація документів, корупція в силових структурах, для створення умов для рейдерських нападів, захоплення та перерозподілу власності в рамках законодавства. Вже 3,7 тисячі суб'єктів господарювання в Україні стали жертвами рейдерських атак. Щорічний обсяг рейдерського перерозподілу власності складає в середньому від 2 до 3 мільярдів доларів США [20].

Термін «рейдерство» відноситься до ситуацій, коли різноманітні випадки рейдерства спостерігаються в різні періоди і майже в усіх країнах з ринковою економікою. Рейдерство з'явилося у Великобританії, коли британські військові кораблі самостійно виконували військові завдання, захоплюючи торгові кораблі інших країн. У сучасному контексті, рейдерство, яке означає руйнування компанії та перерозподіл її власності та корпоративних прав, виникло у США у 60-70-х роках XX століття. За даними експертів, першим рейдером став Джон Рокфеллер, засновник Standard Oil, який використовував різні методи для покупки акцій своїх конкурентів з

метою зміцнення та розвитку свого власного бізнесу вже наприкінці ХІХ століття [21].

Кілька років тому рейдерство активно розвивалося в російській федерації, негативно впливаючи на всі аспекти розвитку російської економіки. Втім, сьогодні, завдяки чіткому законодавству, рівень рейдерства в країні суттєво зменшився. Важливо зазначити, що через це багато структур, спеціалізованих на рейдерстві, перепрофілювали свою діяльність із росії в Україну. За оцінками експертів, до 50% рейдерського ринку країни вже контролюється російськими рейдерами [21].

Історія рейдерства в Україні розділяється на два етапи. Перший етап – це початок 90-х років до 2000 року, коли компанії були захоплені відкритими кримінальними методами, часто з використанням фізичної сили. Другий етап, який почався у 2000 році і триває до сьогодні, характеризується напівлегальним захопленням компаній, більш законними методами боротьби та активним опором рейдерству [21].

Рейдери – це група висококваліфікованих фахівців, які спеціалізуються на захопленні компанії або перехопленні контролю за допомогою спеціально спланованого бізнес-конфлікту. Основна мета рейдерства – підкорення великого бізнесу, великих компаній, підприємств, захоплення великих площ, земельних ділянок, обладнання та нерухомості. Рейдерство можна поділити на наймані структури, які працюють під керівництвом великої бізнес-структури, і на «вільних авантюристів» – незалежні команди. У сучасних умовах експерти розрізняють рейдерів на білих і чорних [20-24].

Білі рейдери використовують метод корпоративного шантажу в межах чинного законодавства. В Україні їх зустрічається досить рідко, і вони є більш характерними для країн з розвиненою економікою та високою бізнес-культурою. Такий тип рейдерства прямо чи опосередковано, через процедуру банкрутства, позбавляє керівництво неефективного управління, підвищує



результативність бізнес-процесів та сприяє працевлаштуванню висококваліфікованих фахівців тощо.

Початок атаки зазвичай полягає в скуповуванні акцій за високими цінами, достатньо 10-15% акцій, щоб ініціювати проведення зборів акціонерів і впровадження необхідних змін, наприклад, зміни керівництва підприємства. У більшості випадків керівники відмовляються від переговорів, і тоді рейдери переходять до чорних дій.

Чорні рейдери застосовують незаконні методи (захоплення, фальсифікація документів, реєстрація компаній на імена маріонеток, корупція в силових структурах, чиновників, суддів і судових виконавців, фізичне видалення осіб, які заважають). Наслідки дій чорних рейдерів в Україні мають негативний вплив, оскільки вони безпосередньо порушують право особи на власність та інші основні права, які гарантуються Конституцією України (право на життя, здоров'я, честь, гідність тощо).

У період захоплень чорні рейдери використовують методи скуповування акцій і облигацій, ініціюють процедури банкрутства, незаконний доступ до реєстру акціонерів, значне заниження вартості підприємства та інші тактики. Особливий інтерес представляють державні та приватні підприємства, які володіють нерухомістю. Схожу оцінку можна висловити щодо явища «гринмейл» – блокування та перешкоджання роботі підприємства через шантаж власників невеликих пакетів акцій.

У контексті рейдерства в Україні агресорами можуть бути різні учасники. Це можуть бути спеціалізовані компанії, які проводять рейдерські атаки на замовлення бізнесменів-конкурентів. Також до агресорів можна віднести незалежні команди, які самостійно займаються рейдерством. Варто відзначити, що в Україні близько 90% рейдерських атак завершуються успішно. Це свідчить про те, що багато підприємств не готові до такого розвитку подій [21].

Інші учасники не є серйозною загрозою для підприємства, принаймні тому, що для успішної реалізації їхніх проектів вони потребують значних матеріальних і адміністративних ресурсів.

Олігархи та фінансові групи мають значні фінансові ресурси і використовують адміністративні, судові та силові ресурси у своїх діях. Для них критично важливо скасувати судові рішення, корумпувати судових виконавців і місцеві силові структури. В результаті, законні власники підприємства, після успішної силової операції перехоплення управління, яку проводять судові виконавці під захистом людей у «масках», опиняються поза воротами і змушені відстоювати свої права, оскаржуючи незаконні дії своїх противників.

Інвестиційні компанії виступають менш агресивно і діють менш жорстко. Вони займаються активами, які є предметом безкінечних судових справ, і які важко продати за максимально високу ціну через їх проблемний статус. Ці компанії вдаються до агресивних дій лише тоді, коли корпоративний конфлікт не може бути вирішений мирним шляхом.

Можливості і тактика інвестиційних компаній-посередників в основному залежать від можливостей їх замовників. Зазвичай на початковій стадії вони мають обмежені кошти і рідко використовують значний адміністративний, судовий або силовий ресурс, оскільки ці інструменти є для них досить вартісними. Однак, якщо замовником є велика організація, то можливості посередника значно збільшуються.

Професійні гринмейлери є найбільш небезпечними, оскільки вони виступають як учасники проекту щодо ворожого поглинання, приховуючи головного гравця або реалізуючи власну стратегію, створюючи передумови для ворожого поглинання. Вони діють досить жорстко, свідомо створюючи собі агресивний імідж, який зазвичай стає своєрідним PR-проектом.

Структура рейдерства та основні методи захоплення підприємства.

Ринок рейдерських послуг в Україні представлений безліччю середніх та дрібних юридичних фірм. Основні складові структури включають:

- відділ, що збирає та аналізує інформацію;
- відділ, що безпосередньо працює над реалізацією проектів щодо ворожого поглинання (рейдери);
- юридичний відділ.

Основне завдання першого та третього відділів – це збір максимальної кількості компрометуючої інформації. Юридичний відділ детально вивчає отримані документи та розробляє юридичні стратегії для агресорів щодо цільової компанії.

Відділ, який безпосередньо займається виконанням проектів щодо придбання, розробляє свою власну стратегію дій на основі результатів роботи двох вищезазначених відділів. Відсутність необхідної інформації та компрометуючих матеріалів становить серйозну перешкоду і може призвести до відмови від намірів. Таким чином, конфіденційність інформації та знання чинного законодавства серйозно обмежують коло потенційних агресорів, забезпечуючи компанії власний захист.

Важливий факт, що лише 25 років становить середній вік рейдерів. Зазвичай рейдер отримує починаючи від 20 і закінчуючи 50 відсотками вартості проекту. Структура рейдерства діє на основі проектного менеджменту: команду та варіанти атаки вибирають під кожен конкретний проект.

На рис. 1.2 наведено основні способи захоплення підприємства (складено на основі [20-24]).



Рисунок 1.2 – Основні способи захоплення підприємства

Придбання акцій може здійснюватися шляхом відмовної купівлі-продажу акцій для отримання блокуючого або контрольного пакету акцій. Додаткова емісія акцій або аналогічний метод придбання підприємства. Банкрутство, яке є витратним методом придбання, передбачає «придбання» кредитної заборгованості від бізнес-партнерів, укладання угод з банківськими та іншими фінансовими організаціями, формування конкурсної комісії і т. д.

Реприватизація, яка є законним способом придбання, включає в себе анулювання судового рішення з наступним переглядом процесу приватизації. Цивільний позов може бути ініційований як акціонерами, так і представниками держави (з метою подальшого перерозподілу власності).

Корпоративний шантаж (грінмейлінг, юридичний терор, послуга, яка сприяє придбанню або рейдерству) часто є самостійним, високоприбутковим видом бізнесу, який не передбачає здійснення контролю над компанією.

Допемісія – це ключовий метод захоплення контролю над підприємством, який використовується для відсторонення непотрібного міноритарного акціонера.

Силове захоплення включає в себе залучення силових структур (спеціальних підрозділів правоохоронних органів, приватних охоронних служб) та використання фальшивого судового рішення.

Встановлення контролю над керівництвом (застосовується до державних підприємств, господарських товариств, основним акціонером яких є держава, реалізується через підкуп, шантаж або загрози керівництву компанії).

Фіктивне банкрутство (порушення діючого законодавства про банкрутство, штучне створення податкової та кредиторської заборгованості, висунення кандидатури свого керівника).

Корупція, яка є необхідною умовою рейдерства, особливо важлива під час перерозподілу державної власності.

Схема проведення рейдерських операцій представлена на рис. 1.3.

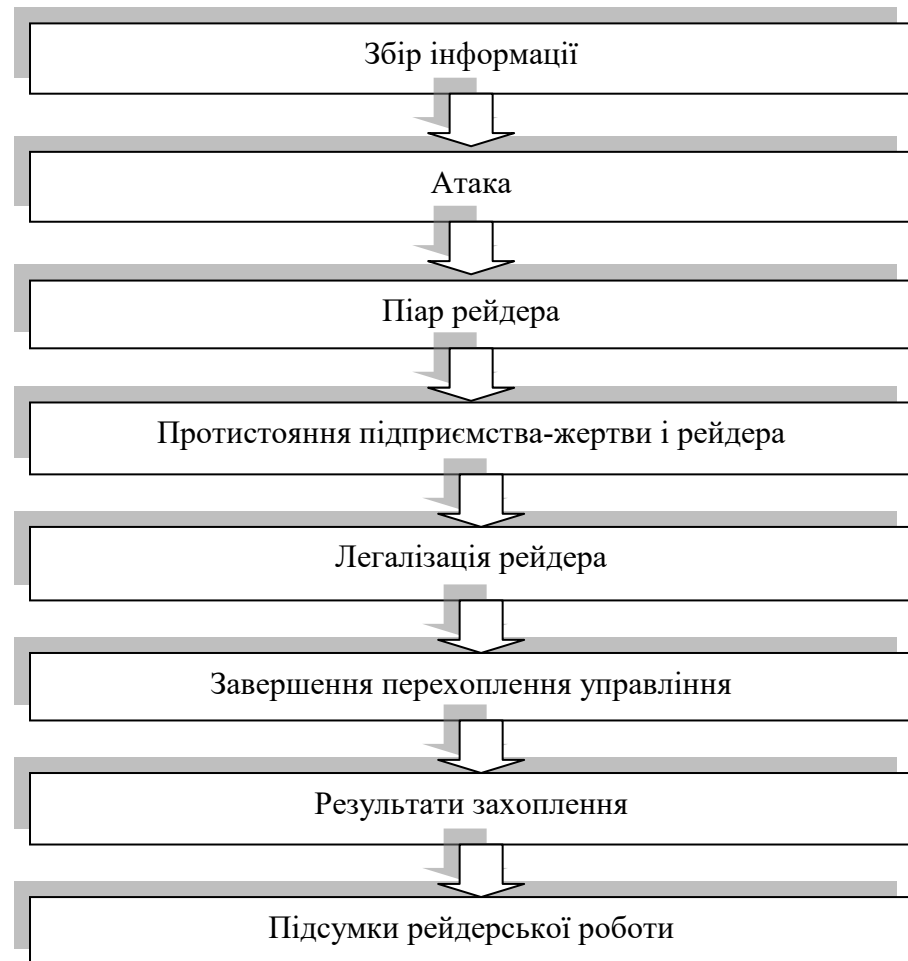


Рисунок 1.3 – Схема проведення рейдерських операцій

Збір інформації є ключовим етапом підготовки для рейдерської атаки. Рейдер накопичує дані про потенційну жертву, оцінює її привабливість та рентабельність операції, визначає напрямки атаки і запускає «пробну кулю» для перевірки здатності підприємства відстояти себе. Тривалість цього етапу залежить від розмірів цільового підприємства та намірів рейдера, варіюючись від 1 до 6-7 місяців.

Кожна атака створюється персонально для кожного підприємства з урахуванням необхідної корекції. Фахівці вважають, що майже на кожному підприємстві існують слабкі місця для рейдерських атак. Перш за все, якщо

контрольний пакет акцій (30 відсотків) не сконсолідовано, рейдер може скористатися трьома «заціпками». Він може викупити акції в працівників, тиснути на менеджмент і через номінального акціонера заволодіти (отримати контроль) підприємством. По-друге, це старі, усіма забуті, борги підприємства. По-третє, незадоволені дрібні акціонери та звільнені працівники або навіть керівники.

Рейдер, використовуючи судові вироки, здобуває контроль над компанією або відчужує її активи (завалює власників позовами від імені акціонерів через різні порушення, подає до арбітражу заздалегідь придбані борги цільового підприємства, ініціює різні перевірки за «сигналами» акціонерів та на вигаданих підставах відкриває кримінальні справи проти керівництва). Тривалість цього етапу може коливатися від одного дня до кількох років, в залежності від зусиль жертви у протистоянні.

Піар рейдера — це стратегічне використання інтриг, змов, маніпулювання громадською думкою та інші тактики для досягнення поставленої мети. Рейдери часто застосовують тактику «розколу» керівного органу, викликають внутрішні суперечності, вдаються до шантажу, тиску на членів сімей акціонерів, чернуть в засобах масової інформації та створюють конфліктну ситуацію з органами виконавчої влади. Рейдер використовує всі доступні засоби, щоб зібрати навколо себе невдоволених дрібних акціонерів і створити умови для приходу до влади штучно створеної опозиції.

Конфронтація між підприємством-жертвою та рейдером полягає спробах власників підприємств та його керівників захиститися. На цьому етапі обидві сторони (керівництво та рейдери) прагнуть продемонструвати підконтрольну їм кредиторську заборгованість підприємства та отримати в будь-якому підконтрольному суді рішення, що блокує виконання угод з активами підприємства. Проте на цьому етапі підприємство зазвичай програє

через більший час, який рейдер витрачає на підготовку та створення перешкод.

Процес легалізації рейдера включає створення формальних умов для захоплення підприємства. Рейдер створює альтернативний орган управління, який максимально дотримується всіх формальних процедур та вимог діючого законодавства. Це включає організацію позачергових зборів акціонерів, переобрання ради директорів та генерального директора. Звісно, власники можуть перешкоджати таким зборам, але у випадку їх проведення можуть оскаржити їх легітимність.

Керуючи значущим пакетом акцій, рейдер створює враження відправки вимоги до діючого органу управління про проведення позачергових акціонерних зборів (відправляє чистий аркуш у конвертах з повідомленням). Це призводить до ігнорування органом управління вимог акціонерів, і рейдер отримує право провести збори, виключивши своїх конкурентів (з обмеженим доступом акціонерів). Цей процес триває до тих пір, поки на зборах з таким самим порядком денним не набереться кворум, і нова рада директорів переобирається більшістю голосів.

Наступним кроком є подання одним із акціонерів позову до суду з вимогою визнання рішення зборів недійсним. Після розгляду справи суд виносить рішення про відмову. В результаті рейдер отримує документ, який суд визнає законним і правомірним засіданням. Завершення процесу перехоплення управління. Паралельний орган управління, створений рейдером, фактично бере під контроль цільове підприємство. На цьому етапі, як правило, починається жорстка інформаційна та адміністративна боротьба.

Результати захоплення. Якщо атака була успішною, подальші дії рейдера залежать від цілей та завдань рейдерської операції. У випадку досягнення цілі (захоплення активів підприємства для отримання значного



прибутку) відбуваються угоди про продаж нерухомості, обладнання, транспортних засобів та іншого майна підприємства.

Якщо рейдерська операція проводилася для захоплення бізнесу взагалі, то захопники вживають ряд заходів для його утримання. Придбане підприємство приєднується до холдингу, що призводить до створення нової вертикалі управління та відповідної структури безпеки.

Висновки з рейдерської діяльності. Рейдери вказують, що головним елементом витрат у бюджеті захоплення є корупція серед правоохоронних органів та суддів. Згідно з експертними оцінками, загальна вартість рейдерської операції з захоплення підприємства варіюється від 100 тисяч до 1 мільйона доларів США.

Стратегії боротьби з рейдерством. Давні римляни казали: «Хто попереджений, той у безпеці». Однак на практиці дуже важко виявити реальне захоплення, і це є основною причиною затримки реакції власника. Не існує універсального методу захисту підприємства від рейдерства. Проте, шанси рейдера на успішну атаку значно зменшуються, якщо власник своєчасно створює кілька ліній оборони, ретельно структурує систему власності та розробляє методи прийняття рішень.

Ефективність заходів проти захоплення підприємства рейдерами, як показує практика, найвища при впровадженні превентивних заходів. Стратегічна мета такого захисту полягає в максимальному підвищенні вартості підприємства для того, щоб зробити рейдерську атаку нерентабельною та недоцільною. Власникам слід здійснити заходи, які переключать інтерес потенційного рейдера з корпоративного захоплення на цивілізований механізм об'єднання та поглиблення. Для цього потрібно провести системну реструктуризацію бізнесу, щоб створити систему володіння та управління найбільш привабливими активами, яка зробить захоплення підприємства рейдерами нерентабельним бізнесом.

Важливо підкреслити, що ефективність боротьби з рейдерством буде досягнута лише у випадку введення кримінальної відповідальності за замовлення, організацію та вчинення неправомірних дій, які мають ознаки рейдерства.

### 1.3 Огляд сучасних методів оцінки ризиків діяльності підприємства

Більшість сучасних науковців, як вітчизняних, так і зарубіжних, класифікують методи оцінки підприємницького ризику на дві групи: кількісні або об'єктивні (математичні, статистичні та ймовірнісні, аналітичні) і якісні або суб'єктивні (моделювання, оптимізація та теорія гри, методи стохастичного програмування, аналогів). Інші автори наводять перелік методів загалом, розглядаючи окремо статистичний, експертний та розрахунково-аналітичний [25-34].

Якісний аналіз ризику є одним з найважчих завдань в економічній ризикології. Він вимагає глибокого розуміння як теорії економіки, бізнесу, фінансів, так і ряду спеціалізованих дисциплін, необхідних для підготовки конкурентоспроможного спеціаліста в певній області. Також потрібен певний практичний досвід в обраній сфері економічної активності. Під час якісного аналізу ризику виявляються джерела та причини ризику. Основне завдання якісної оцінки полягає в визначенні потенційних видів ризиків та факторів, які впливають на рівень ризиків при виконанні певного виду діяльності. На цьому етапі важливо виявити всі можливі обставини і детально описати всі потенційні ризики. Це означає, що в результаті необхідно мати чітке уявлення про всі можливі ризики, виявлені потенційні зони ризику, а також негативні наслідки або додаткові переваги, що можуть виникнути в результаті реалізації певного рішення. Цей аналіз проводиться в кількох

основних напрямках. Перший напрям передбачає порівняння очікуваних позитивних результатів (доходів) вибору конкретного напрямку підприємницької діяльності з можливими наслідками (втратами, збитками), серед яких виділяють: фінансові, матеріальні, часові, соціальні, реалізаційні, екологічні і морально-психологічні. Їх порівнюють з імовірними результатами, які отримає підприємство при розвитку певного напрямку діяльності [26].

Другий напрям аналізу ризику полягає у визначенні впливу рішень, прийнятих керівництвом підприємства під час формування стратегії, на інтереси та поведінку інших учасників ринку, оскільки вони не існують ізольовано, а є частиною ринкового середовища. На цьому етапі також визначаються ті суб'єкти, для яких виникнення певного виду ризику буде корисним.

За допомогою якісного аналізу необхідно виявити негативні наслідки ризику в усіх областях діяльності підприємства. Наприклад, ризик пожежі може вплинути на технологічний процес, виробничо-господарську, фінансово-економічну та соціальну діяльність, і це відбудуватиметься в певній послідовності.

Аналіз ризиків дозволяє не тільки відстежувати їх еволюцію та області розповсюдження, але й виявляти негативні наслідки кумуляції ризиків, тобто їх взаємодію та накопичення. Для цього потрібно використовувати найрізноманітніші джерела інформації та застосовувати найефективніші методи кваліфікованого аналізу ризиків.

Інформаційне забезпечення відіграє важливу роль у аналізі ризику. Воно не лише служить джерелом даних, але й є інструментом зменшення ризику. Однак іноді більш доцільно оперувати обмеженою інформацією, ніж витратити великі ресурси на отримання повної та вичерпної інформації. Обмеження ресурсів або відсутність засобів для обробки інформації,

неточність через використання приблизних методів оцінки даних негативно впливають на визначення ризиків.

Важливо зазначити, що якісний аналіз ризиків також передбачає кількісну оцінку. Тобто процес проведення якісного аналізу має включати не тільки опис специфічних видів ризиків для даного проекту, виявлення можливих причин їх виникнення, аналіз очікуваних наслідків їх реалізації та пропозиції щодо мінімізації виявлених ризиків, але й вартісну оцінку потенційних збитків та всіх заходів, спрямованих на мінімізацію ризиків даного проекту.

Вирішальним аспектом при якісному аналізі оцінки ризику є встановлення його рівня, а точніше визначення допустимої межі для компанії. Рівень ризику - це оцінка відношення масштабу очікуваних втрат до вартості активів підприємства, а також ймовірності виникнення цих втрат. При проведенні оцінки рівня ризику будь-яким способом ключовим параметром є варіативність наслідків конкретного рішення. Варіативність - це кількість відхилень, які виникають в ряду значень при відхиленні від середнього значення. Основний принцип рівня ризику: чим вища варіативність, тим вищий рівень ризику. Якісна оцінка призначена для визначення потенційних видів ризику, факторів, які впливають на його рівень при проведенні певного виду бізнес-діяльності. Якісний аналіз також включає методологічний підхід до кількісної оцінки припустимого рівня ризику. Кінцеве рішення може бути прийняте лише при інтегральній його оцінці.

Так, А.О. Старостіна, В.А. Кравченко наголошують на можливості при якісній оцінці рівня ризику оцінювати можливі наслідки подій та відповідну ймовірність потенційних подій [35].

Таблиця 1.1 – Характеристика методів якісної оцінки рівня ризику

Метод якісної оцінки	Ступінь рівня ризику	Сутність	Переваги методу	Недоліки методу
Аналіз наслідків	Високий, помірний, слабкий	Досліджується фінансовий стан організацій та вплив на її життєздатність загрозливих факторів	Простота розрахунку	Наслідки варіюються в широких межах чи сама подія відбувається кілька разів протягом певного проміжку часу
Аналіз імовірності (стосовно збитку)	Високий, помірний, низький	Аналізується ймовірність настання події у відсотковому значенні протягом певного періоду часу	Можливість виявлення головних ризиків, що впливають на функціонування підприємства	Значний фактор часу (від одного до десяти років), не враховуються заходи, які компанія може вжити для того, щоб знизити цю ймовірність
Аналіз імовірності (стосовно сприятливих можливостей)	Високий, помірний, низький	Досліджується ймовірність настання події у відсотковому значенні протягом певного періоду часу при врахуванні шляхів нейтралізації	Врахування можливих заходів для уникнення ризику чи зниження його ймовірності	Подію важко контролювати через низку зовнішніх факторів, що впливають на ризик
Експертний метод	Катастрофічний, критичний, допустимий, малий, мінімальний	Базуються на опитуванні кваліфікованих спеціалістів із наступною статистико-математичною обробкою результатів цього опитування	Простота розрахунків, можливість оцінки ризиків, що не піддаються аналізу іншими методами	Суб'єктивний характер

В економічній літературі з питань управління ризиком відзначається, що якісний аналіз у пріоритеті кількісному, тобто результати, що були

отримані на етапі виявлення ризику, є якраз вихідною інформацією для здійснення кількісного аналізу.

Як зазначає Л. І. Донець, ці етапи не завжди можна чітко відокремити один від одного. Аналіз може проводитися у двох напрямках: якщо вже виникли втрати, то проводиться дослідження причин, в іншому випадку - на основі аналізу системи виявляються потенційні ризики та можливі наслідки. Метою кількісного аналізу є отримання числового вираження окремих ризиків з визначенням характеристик ймовірності та можливих втрат. Для цього формується набір сценаріїв, і для окремих ризиків можуть бути побудовані функції розподілу ймовірності виникнення втрат в залежності від їх обсягу. Під час визначення рівня ризику необхідно враховувати, що він може змінюватися в залежності від вибраного методу оцінки [31].

Умовою використання більшості цих методів є наявність достатніх ресурсів, включаючи грошові кошти, інформацію, час тощо. Кількісні методи передбачають оцінку ризику в абсолютних та відносних термінах. У абсолютних термінах ризик вимірюється конкретними величинами – частотою або розмірами можливих втрат у грошовому еквіваленті. У відносних термінах ризик вимірюється різними безрозмірними показниками, які є відношенням двох або більше конкретних величин.

Для практичного використання рекомендується застосовувати декілька методів оцінки ризикованої ситуації, обираючи найбільш придатний варіант.

Методи кількісної оцінки до певної міри є уніфікованими, але вони не завжди дозволяють оцінити будь-який вид ризику в усіх можливих економічних ситуаціях (через нестачу часу, інформації, кваліфікації). Існують види ризиків, які вимагають особливого індивідуального підходу до їх оцінки, а також існують комплексні ризики, які включають відразу кілька типів ризиків. Саме тому поряд з універсальними методами використовують спеціалізовані методи оцінки економічного ризику.

Найбільш загальноприйнятими та багатофункціональними є такі методи [25-35]:

- оцінки експертів;
- статистичний;
- аналітичний;
- побудова дерева рішень;
- використання аналогій;
- нормативний;
- рейтинговий.

Для наочності в таблиці 1.2 наведено характеристику основних методів кількісної оцінки ризиків підприємства.

Основними інструментами статистичних методів є: середнє значення випадкової величини, дисперсія, середнє квадратичне відхилення, коефіцієнт варіації.

Середнє значення випадкової величини є кількісною характеристикою очікуваного результату [31-33].

$$\bar{X} = \sum_{x=1}^n X_i \times P_i, \quad (1.1)$$

де  $\bar{X}$  – середнє значення випадкової величини;

$X_i$  – значення випадкової величини;

$P_i$  – імовірність настання випадкової величини.

Важливою характеристикою, що визначає міру коливання очікуваного результату, є дисперсія – середньозважене з квадратів відхилень дійсних результатів від середніх [26-35]:

$$\sigma^2 = \sum_{i=1}^n (X_i - \bar{X})^2 \times P_i, \quad (1.2)$$

де  $\sigma^2$  – дисперсія.

Таблиця 1.2 – Характеристика методів кількісної оцінки

Методи кількісної оцінки	Сутність	Переваги методу	Недоліки методу
Статистичний	Полягає в основі теорії ймовірності розподілу випадкових величин	Найбільш розширена (повна) та достовірна інформація про рівень ризиків	Складність розрахунку, наявність достатньо великого обсягу статистичної інформації
Аналітичний	Такі критерії, як період окупності, норма прибутковості та індекс рентабельності, використовуються для аналізу. Порівнюючи значення цих показників у різних альтернативних проєктів, визначають їхній рівень ризику	Можливість виявлення головних ризиків, що впливають на функціонування підприємства та пошук шляхів зниження їх впливу	Метод недостатньо розроблений для підприємницької діяльності, складність розрахунку
Метод доцільності витрат	Витрати на конкретному напрямку не мають однакового рівня ризику. Стан щодо кожної галузі витрат розподіляється на зони загальних витрат, де конкретні витрати не перевищують встановленого рівня ризику	Пошук ризиків через порівняння витрат, простота в розрахунках	Не враховується вплив окремих ризиків
Метод аналогів	Порівняння з аналогічними багаторазово здійсненими операціями	Використання досвіду попередників	Неврахування фактору часу, необхідність повної та достовірної інформації
Рейтинговий метод	На основі фінансової звітності визначаються основні фінансові показники і проводиться їх класифікація за певною шкалою	Здатність обробки обширної інформації дозволяє порівнювати отримані результати з еталоном, що веде до простоти розрахунків	Можливість неправильного вибору еталону
Метод дерева рішень	Під час формування рішення визначаються різні варіанти, які можуть бути узяті до уваги, а також для кожного варіанту розглядаються можливі ситуації, які можуть виникнути	Пошук можливих сценаріїв розвитку подій, наочність	Можливість неправильного вибору сценарію розвитку подій, необхідність повної та достовірної інформації
Нормативний метод	Базується на використанні системи фінансових коефіцієнтів (ліквідності, автономії, покриття та ін.)	Легкість розрахунків, максимальна точність у розрахунках	Не дає можливості врахувати всю індивідуальність конкретної ситуації



Мірами мінливості очікуваного результату є дисперсія та середнє квадратичне відхилення [26-35]:

$$\sigma = \sqrt{\sigma^2} = \sqrt{\sum_{i=1}^n (X_i - \bar{X})^2 \times P_i}, \quad (1.3)$$

де  $\sigma$  – середнє квадратичне відхилення.

Середнє квадратичне відхилення вимірюється в тих самих одиницях, що і досліджувана характеристика.

Для аналізу ступеня варіативності використовується коефіцієнт варіації, який представляє собою відношення середнього квадратичного відхилення до середнього значення випадкової величини і показує ступінь відхилення отриманих значень [26-35].

$$V = \sigma \div \bar{X}, \quad (1.4)$$

де  $V$  – коефіцієнт варіації.

Аналітичні методи включають оцінку показників ризику на основі теоретичних концепцій. До аналітичних методів належать: метод дисконтування, аналіз окупності витрат, аналіз беззбитковості, аналіз чутливості. Переваги цих методів полягають у тому, що вони добре розроблені і легкі для сприйняття.

Метод дисконтування включає корекцію норми дисконту на коефіцієнт ризику, отриманий за допомогою методу експертних оцінок.

Метод окупності проекту полягає в розрахунках строку, за який повністю окупиться проект.

Аналіз чутливості – це визначення впливу зміни різних факторів на кінцевий показник.

Ризик реалізації рішення (проекту) визначається відносно з деяким схожим рішенням, яке було реалізоване заздалегідь. При цьому передбачається, що економічна система, в межах якої реалізується рішення, також поводить аналогічним чином.

При використанні аналогій застосовуються бази даних і знання щодо факторів ризику. Отримані дані обробляються для визначення залежностей та причин з метою обліку потенційного ризику під час реалізації рішення (проекту).

Метод експертних висновків. Його суть полягає в отриманні числових оцінок ризику на основі аналізу думок кваліфікованих спеціалістів. Використання цього методу ефективне при розв'язанні складних ситуацій, які не можуть бути формалізовані, коли недостатність та ненадійність інформації не дозволяють застосовувати статистичні або інші формалізовані методи кількісної оцінки ризику. Недоліки методу: відсутність гарантій точності отриманих оцінок; складності у проведенні опитувань та обробці отриманих даних.

Кожен тип ризику характеризується рядом показників-факторів. Експерти визначають оцінку цих показників в балах для кожного з них. Кожному показнику призначається вага відповідно до його значущості.

Кількісна оцінка ризику в цілому визначається за допомогою узагальненого показників [26]:

$$R = \sum_{j=1}^N R_j \times g_j, \quad (1.5)$$

де  $R$  – узагальнений показник ризику;  
 $R_j$  – кількісна оцінка  $j$ -го виду ризику;  
 $g_j$  – вага  $j$ -го виду ризику.

При детальній оцінці окремих ризиків та загального ризику використовуються такі правила:

- детальна оцінка кожного фактора проводиться в межах бальної шкали (наприклад, 0 до 10) в залежності від ступеня впливу даного фактора на ризик);
- вага кожного фактора встановлюється в межах від нуля до одного в межах відповідного виду ризику.

Ефективність методу експертних оцінок залежить від рівня кваліфікації експертів, тоді як ефективність рейтингового методу залежить від правильного вибору бази для порівняння. Однак це не означає, що слід відкидати кількісний аналіз ризику. З метою підвищення його ефективності слід використовувати комплексно всі методи кількісної оцінки. Це дозволить доповнити дані одного методу результатами іншого.

Таким чином, уникнення небажаних тенденцій можна здійснити, якщо на підприємствах застосовуватимуться сучасні методи управління, обов'язково враховуючи фактори, що викликають ризики у господарській діяльності. Це вимагає впровадження систем ризик-менеджменту на таких підприємствах, з особливим акцентом на ідентифікацію ризиків конкретних втрат. Важливо визначити функцію управління цими ризиками та встановити механізм для її ефективного виконання.

## **2 АНАЛІЗ ФІНАНСОВИХ РЕЗУЛЬТАТІВ ДІЯЛЬНОСТІ ТА ПРАКТИЧНИХ МЕТОДІВ ОЦІНКИ РИЗИКІВ АТ «ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ»**

### **2.1 Загальна характеристика підприємства**

Приватне акціонерне товариство «Інститут інформаційних технологій» (АТ «ІІТ») спеціалізується на наданні послуг в області проектування, розробки і впровадження рішень щодо забезпечення безпеки інформації у інформаційно-телекомунікаційних системах різного призначення та різного рівня складності.

Основні види діяльності:

- консультування з питань інформатизації;
- комп'ютерне програмування;
- виробництво комп'ютерів і периферійного устаткування.

Компанія володіє ліцензією від Держспецзв'язку України, виданою 15.02.2017 р., що дозволяє здійснювати діяльність, пов'язану з наданням послуг у сфері криптографічного та технічного захисту інформації (включаючи інформацію, яка є державною таємницею). В структурі компанії створено дві групи експертів, які проводять дослідження комплексів і засобів криптографічного захисту інформації, комплексів технічного захисту інформації та засобів захисту від НСД. Компанія має дозвіл на проведення діяльності, що має відношення до державної таємниці.

На рис. 2.1 наведена організаційна структура управління підприємства.

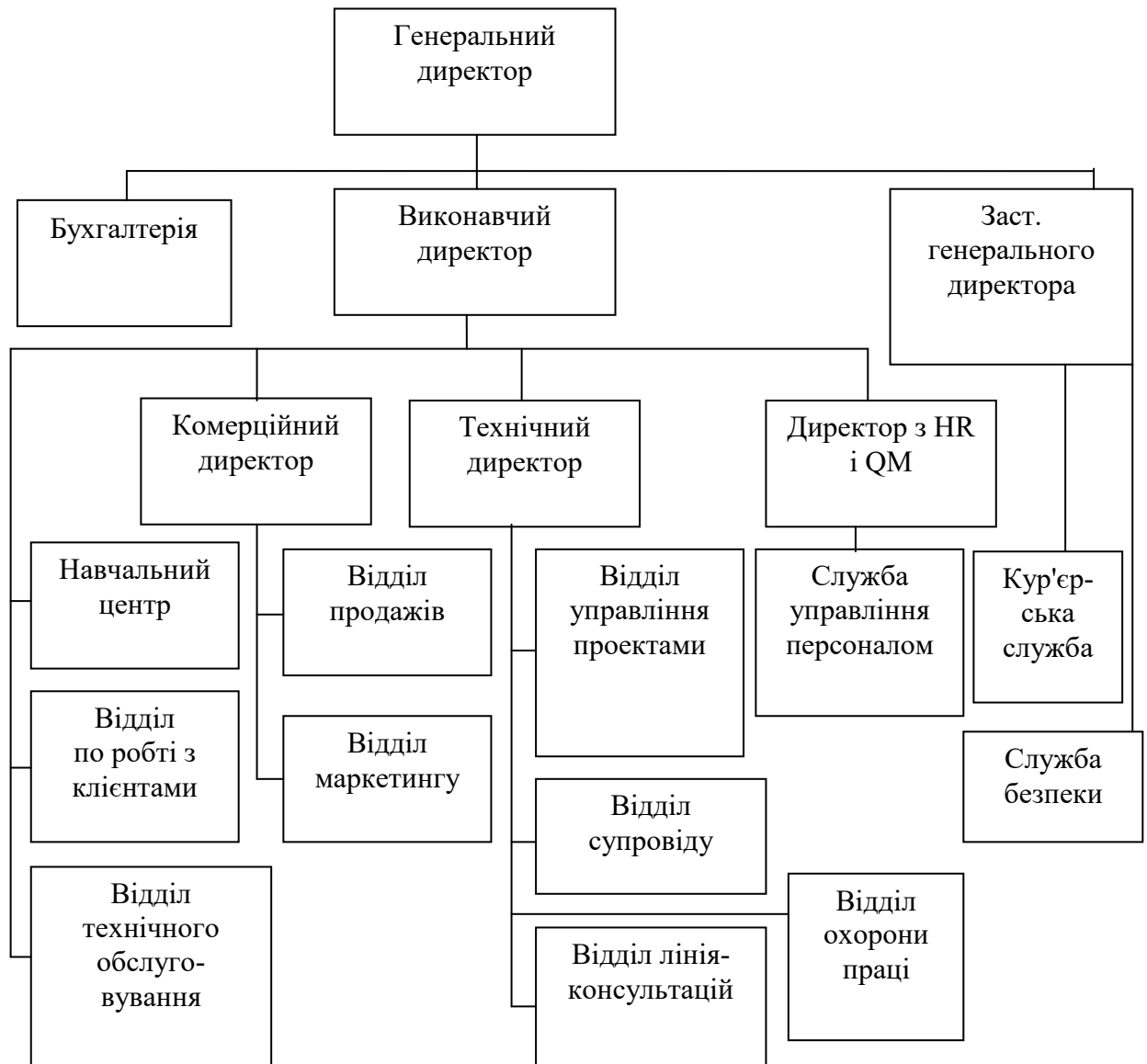


Рисунок 2.1 – Організаційна структура управління  
АТ «Інститут інформаційних технологій»

Один з основних напрямів діяльності компанії – це створення центрів сертифікації ключів та впровадження засобів криптографічного захисту інформації. Розроблені компанією засоби криптографічного захисту інтегруються в різні прикладні системи, такі як офісні пакети, системи електронного документообігу та подання звітності у електронному вигляді до Державної фіскальної служби України, Пенсійного фонду України та інші, а

також в банківські системи, інформаційні системи бюро кредитних історій та багато інших корпоративних та внутрішньовідомчих систем (понад 80).

Більш ніж 100 державних та комерційних організацій довірили АТ «ІТ» виконання робіт з забезпечення безпеки інформації своїх відомчих та корпоративних систем. Основні замовники компанії включають державні компанії, банківські установи, комерційні підприємства.

АТ «ІТ» надає послуги з:

- конфігурування та обслуговування програмного забезпечення (ПЗ) та комп'ютерної техніки;
- створення та обслуговування комплексних систем захисту інформації (КСЗІ) у інформаційно-телекомунікаційних системах;
- розроблення, тестування, супровід та технічну підтримку апаратно-програмних засобів криптографічного захисту інформації та ПЗ;
- консультування щодо функціонування КСЗІ;
- проведення державної експертизи КСЗІ;
- атестації серверних та сейфів;
- інструментального контролю комп'ютерної техніки;
- послуги із пошуку закладних пристроїв всіх типів;
- поставки та монтажу засобів захисту інформації;
- обладнання засобами захисту інформації кімнат для переговорів.

АТ «ІТ» має потужний парк обчислювальної техніки та периферійного обладнання, необхідний для проектування, розроблення, тестування, вихідного контролю продукції власного виробництва (програмних та програмно-апаратних засобів захисту), який є власністю підприємства.

## 2.2 Аналіз фінансових результатів діяльності підприємства

У даному підрозділі роботи було проведено аналіз показників, що висвітлюють результати фінансово-господарської діяльності підприємства, базуючись на даних фінансової звітності (Форма 1 «Баланс», Форма 2 «Звіт про фінансові результати»).

Показники основних фінансових результатів діяльності АТ «ІТ» представлені у таблиці 2.1.

Таблиця 2.1 – Основні показники фінансових результатів діяльності АТ «ІТ»

Показник	2021 р.	2022 р.	Абсолютне відхилення (+; -)	Відносне відхилення, %
Чистий дохід від реалізації продукції, тис. грн	50005	75416	25411,0	50,8
Собівартість реалізованої продукції, тис. грн	29003	52415	23412,0	80,7
Валовий прибуток, тис. грн	21002	23001	1999,0	9,5
Чистий прибуток, тис. грн	11006	9780	-1226,0	-11,1
Рентабельність продукції, %	72,4	43,9	-28,5	–
Дебіторська заборгованість, тис. грн	6216	5653	-563,0	-9,1
Кредиторська заборгованість, тис. грн	5183	15200	10017,0	193,3

У 2022 році чистий дохід від реалізації продукції склав 75,416 тис. грн, що на 50,8% перевищує рівень 2021 року. Також спостерігалася тенденція до збільшення собівартості реалізованої продукції.

Собівартість реалізованої продукції в 2022 році становила 52,415 тис. грн, що на 80,7% більше, ніж у 2021 році.

Сума валового прибутку склала в 2022 році 23,001 тис. грн, що вище рівня 2021 року на 9,5 %.

Чистий прибуток у 2022 році знизився на 11,1 % (1226,0 тис. грн) порівняно з 2021 роком і склав 9780 тис. грн.

Рентабельність продукції у 2022 році знизилася на 28,5% і становила 43,9 %, що можна розглядати як негативну тенденцію у результатах діяльності підприємства.

На рис. 2.2. представлена динаміка основних показників, що характеризують фінансово-економічні результати діяльності підприємства.

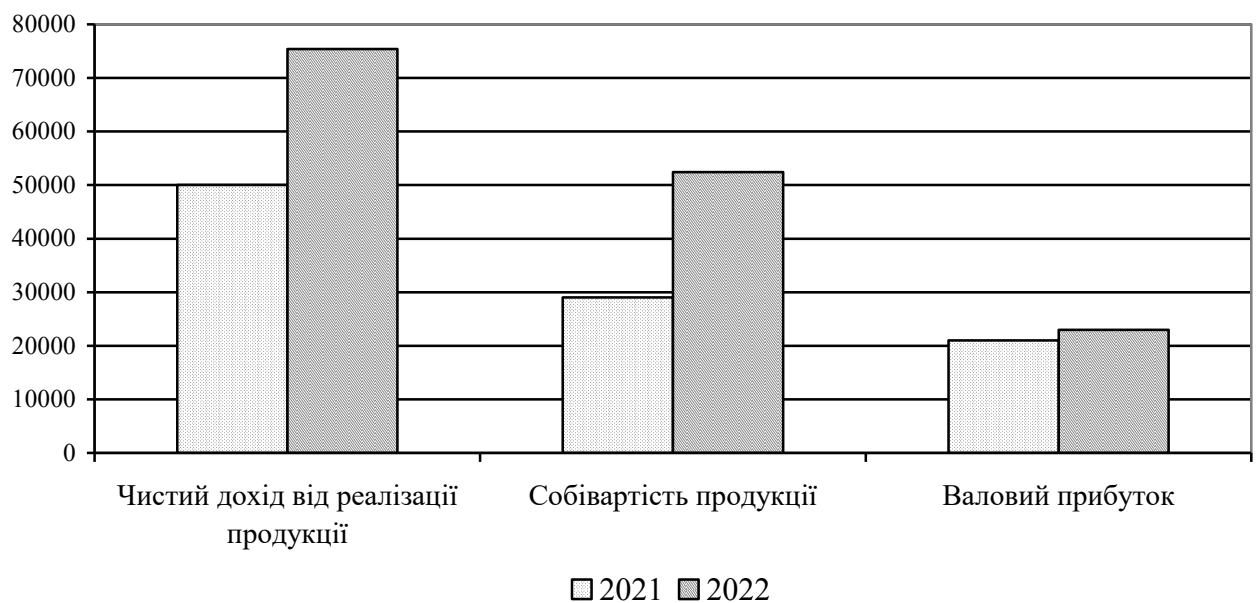


Рисунок 2.2 – Динаміка основних показників фінансових результатів діяльності АТ «ІТ», тис. грн

Динаміка сум дебіторської та кредиторської заборгованостей у 2021-2022 рр. АТ «ІТ» представлена на рис. 2.3.



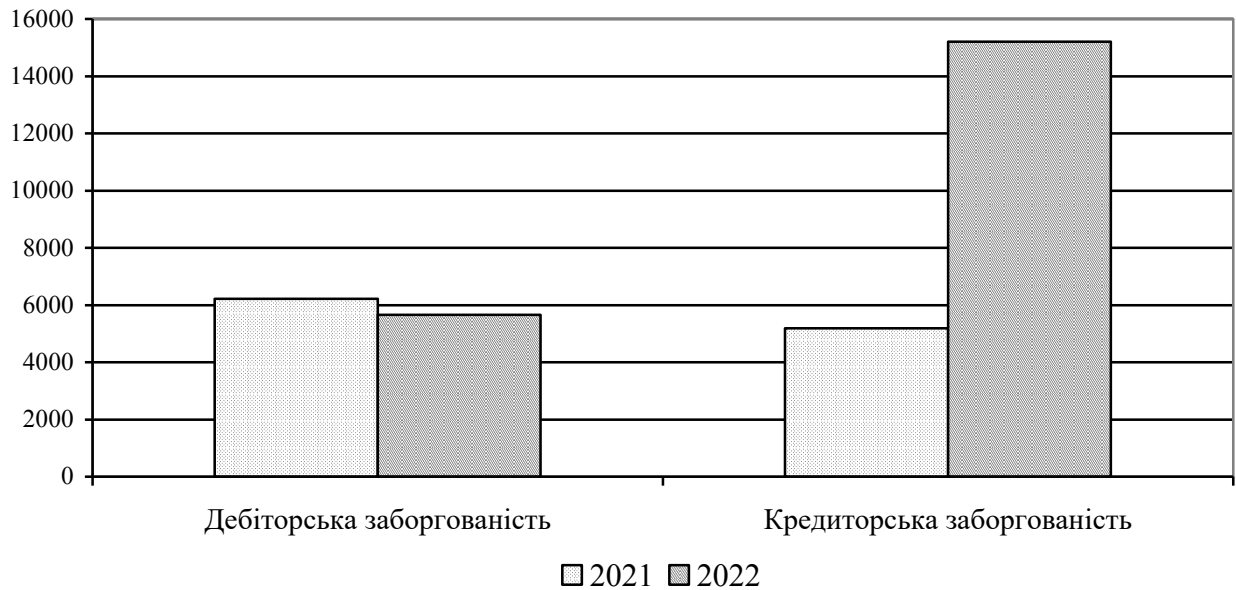


Рисунок 2.3 – Динаміка дебіторської та кредиторської заборгованостей  
АТ «ІТ» за 2021-2022 рр., тис. грн

Склад і структура операційних витрат АТ «ІТ» за 2021-2022 рр. наведений у таблиці 2.2.

Таблиця 2.2 – Склад і структура операційних витрат АТ «ІТ» за 2021-2022 рр.

Показник	2021 р.		2022 р.		Відхилення	
	Сума, тис. грн	Питома вага, %	Сума, тис. грн	Питома вага, %	абсол.	відносне, %
Матеріальні затрати	10887	28,1	17067	26,6	6180,0	56,8
Витрати на оплату праці	18840	48,6	35010	54,5	16170,0	85,8
Відрахування на соціальні заходи	2168	5,6	3201	5,0	1033,0	47,6
Амортизація	868	2,2	1052	1,6	184,0	21,2
Інші операційні витрати	5963	15,4	7937	12,4	1974,0	33,1
Разом	38726	100,0	64267	100,0	25541,0	66,0

На рис. 2.4 і 2.5 графічно представлено динаміку операційних витрат АТ «ІТ».

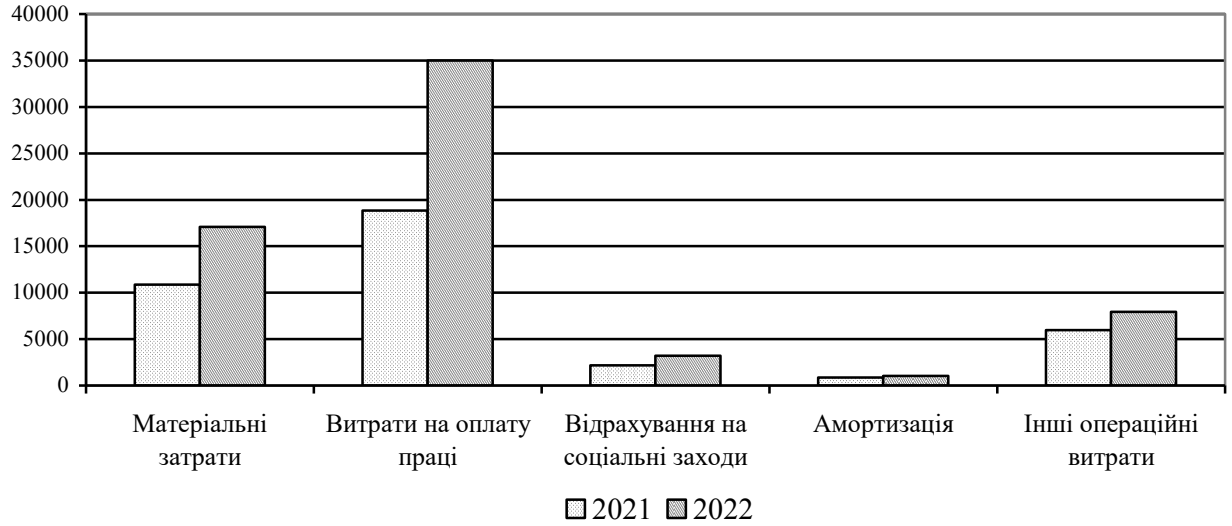


Рисунок 2.4 – Динаміка операційних витрат за елементами, тис. грн

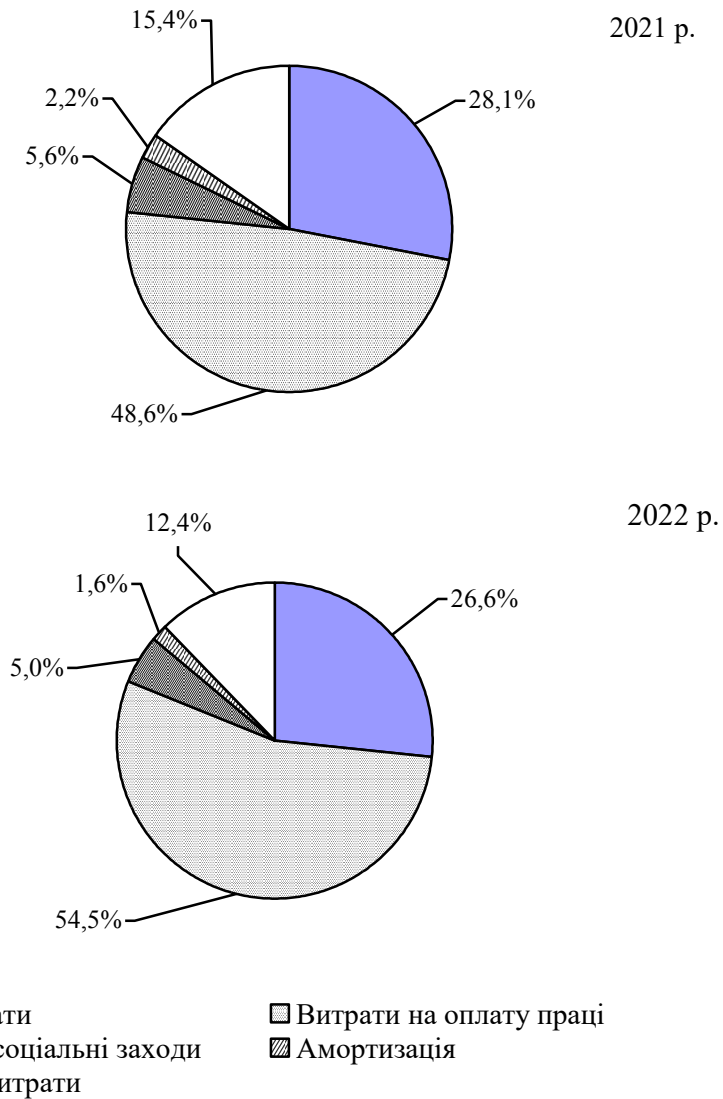


Рисунок 2.5 – Структура операційних витрат за елементами у 2021-2022 рр.

Згідно з рис. 2.5 слід зазначити, що «Витрати на оплату праці» мають найбільший внесок у структурі операційних витрат: у 2021 р. – 48,6%, у 2022 р. – 54,5%. Другим за величиною видом витрат є «Відрахування на соціальні заходи»: у 2021 р. – 28,1%, у 2022 р. – 26,6%, що можна розцінювати як позитивну тенденцію на підприємстві.

Підприємство не має окремих структурних підрозділів. Загальна чисельність працівників на 2022 рік становить 64 осіб, з них штатних працівників облікового складу – 40 осіб.

Бухгалтерський облік та фінансова звітність на підприємстві проводяться відповідно до українського законодавства, включаючи Закон «Про бухгалтерський облік та фінансову звітність в Україні» з усіма змінами та доповненнями. Всі економічні операції вимірюються та об'єднуються в бухгалтерському обліку та фінансовій звітності в гривнях. Облік виробничих запасів ведеться за вартістю придбання. Вартість запасів при їх відпуску, використанні в виробництві або іншому списанні визначається за методом ідентифікованої собівартості відповідного запасу.

Придбані (створені) основні засоби включаються до балансу підприємства за первісною вартістю. Амортизація основних засобів проводиться прямолінійним методом з використанням строків, встановлених для кожного об'єкта основних засобів, зокрема:

- для будівель – 20 років;
- для споруд – 15 років;
- для передавальних пристроїв – 10 років;
- для машин і устаткування (включаючи комп'ютерну техніку) – 5 років;
- для інструментів, приладів, інвентаря (меблів) – 5 років.

Амортизація для малоцінних необоротних матеріальних активів (МНМА) та бібліотечних фондів встановлюється у перший місяць їх експлуатації і становить 100% від їх вартості.

Нематеріальні активи, які були придбані або створені, включаються до балансу підприємства за їх первісною вартістю. Амортизація нематеріальних активів проводиться протягом періоду їх корисного використання, який визначається на момент прийняття цього об'єкта як активу (при його зарахуванні на баланс), але не більше 10 років. Термін корисного використання встановлюється індивідуально для кожного нематеріального активу.

Амортизація нематеріальних активів нараховується з використанням прямолінійного методу.

Амортизація необоротних нематеріальних активів складає 1187 тис. грн. За 2022 рік нараховано амортизації в обсязі 413 тис. грн. Вибуло протягом року нематеріальних активів на загальну суму 28 тис. грн, зокрема через знос – 25 тис. грн. У 2022 році було збільшено початкову вартість нематеріальних активів за рахунок витрат на доопрацювання комп'ютерних програм на суму 778 тис. грн.

У складі нематеріальних активів розташоване програмне забезпечення, яке повністю амортизоване на суму 14 тис. грн. Основні засоби підприємства на 31.12.2022 року становлять 3387 тис. грн. Нараховано амортизації за звітний період на суму 639 тис. грн.

Загальна сума накопиченої амортизації складає 1909 тис. грн або 56,36%. За рік надійшло до складу основних засобів 1224 тис. грн. Вибуло за рік основних засобів на загальну суму 48 тис. грн, у тому числі за рахунок зносу 48 тис. грн. У складі основних засобів розташоване обладнання, яке повністю амортизоване на суму 1205 тис. грн.

До виробничих запасів включено вартість закупівельних напівфабрикатів та комплектуючих виробів, придбаних для подальшого комплектування апаратно-програмних засобів (8686 тис. грн.), які виготовляє АТ «ІТТ», та інші матеріали (69 тис. грн.), які використовуються в господарській діяльності підприємства.

Загальна сума запасів становить 8755 тис. грн. Вартість незавершеного виробництва – 1234 тис. грн. та напівфабрикатів власного виробництва – 1881 тис. грн.

Вартість готової продукції складає 2459 тис. грн., в тому числі вартість переданої на комісію продукції – 1309 тис. грн.

Дебіторська заборгованість становить 13031 тис. грн., зокрема:

- заборгованість покупців за товари та послуги 5653 тис. грн.;
- сума авансів, які надані іншим підприємствам в рахунок майбутніх поставок 6938 тис. грн.;
- інша заборгованість 440 тис. грн.

Облік розрахунків аналітичним методом із дебіторами ведеться окремо по кожному контрагенту відповідно до чинного законодавства.

Залишок грошових коштів в національній валюті на 31.12.17 року становить 13328 тис. грн., в тому числі на поточних рахунках у банку 621 тис. грн., на інших рахунках у банку (депозитні рахунки) – 12410 тис. грн. та на спецрахунку ПДВ – 297 тис. грн. Інші оборотні активи становлять 1040 тис. грн.

Сума зареєстрованого капіталу – 750 грн., який поділено на 100 простих іменних акцій вартістю 7,50 грн. кожна. Резервний капітал становить 8 тис. грн.

Нерозподілений прибуток на кінець року становить 19440 тис. грн., в тому числі прибуток минулих років 10310 тис. грн., виплачені дивіденди

акціонерам у 2022 році у розмірі 650 тис. грн. та прибуток поточного року 9780 тис. грн.

Кредитами банку підприємство не користується.

Поточна кредиторська заборгованість становить 1759 тис. грн.

Заборгованість перед бюджетом підприємства становить 2514 тис. грн, в тому числі з податку на прибуток підприємств 1402 тис. грн, з податку на додану вартість 1112 тис. грн.

У фінансовому звіті підприємства представлені основні показники фінансово-господарської діяльності, включаючи стан заборгованості та зобов'язань, оборотні та нематеріальні активи, а також звітність перед різними контрагентами.

На основі проведених досліджень можна зробити наступні висновки:

- основні показники фінансових результатів діяльності АТ «ІТ» в аналізованому періоді характеризують тенденцію до збільшення;
- сума дебіторської заборгованості зменшується;
- протягом періоду, що аналізується, питома вага витрат на заробітну плату в загальному обсязі витрат підприємства підвищується.

Така динаміка поліпшення основних показників діяльності підприємства підвищує його інвестиційну привабливість і разом з тим збільшує загальну привабливість підприємства для рейдерського захоплення.

Виходячи з цього, керівництво АТ «ІТ» прагне розробити та впровадити в практику науково-обґрунтовані методи оцінювання ризиків з метою забезпечення економічної безпеки підприємства.

### 2.3 Практичні методи оцінки ризиків на підприємстві

Інформація стала ключовим ресурсом, який визначає конкурентоспроможність фірми в XXI столітті. Швидке зростання швидкості передачі даних, збільшення обсягів накопичених знань, розвиток інформаційних технологій змінили не лише середовище бізнесу, але й управлінське завдання, зсунувши фокус управлінської активності з традиційних ресурсів (праці і капіталу) на інформаційний ресурс. Без побудови автоматизованої системи управління інформаційними потоками як всередині фірми, так і із зовнішнім середовищем, неможливо досягти успіхів в конкурентній боротьбі. Сучасний ринок характеризується динамічністю, тому швидкість прийняття управлінських рішень і гнучкість бізнесу стають основними конкурентними перевагами фірми.

Основою досягнення конкурентних переваг є інформаційні системи, що базуються на інформаційній технології, сучасному комп'ютерному обладнанні і висококваліфікованому персоналі. Впровадження проектів в області інформаційних систем і технологій – дуже складний і дорогий процес, здійснення якого пов'язане з цілим рядом різнопланових ризиків, що важко детермінуються, які призводять до того, що проект або взагалі терпить фіаско, або не досягає поставлених цілей. Таким чином, в сучасному українському бізнесі питання управління ризиками при реалізації проектів в цій сфері мають особливу специфіку, адже від успішності їх вирішення в значній мірі залежить конкурентність наших компаній як на внутрішньому, так і на міжнародному ринку.

Управління ризиками стає, по суті, повсякденною діяльністю для багатьох учасників ІТ-проекту відразу після його ініціації і аж до завершення. Разом з тим класифікація ризиків і відповідно оцінка значущості

кожній з категорій ризиків в контексті конкретного проекту – це роботи, що виконуються на передпроектній стадії.

В економічній літературі відзначається різноманітність трактування особливостей та елементів ризику, зокрема ризику впровадження проектів в області інформаційних систем і технологій. Різні точки зору на сутність ризику пояснюються багатовекторністю цього явища, практично повним його ігноруванням у чинному законодавстві, недостатнім використанням у реальній економічній практиці та управлінській діяльності. У інвестиційному та фінансовому менеджменті найчастіше ризик розглядають як ступінь невпевненості у отриманні очікуваних доходів від інвестицій. Якщо уточнити загальне поняття ризику для проектного аналізу, то цільовим завданням системи є досягнення прогнозованого рівня рентабельності, а засобом досягнення цієї мети є виконання даного проекту. Отже, ризик проекту – це ступінь невизначеності у досягненні прогнозованого рівня рентабельності в процесі виконання проекту [23-25].

Складність класифікації ризиків полягає в їхній різноманітності. Існують різні системи класифікації проектних ризиків – залежно від обраного критерію. Найважливішими елементами, покладеними в основу класифікації ризиків, є [26]:

- час виникнення;
- характер обліку та наслідки;
- основні чинники виникнення;
- сфера виникнення та інші.

При класифікації ризиків, що виникають під час впровадження проектів в області інформаційних систем і технологій, є кілька запропонованих параметрів:

- ризики, пов'язані з масштабом проекту;
- ризики, пов'язані з недостатнім досвідом у сфері ІТ;



- технічні ризики проекту;
- організаційні ризики;
- оперативні ризики проекту [27-30].

Будь-який бізнес-проект розробляється з урахуванням його ефективності з точки зору прибутковості. Зазвичай переваги автоматизованих інформаційних систем для керівництва підприємством не викликають сумнівів. Більшість представників топ-менеджменту компаній визнає вигоди від інформаційних технологій, проте наразі відсутня єдина формула для обчислення ефективності інформаційних систем. Інвестиції в автоматизовані інформаційні системи приносять віддачу у вигляді зростання ринкової капіталізації компанії завдяки більшій управлінській ефективності, прозорості, корпоративній культурі, привабливості для клієнтів і співробітників, а також зменшенню бізнес-ризиків.

Проект з автоматизації діяльності підприємства – це складна система, яка піддається впливу різноманітних внутрішніх і зовнішніх ризиків. Ці фактори можуть бути вбудовані в організацію самого проекту або стратегії досягнення його цілей, або виступати результатом діяльності як учасників проекту, так і зовнішніх сторін відносно проекту. Ризики будь-якого проекту завжди мають об'єктивні і суб'єктивні основи. Об'єктивними, як правило, виступають умови зовнішнього середовища, на які діяльність з управління проектом не може більш-менш суттєво впливати (законодавство, регулювання підприємницької діяльності, податкова система, взаємини з партнерами, економічна обстановка в країні, стихійні лиха і т.д.). Дії щодо зниження ризиків цих видів проводяться на рівні всієї компанії, а не на рівні окремого проекту. Суб'єктивну основу ризиків становлять управлінські рішення, які ухвалюються. Тому для ефективного управління проектом дуже важливо знати ступінь впливу таких суб'єктивних чинників на досягнення цілей проекту. Впровадження інформаційної системи на рівні

функціональних відділів може вирішити виклики, що виникли в «реальній» системі взаємодії. Кожен відділ має свій власний набір критеріїв для оцінки ефективності системи. Наприклад, відділ технологічної підготовки виробництва покращує продуктивність технологів, маркетинг забезпечує контроль за виконанням замовлень, відділ постачання здійснює оперативне планування закупівель, спрямоване на матеріальне забезпечення виробництва і так далі.

Зазвичай основний ефект від впровадження інформаційних систем – це збільшення продуктивності праці:

- економія робочого часу менеджерів;
- ефективне використання людських ресурсів на підприємстві;
- скорочення вартості здійснення тої чи іншої трансакції на підприємстві.

Серед основних ризиків проекту впровадження інформаційної системи можна виділити наступні:

- невизначеність цілей проекту;
- недостатня відповідність функцій системи цілям і завданням підприємства;
- відсутність етапів попереднього вивчення і планування;
- ризики, пов'язані з «людським чинником» (незгуртована робота учасників проекту, висока залежність від внутрішньої структури організації-замовника і від лояльності персоналу зокрема);
- дестабілізаційна дія проекту впровадження на систему управління;
- негативний вплив проекту на грошові потоки підприємства через високу вартість продукту і сукупні витрати;
- відхилення фактичної ефективності впровадження системи від заданої, короткострокові ефекти;

- ризик перевитрат бюджету проекту, ризики втрати можливостей у результаті невірного вибору конфігурації ERP-рішення;
- зниження ефективності підприємства в результаті невдалого впровадження ІС, втрата менеджментом інструментів контролю.

Неспівпадіння функціональних властивостей з цілями та завданнями компанії можна віднести до недостатнього використання функціональних можливостей встановлюваної системи (оплата за непотрібні функції) або до вибору слабкої системи, функціонал якої не відповідає цілям організації. Тут можна згадати спробу оптимізувати організаційну структуру компанії за допомогою впровадження інформаційної системи, хоча в світовій практиці прийнято, що ефективне впровадження інформаційної системи можливе лише в компанії з оптимізованою організаційною структурою, без дублювання управлінських функцій та перекриття інформаційних потоків.

Також важливо врахувати ризик погіршення діяльності підприємства, особливо на початкових стадіях впровадження інформаційної системи, що може бути спричинено несумісністю функціональних характеристик системи з бізнес-процесами підприємства, опором або тривалим періодом навчання персоналу, а також некоректним функціонуванням інформаційної системи. Втрата інструментів керування та контролю пов'язана з інертністю мислення керівників, які в нових, змінених умовах віддають перевагу старим методам, які більше орієнтовані на емоційні фактори, ніж на логічне обґрунтування управлінських процесів.

Ризик, що виникає через «людський фактор», перш за все, пов'язаний з недостатньою кваліфікацією керівництва для реалізації проекту. Часто керівники компанії при прийнятті рішення про впровадження нової інформаційної системи недооцінюють час, необхідний для навчання персоналу роботі з новою системою. Знайти кваліфікованих спеціалістів часто буває важко. Важливо враховувати можливий опір співробітників

компанії щодо впровадження таких проектів, що, в першу чергу, пов'язано з прийняттям непопулярних рішень про скорочення непотрібних посад.

Джерелами інформації, призначеної для оцінки ризику ІТ-проекту, можуть, наприклад, служити:

- технічна інфраструктура для визначення технічних і технологічних ризиків;
- вимоги до безпеки даних для визначення ризиків інформації;
- організаційна структура і штатний розклад підприємства для виявлення організаційних ризиків;
- карти технологічних потоків для визначення техніко-виробничих ризиків;
- договори і контракти для визначення ділових і юридичних ризиків та інше.

Одним із головних ризиків впровадження інформаційних систем є відсутність чітких цілей проекту та недостатнє попереднє вивчення і планування. Недолік чіткості у цілях може призвести до втрати фокусу і неефективного використання ресурсів, а відсутність попереднього вивчення може спричинити неврахування ключових факторів ризику.

Також, значний ризик пов'язаний з «людським фактором», включаючи незлагоджену роботу учасників проекту, велику залежність від внутрішньої структури організації-замовника та лояльність персоналу. Це може призвести до дестабілізації проекту та негативного впливу на грошові потоки підприємства.

Крім того, ризик перевитрати бюджет проекту, втрата ефективності внаслідок невдалого впровадження інформаційної системи, а також втрата менеджментом інструментів контролю є важливими чинниками, що можуть впливати на успішність проекту.

Ризик перевитрати бюджет може виникнути через неправильну попередню оцінку проекту впровадження або неочікувані відхилення, які виникають у процесі його реалізації. Оцінка ризиків в області ІС і Т може бути якісною або кількісною.

Кількісний аналіз надає конкретні значення ризиків, проте ці значення, як правило, не мають високої точності через неможливість кількісного обліку багатьох факторів ризику. Найчастіше використовується швидкий якісний аналіз, спрямований на розподіл чинників ризику за групами. Масштаб якісного аналізу може відрізнятися в різних методиках, проте основна мета – виявлення найсерйозніших загроз.

Якісний метод оцінки передбачає визначення факторів ризику та етапів роботи, під час яких виникає ризик, тобто встановлення потенційних сфер ризику. Після цього відбувається ідентифікація всіх можливих ризиків. Наприклад, на етапі концептуалізації для зменшення ймовірності виникнення ризику, пов'язаного з недостатнім досвідом у сфері ІТ, розробляють і затверджують концепцію проекту якнайшвидше. Також актуальним є навчання користувачів, включаючи керівництво, в дотриманні технологій роботи. Якісна оцінка ризиків виконується на етапах аналізу, планування і реалізації проекту з урахуванням отриманих даних в результаті ідентифікації ризиків.

Одним з прикладів об'єктивного критерію і якісної оцінки в ІТ-проекті є ймовірність виходу з ладу якого-небудь обладнання, наприклад, ПК, протягом певного періоду часу. Прикладом суб'єктивного критерію при оцінці ІТ-ризиків може бути оцінка власником інформаційного ресурсу ризику виходу з ладу ПК. Зазвичай для цього створюється якісна шкала з декількома градаціями.

Для оцінки ризиків у впровадженні проектів в галузі інформаційних систем і технологій можна скористатися такими кількісними методами оцінки, як [28]:

- метод аналізу доцільності витрат;
- статистичний метод;
- метод експертних оцінок;
- метод аналогій.

Статистичний метод полягає в числовому визначенні імовірності виникнення ризикової ситуації та обсягу фінансових втрат. Оскільки цей метод вимагає інформації про кількість ризикових ситуацій та фінансові наслідки, для підприємства, де планується впровадження інформаційної системи, потрібно використовувати досвід інших компаній, які вже мали досвід роботи в цій галузі. Крім того, слід звернутися за інформацією до підрядника, який безпосередньо буде реалізовувати проект на підприємстві.

При оцінці ймовірності кожна подія позиціонується в наступних координатах (рис. 2.6, де  $P_i$  – ймовірність настання ризикової події).

Статистичний метод не застосовний, якщо підприємство тільки створене. Існують недоліки даного методу, які полягають в тому, що за допомогою цих розрахунків можна отримати сигнал про наявність ризику, не дізнавшись при цьому напрям відхилення від очікуваного результату [26]. За допомогою статистичного методу можна оцінити такі ризики, як ризик перевитрати бюджет проекту, ризик зниження ефективності підприємства в результаті неуспішного впровадження ІС, ризик відхилення фактичної ефективності впровадження системи від заданої.

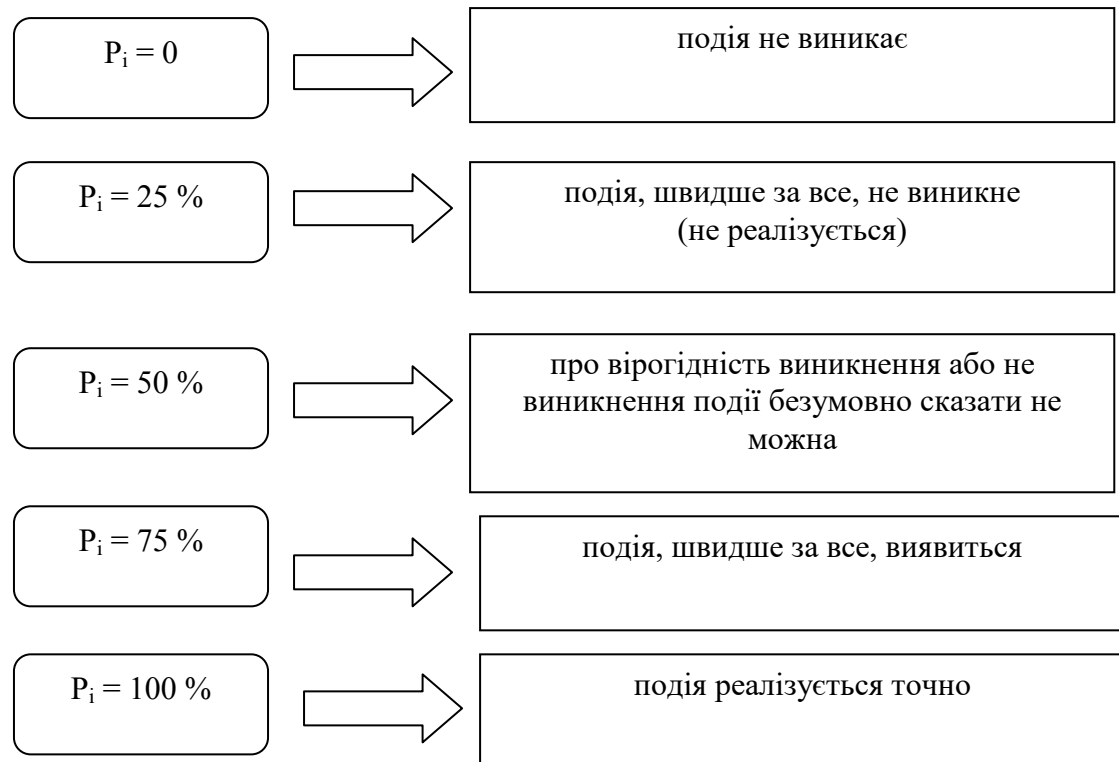


Рисунок 2.6 – Вірогідність настання ризикової ситуації

Оцінка ризиків методом аналізу доцільності витрат передбачає ідентифікацію потенційних зон ризику. Для цього стан кожного з елементів розділяється на область ризику, яка є зоною загальних витрат, в межах якої конкретні витрати не перевищують граничного значення встановленого рівня ризиків:

- область абсолютної стабільності;
- область нормальної стабільності;
- область нестабільного стану;
- область критичного стану;
- область кризового стану.

Важливо відзначити, що на фазі концептуалізації ідентифіковані ризики найімовірніше будуть віднесені до областей нормальної стабільності і нестабільного стану. Це пов'язано з невизначеністю інформації та

відсутністю досвіду на підприємстві в даній сфері. З часом ризику, як правило, переміщуються в області критичного або кризового стану, що пов'язано з ігноруванням цих ризиків на більш ранніх стадіях життєвого циклу проекту.

Метод експертних оцінок. До найбільш поширених методів експертних оцінок ризику відносять [27]:

- метод «Дельфі»;
- ранжування;
- метод парного порівняння;
- метод бальної оцінки ризику.

Надійність отриманих оцінок залежить від кваліфікації експертів, незалежності їхніх думок і методичного забезпечення проведення експертизи. Коефіцієнт конкордації (узгодженості) думок експертів є одним з показників достовірності отриманих значень. В Україні експертні методи для оцінки ризиків бізнесу використовуються рідко. За даними [27], більшість українських підприємств малого і середнього бізнесу мають критичний рівень прогнозованого ризику на даний час.

Метод аналогій. Якщо потрібно визначити ступінь ризику по будь-якому інноваційному напрямку діяльності фірми, такому як впровадження проектів в області інформаційних систем і технологій, коли немає чіткої бази для порівняння, краще знати минулий досвід інших компаній, ніж не знати нічого. Управління ризиками не є одномоментною подією, а здійснюється періодично, по мірі того як зміни відбулися або проблеми виявлені. Тому протягом всього проекту керівникові проекту необхідно проводити контроль ризиків проекту.

Отже, управління ризиками ІТ-проектів – це визначення, оцінка і контроль внутрішніх і зовнішніх чинників, які можуть негативно вплинути на вартість і процес впровадження нових інформаційних систем у компанії.



Головною ціллю управління ризиками таких проектів є вчасне ідентифікація ризиків, що виникають при впровадженні інформаційної системи або системи автоматизації, які можуть мати негативний вплив на успішність проекту, а також ефективне планування дій для їх зменшення. У результаті проведеного аналізу були виявлені основні ризики, пов'язані з впровадженням проектів у сфері інформаційних систем і технологій. Розглянуті якісні й кількісні методи оцінки ризиків. Представлено умови застосування окремих методів оцінки, їх актуальність для підприємства. Далі планується розробка інтегрального методу оцінки ризиків впровадження проектів у сфері інформаційних систем і технологій, який буде поєднувати в собі вже відомі кількісні і якісні методи.

Для аналізу господарської діяльності підприємства, що досліджується, у даному розділі використано підходи, наведені у роботах [36-46].

### **3 НАПРЯМИ УДОСКОНАЛЕННЯ УПРАВЛІННЯ РИЗИКАМИ В КОНТЕКСТІ ЗАБЕЗПЕЧЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА**

#### **3.1 Концептуальний підхід до формування системи ризик-менеджменту на підприємстві**

Необхідною передумовою для успішної діяльності підприємства є впровадження системи управління ризиками. У розвинених країнах управління ризиками вже давно є необхідною складовою системи управління підприємством в цілому. Оскільки ризик є економічною категорією, його рівень можна впливати через формування та реалізацію стратегії, використання засобів та принципів. Цей процес визначає створення ефективного механізму управління ризиками, відомого як ризик-менеджмент [47-49].

Аналіз наукових робіт у галузі управління ризиками показує різноманітні тлумачення цього поняття:

- розгляд ризиків як специфічної області діяльності підприємства;
- розгляд ризиків як багатоетапного процесу, що включає розробку загальної філософії управління ризиками, їх ідентифікацію, аналіз та оцінку з метою зменшення та нейтралізації негативних наслідків;
- розробка та впровадження різноманітних методів, рекомендацій і заходів, що дозволяють прогнозувати ризики та зменшувати їх ступінь;
- процес впливу на суб'єкт господарювання, що забезпечує широкий охоплення можливих ризиків, їх обґрунтоване прийняття та зведення ступеня впливу на мінімум;
- комбінація трьох елементів: встановлення цілей (визначення цілей), ризик-маркетинг (вибір інструментів для управління ризиками) та ризик-

менеджмент (забезпечення рівноваги в трикутнику «люди-цілі-ресурси» під час досягнення встановлених цілей за допомогою вибраних інструментів).

Сутність ризик-менеджменту полягає в здійсненні комплексу економічних, організаційних та технічних заходів, спрямованих на визначення видів, факторів та джерел ризику, оцінку їхньої величини, а також розробку та впровадження заходів для зниження рівня ризику та запобігання можливим негативним наслідкам [35, 50-54].

Відповідно до сучасної концепції управління ризиками, ризик-менеджмент може бути визначений як система або процес. Як система управління, ризик-менеджмент включає об'єкти управління – підсистему, що керується, та суб'єкти управління – керуючу підсистему (рис. 3.1) [51].

Взаємодія об'єктів та суб'єктів управління в ризик-менеджменті може відбуватися лише при наявності інформаційного забезпечення, яке включає статистичні, інформаційні та комерційні дані. Оскільки процес управління завжди передбачає отримання, передачу та використання конкретної інформації, інформаційне забезпечення вважається ключовим елементом у структурі управління ризиком. Від достовірності та якості цього забезпечення залежить величина підприємницького ризику та прийняття ефективних господарських рішень.

Як для об'єкта, так і для суб'єкта системи управління господарськими ризиками визначено конкретні функції.

Функції керуючої підсистеми охоплюють організацію вирішення питань, пов'язаних з ризиком та капіталовкладеннями, здійснення заходів з зниження рівня ризику, управління процесом страхування ризиків, а також економічних відносин і зв'язків між суб'єктами господарювання.

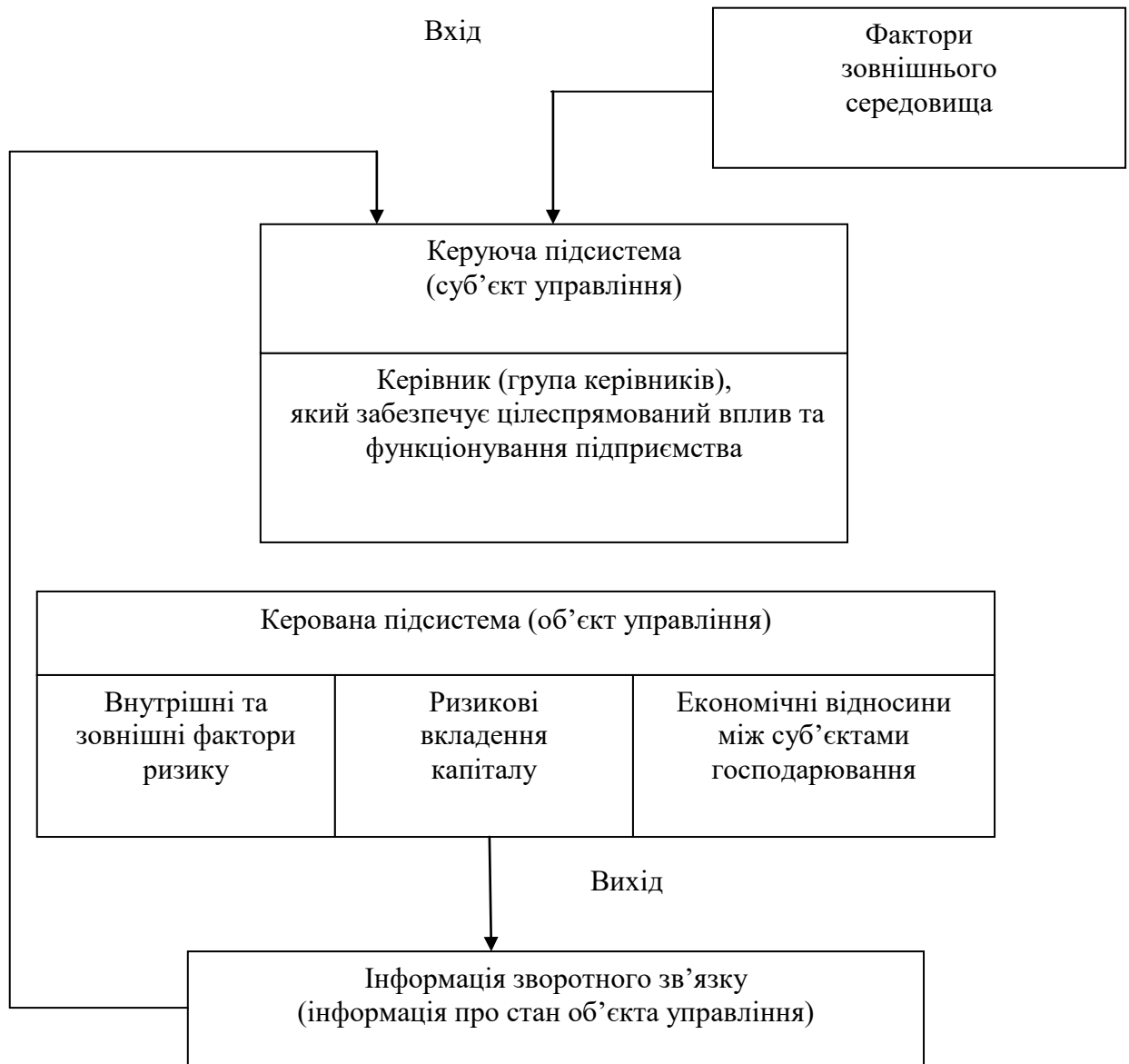


Рисунок 3.1 – Структурно-логічна схема системи ризик-менеджменту

До функцій керуючої підсистеми відносяться:

- прогнозування (розробка майбутніх змін фінансово-економічного стану об'єкта та його складових);
- організацію (об'єднання людей, задіяних у управлінні ризиками, на основі визначених правил та процедур: формування органів управління, створення структури управлінського апарату, розробка стандартів та норм);
- регулювання (вплив на об'єкт управління для забезпечення його стабільності при відхиленнях від встановлених параметрів);

- координацію (забезпечення взаємодії всіх елементів системи управління ризиками, управлінського апарату та фахівців);
- стимулювання (заохочення спеціалістів до активної участі в управлінні ризиками);
- контроль (перевірка ефективності регулювання рівня ризику).

В ідеалі для ефективного функціонування системи управління ризиками повинна існувати організація управління ризиками, обладнана конкретними функціональними обов'язками і необхідними матеріальними, фінансовими, трудовими та інформаційними ресурсами.

На підприємстві повинен бути створений спеціальний підрозділ – відділ (або відділення) управління ризиками під керівництвом ризик-менеджера (на малих підприємствах функції ризик-менеджера може виконувати фінансовий менеджер).

Більшість великих західних компаній мають у штаті спеціального менеджера з ризиків, який спільно з іншими менеджерами компанії (маркетологом, менеджером з персоналу, інженером з техніки безпеки) бере на себе відповідальність за управління ризиками. Він є одним із перших помічників вищого керівництва. Ризик-менеджер разом із відповідними спеціалістами бере участь у прийнятті рішень, пов'язаних з ризиками (наприклад, надання кредитів, вибір об'єктів інвестування) та розробляє способи уникнення небажаних ризиків.

Функції менеджера з управління ризиками можуть включати наступне:

- ідентифікація ризиків (виявлення потенційних ризиків, які можуть вплинути на проект або організацію);
- аналіз ризиків (оцінка ймовірності та потенційного впливу ідентифікованих ризиків);

- планування реагування на ризики (розробка стратегій для управління ризиками, що можуть включати уникнення ризику, зменшення його впливу або ймовірності, передачу ризику або прийняття ризику);

- моніторинг та контроль ризиків (слідкування за ідентифікованими ризиками, моніторинг залишкових ризиків, виявлення нових ризиків, виконання плану реагування на ризики та оцінка його ефективності протягом всього життєвого циклу проекту);

- комунікація та консультування (важливо забезпечити, що всі зацікавлені сторони розуміють стан ризиків проекту та їх вплив, а також що вони залучені в процеси ідентифікації, аналізу та управління ризиками).

Відділ управління корпоративними ризиками зосереджується на практичних питаннях, що стосуються виявлення ризиків, статистичної та реєстраційної обробки інцидентів, розробки та виконання заходів для збільшення безпеки компанії, здійснення страхових операцій та укладання договорів про страхування та перестраховування.

Основне ідеологічне завдання ризик-менеджера та його відділів – це формування стратегії та принципів управління ризиками на підприємстві, які мають бути відображені в внутрішніх регулятивних документах.

Процес ризик-менеджменту включає в себе формування стратегічних та тактичних рішень.

Стратегія ризик-менеджменту – це загальний довготерміновий план досягнення встановлених цілей, який базується на прогнозуванні ризиків та шляхах їх мінімізації. Тактика надає конкретні методи та техніки для вибору найкращого рішення та досягнення результатів в певних обставинах. Згідно з оцінками дослідників, можна вибрати такі типи стратегій управління ризиками [50]:

- індуктивну – збір, систематизація, узагальнення даних;

- дедуктивну – формулювання гіпотез та порівняння їх з реальними даними;
- позитивну – дослідження поточної ситуації;
- нормативну – створення суб'єктивних уявлень про майбутні події.

Управління ризиками включає в себе набір дій, спрямованих на збільшення ефективності бізнес-діяльності компанії та зниження (або, ідеально, повне усунення) потенційних втрат (збитків) під час проведення різноманітних операцій. Аналіз наукових думок та власні роздуми допомогли створити схему процесу управління ризиками (рис. 3.2).

На початковому етапі управління ризиками важливо оцінити економічну ситуацію та виявити всю сукупність ризиків, їх джерел і об'єктів. Спочатку ідентифікують найбільш ймовірні та небезпечні ризики, поступово переходячи до менш ймовірних і формуючи портфель ідентифікованих ризиків.

Це складний процес, який потребує високого рівня кваліфікації та глибокого розуміння особливостей економічних, технологічних, технічних та організаційних процесів. Виявлення може проводитися за допомогою набору формальних і неформальних методів та підходів, які базуються на використанні суб'єктивної або об'єктивної інформації. Для прийняття відповідних рішень на всіх стадіях управління ризиками необхідно мати достатньо інформації.

Аналіз рівня бізнес-ризиків є найбільш відповідальним та методологічно складним етапом процесу управління, від якого залежить загальна ефективність ризик-менеджменту. Він включає якісну та кількісну оцінку ризику, методи проведення якої описано в попередньому розділі.



Рисунок 3.2 – Процес управління ризиками господарської діяльності на підприємстві

Оскільки управління ризиками є частиною практичного менеджменту, воно вимагає постійного оцінювання та перегляду як самого припустимого рівня ризиків для певного підприємства, так і прийнятих рішень, у зв'язку з



постійною зміною внутрішніх та зовнішніх факторів, що впливають на його діяльність.

Після виявлення та оцінювання ризиків наступним кроком є етап регулювання рівня ризику, який включає два етапи:

- вибір методів управління ризиками (з оцінкою їх відносної ефективності на основі різних критеріїв);
- безпосереднє впливання на рівень ризиків шляхом виконання обраних методів зменшення ризику.

Протягом останнього десятиріччя відбулися зміни у розумінні ролі ризик-менеджменту в досягненні цілей організації. Тепер основна мета полягає не в усуненні ризику, а в запобіжній модифікації ризикового профілю підприємства та приведенні його у відповідність із системою своїх цілей.

На стадії оцінки результатів та їх налаштування відбувається визначення ступеня нейтралізації можливих втрат на основі системи показників ефективності, економічності та доцільності заходів (відношення витрат на регулювання рівня ризику до потенційних збитків), а також величини загального ризику бізнес-діяльності компанії, враховуючи проведені заходи для його оптимізації. Прийняття та виконання рішень щодо регулювання ступеня ризику також вимагає розробки та впровадження процедур контролю за процесом ризик-менеджменту.

Важливим етапом роботи ризик-менеджменту є планування дій щодо виконання запланованої програми управління ризиками – визначення типів заходів, обсягів та джерел їх фінансування, конкретних виконавців та термінів виконання. Під час процесу управління ризиками бізнес-діяльності також повинен проводитися нагляд за прогресом виконання дій з ризик-менеджменту.

Ризик-менеджмент визначає свої власні правила для прийняття рішень в умовах невизначеності, вимагаючи завжди враховувати можливі наслідки ризиків. Позитивні рішення слід приймати лише у відсутності сумніву, уникаючи значущих ризиків заради незначних та вдаючись до альтернативних рішень.

Формування системи ризик-менеджменту на підприємстві є важливим етапом для забезпечення ефективного управління ризиками і досягнення стратегічних цілей.

На рис. 3.3. наведено етапи формування системи ризик-менеджменту.

Перший етап передбачає визначення мети та стратегії:

- розробка чіткої стратегії підприємства та визначення цілей;
- виявлення найбільш впливових ризиків на досягнення цілей.

На другому етапі здійснюється ідентифікація ризиків, що передбачає:

- аналіз усіх сторін діяльності підприємства;
- визначення потенційних ризиків, які можуть виникнути в процесах, проектах, фінансовій діяльності та інших сферах.

На третьому етапі запропонованого підходу здійснюється оцінка ризиків, що передбачає:

- оцінку ймовірності виникнення кожного ризику та його потенційних наслідків;
- використання кількісних та якісних методів оцінки ризиків.

Четвертий етап запропонованого підходу передбачає визначення стратегії управління ризиками, який містить такі підетапи:

- розробка стратегії для кожного визначеного ризику (уникання, зменшення, передача чи прийняття ризику);
- розробка конкретних заходів для втручання у разі виникнення ризиків.



Рисунок 3.3 – Основні етапи формування системи ризик-менеджменту на підприємстві

На п'ятому етапі здійснюється моніторинг і контроль, що передбачає:

- розробку системи моніторингу ризиків;
- визначення відповідальних за моніторинг та введення системи звітності.

На шостому етапі запропонованого підходу передбачаються заходи щодо залучення персоналу, серед яких:

- навчання персоналу щодо ризиків та методів управління ними;
- визначення ролі та відповідальності з управління ризиками.

Сьомий етап запропонованого підходу передбачає проведення аудиту та оновлення системи ризик-менеджменту, у межах чого:

- здійснюється систематичний аудит системи ризик-менеджменту;
- здійснюється оновлення стратегії та методів управління ризиками відповідно до змін в оточенні підприємства.

На останньому восьмому етапі запропонованого підходу передбачається впровадження технологій, у межах чого здійснюється:

- визначення можливості використання інформаційних систем для збору та обробки даних щодо ризиків;
- визначення ймовірних інформаційних ризиків.

Система ризик-менеджменту є динамічною та повинна адаптуватися до змін внутрішнього та зовнішнього середовища підприємства.

Отже, управління господарськими ризиками спрямоване на ідентифікацію, аналіз та регулювання всіх видів ризиків підприємства у його операційній, фінансовій та стратегічній діяльності. Завершальною метою ризик-менеджменту є досягнення цільової функції підприємства, яка полягає в тому, що відбувається отримання найбільшого прибутку за оптимального, прийняттого для суб'єкта господарювання, рівня ризику.

### 3.2 Рекомендації щодо управління ризиком рейдерського захоплення для АТ «Інститут інформаційних технологій»

Сучасний етап розвитку інвестиційних процесів в Україні характеризується зростанням явища рейдерства. Компанії часто виявляються беззахисними перед спробами незаконного захоплення їх власності, тому їм необхідно визначити конкретні заходи протидії рейдерам. Однак, не кожна компанія може стати об'єктом інтересу рейдерів. Тому, щоб зберегти свої фінансові ресурси від непотрібної боротьби з маловірогідним ризиком захоплення, потрібна спеціальна методика, яка дозволить оцінити ймовірність виникнення такого ризику, як ризик рейдерського захоплення, в діяльності підприємства.

У результаті проведених досліджень було визначено ряд факторів, що сприяють виникненню ризику рейдерського захоплення підприємства (рис. 3.4) [55-58]:

- потенційна фінансова привабливість підприємства;
- низька відомість підприємства серед звичайних громадян;
- монопольний (або домінуючий) статус підприємства на ринку;
- кількість акціонерів на підприємстві;
- можливість подальшого перепродажу підприємства;
- наявність умов для стабільної роботи підприємства.

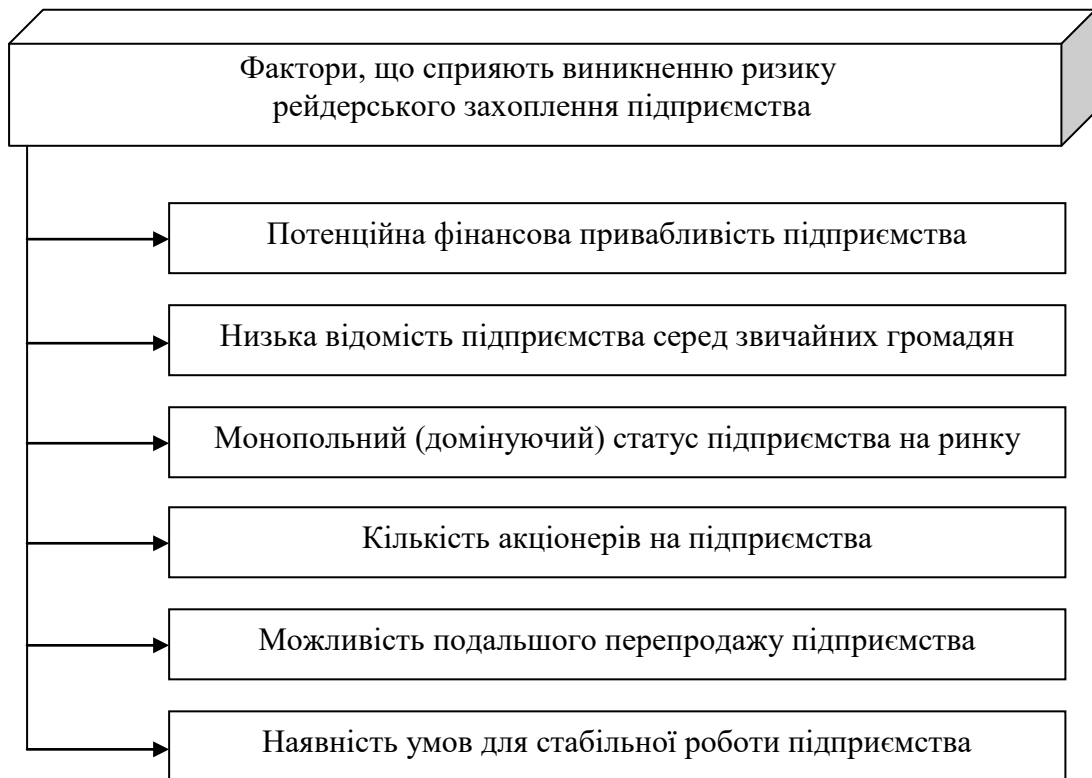


Рисунок 3.4 – Фактори, що сприяють виникненню ризику рейдерського захоплення підприємства

На основі бальної оцінки окремих показників, що відображають зазначені фактори, та контент-аналізу публікацій на досліджувану тему можна встановити значущість кожного з них.

Підприємства в умовах сучасної української економіки повинні мати ефективну систему управління ризиками, що можуть виникнути на різних етапах та в окремих складових їх діяльності. Одним з головних ризиків, що негативно впливають на діяльність українських підприємств, зокрема на їх інвестиційну складову, є ризик рейдерського захоплення. Оскільки держава фактично не може гарантувати інвестору збереження його коштів, вкладених у певні об'єкти власності, інвестор повинен мати засоби для захисту себе від напівлегальних і навіть відкрито незаконних дій агресорів. Таким чином, сучасному українському підприємству необхідна певна модель управління ризиком рейдерського захоплення.

Якісна модель управління цим ризиком повинна бути ефективною з економічного погляду та практичною від точки зору реалізації. Досягнення цього можливе шляхом оцінки привабливості підприємства для рейдерів, оскільки не кожне підприємство може потрапити у коло їхніх інтересів. Проте, соціальний відгук на досліджувану проблему може стимулювати власників численних компаній до впровадження надлишкових заходів захисту своєї власності, що може негативно відобразитися на їхній діяльності. Отже, заходи захисту, які реалізуються компаніями, мають бути пропорційні рівню ризику його вилучення.

Практична ефективність заходів захисту підприємства є дуже важливою. Власники та керівництво не повинні діяти випадково під час виконання захисних дій. Іншими словами, вони повинні мати змогу передбачати дії агресорів, прогнозувати їх та використовувати це на свою вигоду, маючи повну інформацію про фінансовий стан, активи, контрагентів свого підприємства тощо. Правильно оцінивши доступну інформацію, вони зможуть самостійно виявити свої слабкі місця та розробити конкретні заходи для їх усунення.

Таким чином, ефективна модель управління ризиком рейдерського захоплення повинна включати наступні етапи (рис. 3.5):

- оцінка ризику рейдерського захоплення підприємства, тобто його потенційної привабливості для рейдерів;
- аналіз характеристик діяльності підприємства з метою виявлення потенційних методів захоплення;
- виявлення та розробка заходів з впровадження ефективного методу захисту підприємства.

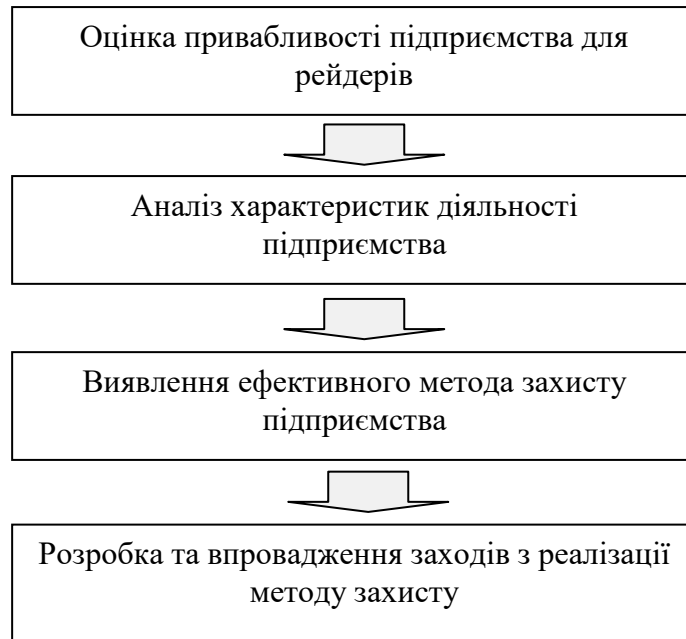


Рисунок 3.5 – Етапи управління ризиком рейдерського захоплення підприємства

На початковому етапі управління визначається, чи взагалі існує ризик захоплення в діяльності підприємства. Якщо після оцінки привабливості підприємства в його діяльності виявляється досліджуваний ризик, воно повинне впроваджувати систему управління ризиком рейдерського захоплення, тобто переходити до наступного етапу – етапу виявлення слабких сторін. Якщо під час аналізу характеристик критичних і навіть небезпечних ланок не виявлено, підприємство також може утриматися від активних захисних дій, але слід враховувати, що воно потенційно є привабливим для агресорів. Тому необхідно обов'язково відстежувати ситуацію на підприємстві та запобігати виникненню слабких ланок в його діяльності та документації.

Підприємство, в діяльності якого були виявлені небезпечні та критичні ланки характеристик, повинно перейти до наступного етапу управління ризиком рейдерського захоплення – вибору відповідного до потенційного



методу захоплення методу захисту та впровадження його на підприємстві через низку відповідних заходів.

Таким чином, захисні дії проти рейдерського захоплення підприємства повинні бути своєчасними та відповідними реальному ризику настання такої події та слабким ланкам організації діяльності підприємства, через які таке захоплення ймовірне. Лише у такому випадку можлива побудова ефективної системи захисту від ризику рейдерського захоплення підприємства.

На основі розроблених рекомендацій [55-58] формується список ефективних захисних заходів для підприємств. Виявлені слабкі ланки в їх діяльності дозволяють визначити наступні потенційні методи захоплення (в порядку поширення):

- витіснення менших акціонерів;
- використання кредиторської заборгованості;
- маніпуляції з реєстром (головним чином як додатковий захід при реалізації інших методів, пов'язаних з захопленням через акціонерний капітал);
- конфлікт між мажоритарними акціонерами.

Для захисту від ризику рейдерського захоплення компанії можуть використовувати різноманітні заходи, що спрямовані на ускладнення або уникнення таких сценаріїв. У результаті аналізу методів захоплення з точки зору їх реального застосування для АТ «Інститут інформаційних технологій» запропоновано рекомендації, що наведено у таблиці 3.1.

Таким чином, більшість підприємств мають спільні слабкі місця в таких аспектах, як: статутні документи, організація реєстрації та голосування акціонерів на загальних зборах, процес прийняття рішень, розподіл обов'язків між керівними органами, обмеження правління при прийнятті окремих рішень.

Таблиця 3.1 – Заходи від ризику рейдерського захоплення для АТ «Інститут інформаційних технологій»

Група заходів	Вид заходу	Зміст заходу
1. Статутні заходи	Розділена Наглядова рада	Створення системи розділеної наглядової ради, де термін повноважень кожного члена закінчується в різний час, може ускладнити рейдерське захоплення
	Золоті парашути	Включення у трудові договори з керівництвом «золотих парашутів» (golden parachutes) – великих вихідних виплат при зміні власника – може відлякати потенційних захопників
2. Фінансові заходи	Викуп власних акцій	Компанія може використовувати стратегію викупу власних акцій, щоб підняти їхню вартість і робити поглинання менш вигідним
	Отруйні пігулки	Застосування «отруйних пігулок» (poison pills) – прав акціонерів на купівлю додаткових акцій зі знижкою – може додатково ускладнити рейдерське захоплення
3. Юридичні заходи	Клаузули про заповітність та конфіденційність	Включення в угоди та договори клаузулей, які обмежують передачу конфіденційної інформації сторонам, може захистити компанію від потенційних захопників
	Захист активів	Забезпечення надійного захисту ключових активів та патентів може ускладнити спроби рейдерського захоплення
4. Стратегічні заходи	Пошук «Білого лицаря»	Активний пошук потенційних стратегічних партнерів або «білих лицарів» (white knights), які можуть виявитися більш привабливими захопникам, може змусити їх відмовитися від поглинання
	Стратегічне планування	Розробка та виконання стратегічного планування, яке максимізує цінність компанії для акціонерів, може взаємодіяти з рейдерськими спробами
5. Комунікації	Ефективна внутрішня та зовнішня комунікація	Забезпечення ефективної комунікації з акціонерами, клієнтами, та працівниками щодо стратегій та перспектив компанії може зменшити підтримку для рейдерів

Ці заходи можуть варіюватися в залежності від конкретних умов і характеристик компанії. Важливо ретельно аналізувати ситуацію та вибирати стратегії, які найкраще відповідають конкретним обставинам.

Щодо аналізу технологій захоплення, безперервно розробляються нові стратегії для захисту компаній від потенційних корпоративних захоплень. Сучасний світ використовує різні підходи, які можна узагальнити як «не операційні» та «операційні» методи, і їх застосування розглядається в контексті ситуації в Україні.

До «не операційних» стратегій входять розділена рада акціонерного товариства (staggered board), «отруйні пігулки» (poison pills) і «золоті парашути» (golden parachutes). Наприклад, розділена наглядова рада акціонерного товариства передбачає, що склад ради обирається таким чином, що строк повноважень членів закінчується регулярно тільки для частини ради. Це означає, що реальне переобрання більшості членів стає можливим лише через декілька років після спроби захоплення.

Також на практиці використовуються стратегії для ускладнення можливості дострокового звільнення членів наглядової ради та визначення кваліфікованої більшості (3/4) для ухвалення ключових рішень. «Отруйні пігулки» надають право акціонерам придбати додаткові акції за значними знижками та викуп власних акцій з премією. «Золоті парашути» передбачають значні вихідні виплати для керівництва та інших працівників компанії у випадку зміни власника, роблячи вартість поглинання занадто великою для потенційного захопника і тим самим сприяючи опору.

Натомість «операційні» методи захисту включають «дорогоцінності корони» (crown jewels), «акулячу отруту» (shark repellent), викуп власних акцій (shares buy-back), «білого лицаря» (white knight), «зелену броню», та «захист пекмен» (rampart defense). «Білий лицар» передбачає пошук дружньої компанії, яка згодна придбати чи здійснити інвестицію у компанію. Використання «дорогоцінностей корони» передбачає продаж чи передачу ключових активів для ускладнення процесу поглинання. «Акуляча отрута» включає угоди з кредиторами та інші заходи, щоб зробити поглинання менш вигідним. Викуп власних акцій, «зелена броня», та «захист пекмен» – це інші стратегії, які можуть використовуватися для захисту компанії від недружніх поглинань.

Застосування запропонованих заходів дозволить виявити ключові напрями захисту від ризику рейдерського захоплення: оптимізація структури

та обсягів пакетів акцій мажоритарних акціонерів, максимальне збільшення пакету акцій основного мажоритарного акціонера, моніторинг кредиторської заборгованості, формування ефективної дивідендної політики.

Запропоноване організаційне забезпечення дозволить впровадити на підприємстві ефективну систему управління ризиком рейдерського захоплення, перевагою якої є врахування реального рівня ризику та характеристик діяльності в умовах конкретного підприємства.

### 3.3 Структурно-логічна характеристика результатів дослідження

Структурно-логічна характеристика результатів дослідження наведена на рис. 3.6.

Отримані результати дослідження розділено на групи: теоретичні, аналітичні, практичні.

У межах теоретичних результатів роботи:

- розкрито економічний зміст та етапи управління ризиками в контексті забезпечення економічної безпеки підприємства;
- розглянуто сутність ризику рейдерських захоплень підприємства;
- здійснено огляд сучасних методів оцінки ризиків діяльності підприємства.

У другому розділі роботи:

- проаналізовано фінансові результати діяльності АТ «Інститут інформаційних технологій»;
- досліджено практичні методи оцінки ризиків, що використовуються в АТ «Інститут інформаційних технологій».



Рисунок 3.6 – Структурно-логічна схема результатів дослідження

У третьому розділі роботи:

- запропоновано концептуальний підхід до формування системи ризик-менеджменту на підприємстві;
- розроблено практичні рекомендації щодо управління ризиком рейдерського захоплення для АТ «Інститут інформаційних технологій».

Сфера використання результатів роботи – система функціонування економічної безпеки підприємства.

У межах структурно-функціонального опису використання практичних результатів зазначено:

- функціональне призначення (управління ризиками в системі економічної безпеки підприємства);
- структурна належність (служба безпеки; фінансово-економічний відділ; інші відповідні функціональні підрозділи);
- склад користувачів (директор підприємства; - заступники директора; керівники відповідних підрозділів).

Напрями практичного використання результатів дослідження:

- державні та приватні підприємства;
- корпоративні бізнес-структури;
- консалтингові фірми

Перспективою подальших досліджень є розробка методичного інструментарію та програмного забезпечення оцінки ризиків в системі економічної безпеки підприємства

## ВИСНОВКИ

У першому розділі роботи розглянуті теоретичні аспекти управління ризиками в контексті забезпечення економічної безпеки підприємства.

Розкрито економічний зміст та етапи управління ризиками в контексті забезпечення економічної безпеки підприємства.

Сутність поняття «економічна безпека» розглядається різними науковцями індивідуально. Вона може бути визначена як стан підприємства, що забезпечує йому здатність протидіяти несприятливим зовнішнім впливам. Економічна безпека також охоплює корпоративні ресурси та підприємницькі можливості, гарантуючи їхнє ефективне використання для стабільного функціонування та розвитку.

Наведено етапи процесу управління ризиками в контексті забезпечення економічної безпеки.

Управління ризиками в контексті забезпечення економічної безпеки підприємства є важливою складовою стратегічного управління і включає в себе ряд економічних аспектів:

- мінімізація втрат;
- оптимізація фінансових ресурсів;
- забезпечення стійкості підприємства;
- збереження репутації;
- сприяння інноваціям та розвитку;
- відповідність законодавчим вимогам.

У цілому, управління ризиками та економічна безпека взаємодіють, формуючи цілісний підхід до забезпечення стійкості та процвітання підприємства в динамічному економічному середовищі.

Розкрито сутність ризику рейдерських захоплень підприємства.

Загалом рейдерство розглядається як прояв недоліків у політичних та правових структурах влади в країні, недосконалості чинного законодавства, відсутності належних умов для захисту бізнесу, прав власників та рівноправної конкуренції.

Рейдери – це група висококваліфікованих фахівців, які спеціалізуються на захопленні компанії або перехопленні контролю за допомогою спеціально спланованого бізнес-конфлікту. Основна мета рейдерства – підкорення великого бізнесу, великих компаній, підприємств, захоплення великих площ, земельних ділянок, обладнання та нерухомості.

Представлена схема проведення рейдерських операцій.

Графічно наведено основні способи захоплення підприємства.

Придбання акцій може здійснюватися шляхом відмовної купівлі-продажу акцій для отримання блокуючого або контрольного пакету акцій. Додаткова емісія акцій або аналогічний метод придбання підприємства. Банкрутство, яке є витратним методом придбання, передбачає «придбання» кредитної заборгованості від бізнес-партнерів, укладання угод з банківськими та іншими фінансовими організаціями, формування конкурсної комісії і т. д.

Реприватизація, яка є законним способом придбання, включає в себе анулювання судового рішення з наступним переглядом процесу приватизації. Цивільний позов може бути ініційований як акціонерами, так і представниками держави (з метою подальшого перерозподілу власності).

Корпоративний шантаж (грінмейлінг, юридичний терор, послуга, яка сприяє придбанню або рейдерству) часто є самостійним, високоприбутковим видом бізнесу, який не передбачає здійснення контролю над компанією.

Допемісія – це ключовий метод захоплення контролю над підприємством, який використовується для відсторонення непотрібного міноритарного акціонера.



Силове захоплення включає в себе залучення силових структур (спеціальних підрозділів правоохоронних органів, приватних охоронних служб) та використання фальшивого судового рішення.

Встановлення контролю над керівництвом (застосовується до державних підприємств, господарських товариств, основним акціонером яких є держава, реалізується через підкуп, шантаж або загрози керівництву компанії).

Фіктивне банкрутство (порушення діючого законодавства про банкрутство, штучне створення податкової та кредиторської заборгованості, висунення кандидатури свого керівника).

Корупція, яка є необхідною умовою рейдерства, особливо важлива під час перерозподілу державної власності.

Здійснено огляд сучасних методів оцінки ризиків діяльності підприємства.

Якісний аналіз ризику є одним з найважчих завдань в економічній ризикології. Основне завдання якісної оцінки полягає в визначенні потенційних видів ризиків та факторів, які впливають на рівень ризиків при виконанні певного виду діяльності.

Наведена характеристика методів якісної оцінки рівня ризику.

Метою кількісного аналізу є отримання числового вираження окремих ризиків з визначенням характеристик ймовірності та можливих втрат. Для цього формується набір сценаріїв, і для окремих ризиків можуть бути побудовані функції розподілу ймовірності виникнення втрат в залежності від їх обсягу.

Наведено характеристику основних методів кількісної оцінки ризиків підприємства.

У другому розділі роботи проаналізовано результати господарської діяльності та практичні методи оцінки ризиків АТ «Інститут інформаційних технологій».

Приватне акціонерне товариство «Інститут інформаційних технологій» (АТ «ІТ») спеціалізується на наданні послуг у сфері проектування, розробки та впровадження рішень щодо забезпечення безпеки інформації у інформаційно-телекомунікаційних системах різного призначення та рівня складності.

Наведено організаційну структуру управління підприємства.

Основні напрями діяльності компанії включають захист інформації у інформаційно-телекомунікаційних системах, створення засобів та комплексів технічного захисту інформації, експертизу та аудит інформаційної безпеки.

АТ «ІТ» володіє потужним парком обчислювальної техніки та периферійного обладнання, необхідного для проектування, розробки, тестування та вихідного контролю продукції власного виробництва, яке є власністю підприємства.

Проаналізовано основні показники, що характеризують фінансово-економічні результати діяльності АТ «Інститут інформаційних технологій».

У 2022 році чистий дохід від реалізації продукції склав 75,416 тис. грн, що на 50,8% перевищує рівень 2021 року. Також спостерігалася тенденція до збільшення собівартості реалізованої продукції.

Собівартість реалізованої продукції в 2022 році становила 52,415 тис. грн, що на 80,7% більше, ніж у 2021 році.

Сума валового прибутку склала в 2022 році 23,001 тис. грн, що вище рівня 2021 року на 9,5 %.

Чистий прибуток у 2022 році знизився на 11,1 % (1226,0 тис. грн) порівняно з 2021 роком і склав 9780 тис. грн.

Рентабельність продукції у 2022 році знизилася на 28,5% і становила 43,9 %, що можна розглядати як негативну тенденцію у результатах діяльності підприємства.

Наведено динаміку дебіторської та кредиторської заборгованостей підприємства за 2021-2022 рр.

Проаналізовано склад і структуру операційних витрат досліджуваного підприємства.

Слід зазначити, що «Витрати на оплату праці» мають найбільший внесок у структурі операційних витрат: у 2021 р. – 48,6%, у 2022 р. – 54,5%. Другим за величиною видом витрат є «Відрахування на соціальні заходи»: у 2021 р. – 28,1%, у 2022 р. – 26,6%, що можна розцінювати як позитивну тенденцію на підприємстві.

Таким чином, основні показники фінансово-господарської діяльності підприємства в аналізованому періоді мають позитивну тенденцію. Така динаміка поліпшення основних показників діяльності підприємства підвищує його інвестиційну привабливість і разом з тим збільшує загальну привабливість підприємства для рейдерського захоплення.

Виходячи з цього, керівництво АТ «ІТ» прагне розробити та впровадити в практику науково-обґрунтовані методи оцінювання ризиків з метою забезпечення економічної безпеки підприємства.

У третьому розділі роботи запропоновано концептуальний підхід до формування системи ризик-менеджменту на підприємстві.

Оскільки ризик є економічною категорією, на його ступінь можна впливати через формування та реалізацію стратегії, використання певних засобів, принципів, тобто через створення своєрідного механізму управління ризиками – ризик-менеджменту.

Сутність ризик-менеджменту полягає в здійсненні комплексу економічних, організаційних та технічних заходів, спрямованих на визначення видів, факторів та джерел ризику, оцінку їхньої величини, а також розробку та впровадження заходів для зниження рівня ризику та запобігання можливим негативним наслідкам

Відповідно до сучасної концепції управління ризиками, ризик-менеджмент може бути визначений як система або процес. Як система управління, ризик-менеджмент включає об'єкти управління – підсистему, що керується, та суб'єкти управління – керуючу підсистему.

Наведено структурно-логічну схему системи ризик-менеджменту.

Функції керуючої підсистеми охоплюють організацію вирішення питань, пов'язаних з ризиком та капіталовкладеннями, здійснення заходів з зниження рівня ризику, управління процесом страхування ризиків, а також економічних відносин і зв'язків між суб'єктами господарювання.

Процес ризик-менеджменту включає в себе формування стратегічних та тактичних рішень. Стратегія ризик-менеджменту – це загальний довготерміновий план досягнення встановлених цілей, який базується на прогнозуванні ризиків та шляхах їх мінімізації. Тактика надає конкретні методи та техніки для вибору найкращого рішення та досягнення результатів в певних обставинах.

Наведено схематично процес управління ризиками господарської діяльності на підприємстві.

Формування системи ризик-менеджменту на підприємстві є важливим етапом для забезпечення ефективного управління ризиками і досягнення стратегічних цілей.

Тому у роботі запропоновано до практичного використання етапи формування системи ризик-менеджменту.

Система ризик-менеджменту є динамічною та повинна адаптуватися до змін внутрішнього та зовнішнього середовища підприємства.

Отже, управління господарськими ризиками спрямоване на ідентифікацію, аналіз та регулювання всіх видів ризиків підприємства у його операційній, фінансовій та стратегічній діяльності. Завершальною метою ризик-менеджменту є досягнення цільової функції підприємства, яка полягає в тому, що відбувається отримання найбільшого прибутку за оптимального, прийняттого для суб'єкта господарювання, рівня ризику.

У результаті проведених досліджень у роботі запропоновано практичні рекомендації щодо управління ризиком рейдерського захоплення для АТ «Інститут інформаційних технологій».

Систематизовано фактори, що сприяють виникненню ризику рейдерського захоплення підприємства:

- потенційна фінансова привабливість підприємства;
- низька відомість підприємства серед звичайних громадян;
- монопольний (або домінуючий) статус підприємства на ринку;
- кількість акціонерів на підприємстві;
- можливість подальшого перепродажу підприємства;
- наявність умов для стабільної роботи підприємства.

Ефективна модель управління ризиком рейдерського захоплення повинна включати наступні етапи:

- оцінка ризику рейдерського захоплення підприємства, тобто його потенційної привабливості для рейдерів;
- аналіз характеристик діяльності підприємства з метою виявлення потенційних методів захоплення;
- виявлення та розробка заходів з впровадження ефективного методу захисту підприємства.

Для захисту від ризику рейдерського захоплення компанії можуть використовувати різноманітні заходи, що спрямовані на ускладнення або уникнення таких сценаріїв. У результаті аналізу методів захоплення з точки зору їх реального застосування для АТ «Інститут інформаційних технологій» запропоновано практичні рекомендації.

Запропоноване організаційне забезпечення дозволить впровадити на підприємстві ефективну систему управління ризиком рейдерського захоплення, перевагою якої є врахування реального рівня ризику та характеристик діяльності в умовах конкретного підприємства.

Основні результати досліджень опубліковано в роботах [59, 60], копії яких наведено в додатку А.

## ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Сучасне управління: ризики, виклики, безпека, перспективність використання та проблеми впровадження в державному та приватному секторах економіки : колект. монографія / ред.: Н. Е. Аванесова, О. Чупир, Д. Терещенко, Т. Андрєєва, О. Гетьман. Харків: Панов А. М. , 2021. 634 с.
2. Тютченко С. М. Забезпечення економічної безпеки підприємств в умовах трансформаційних змін в економіці: монографія; Дніпропетровський державний університет внутрішніх справ. Дніпро: Біла К. О., 2021. 211 с.
3. Бойченко М. В. Розробка механізму управління професійними ризиками. *Актуальні проблеми економіки*. 2015. № 10. С. 435-443.
4. Герасимчук Н. А., Мірзоєва Т. В., Томашевська О. А. Економічні і фінансові ризики: навч. посіб.; Нац. ун-т біоресурсів і природокористування України. Київ: Компринт, 2015. 288 с.
5. Камінський С. І. Управління ризиками в процесі управління фінансовим циклом підприємства торгівлі. *Актуальні проблеми економіки*. 2017. № 9. С. 117-125.
6. Кондрашихін, А.Б. Теорія та практика підприємницького ризику: навчальний посібник. Київ: ТОВ «Центр учбової літератури», 2009. 224 с.
7. Антонова О. М. Основні типи та характеристика негативного впливу на економічну безпеку підприємства. *Актуальні проблеми економіки*. 2015. № 2. С. 189-194.
8. Бойченко М. В. Управління професійними ризиками: теорія і практика : монографія; НАН України, Ін-т економіки пром-сті, ДВНЗ «Нац. гірн. ун-т». Київ: ІЕП НАН України, 2015. 295 с.
9. Загурський О. М. Управління ризиками: навч. посіб. Київ: Ун-т «Україна», 2017. 242 с.

10. Макаренко І. О. Особливості управління господарським ризиком в умовах ринкової економіки. *Актуальні проблеми економіки*. 2006. № 6 (60). С. 159-164.
11. Гринкевич С. С., Іляш О. І., Кокнаєва М. О. Стратегічні імперативи управління фінансово-економічною безпекою підприємств торгівлі: монографія; Львів. комерц. акад. Львів, 2015. 209 с.
12. Фінансово-економічна безпека: стратегічна аналітика та аудиторський супровід: монографія / ред.: Т. В. Момот; Харків. нац. ун-т міськ. госп-ва ім. О. М. Бекетова. Харків : ХНУМГ ім. О. М. Бекетова, 2015. 340 с.
13. Онищенко О. В., Яценко Н. М., Гончаренко Н. О. Роль економічної безпеки у стратегічному управлінні промисловим підприємством. *Міжнародний науковий журнал «Інтернаука». Серія: Економічні науки*. 2022. № 4. С. 119-127.
14. Polozova T.V., Nicola Jennifer John Elia. Enterprise economic security system: theoretical aspects of formation. Економічні та безпекові виклики сучасного бізнес-середовища: колективна монографія / За заг. ред. д.е.н., проф. Т. В. Полозової. Харків: ХНУРЕ, 2020. С. 355-362.
15. Герасименко Л. В. Формування системи адаптивно-орієнтованого управління економічною безпекою підприємства. *Ефективна економіка*. 2021. № 4. URL: [http://nbuv.gov.ua/UJRN/efek\\_2021\\_4\\_34](http://nbuv.gov.ua/UJRN/efek_2021_4_34). (дата звернення 28.11.2022)
16. Шмалій Л. В., Ількевич М. В. Управління економічною безпекою підприємства. *Економіка. Менеджмент. Бізнес*. 2020. № 4. С. 68-73.
17. Ткаченко Т. П. Просторові виклики та ризики впливу на систему економічної безпеки підприємств промисловості України та напрями їх пом'якшення. *Economic synergy*. 2022. Iss. 4. С. 239-247.



18. Марченко О. С., Шевченко Л. С. Підприємництво в конкурентному середовищі: ризики, дисбаланси та безпека. *Економічна теорія та право*. 2023. № 2. С. 24-47.

19. Корнієнко Т. О. Вплив загроз та ризиків на формування системи економічної безпеки підприємства. *Міжнародний науковий журнал «Інтернаука»*. Серія: Економічні науки. 2022. № 4. С. 43-48.

20. Бабич Т. Рейдерство в Україні – загроза національній безпеці. URL: <http://www.viche.info/journal/2105/>.

21. Економічна безпека підприємства в умовах рейдерських загроз: колект. монографія / О. А. Бурбело, С. К. Рамазанов, О. М. Заєць, Т. С. Гудіма, О. М. Кузьменко; ред.: О. А. Бурбело, С. К. Рамазанов; НАН України, Ін-т екон.-прав. дослідж., Одес. нац. ун-т внутр. справ, Східноукр. нац. ун-т ім. В. Даля, Київ. нац. екон. ун-т ім. В. Гетьмана. Київ: Вид-во СНУ ім. В. Даля, 2015. 285 с.

22. Ніпіаліді О. Ю. Рейдерство як реальна загроза безпеці власника бізнесу в Україні. *Правова держава*. 2019. № 34. С. 83-88.

23. Згадова Н. С., Рогатіна Л. П., Губко В. І. Рейдерство в Україні – загроза економічній безпеці підприємств. *Економічний простір*. 2020. № 159. С. 49-52.

24. Тульчинська С. О., Солосіч О. С. Теоретичні та прикладні аспекти організації рейдерської діяльності як ключова загроза забезпеченню силової складової економічної безпеки підприємства. *Ефективна економіка*. 2020. № 12. URL: [http://nbuv.gov.ua/UJRN/efek\\_2020\\_12\\_3](http://nbuv.gov.ua/UJRN/efek_2020_12_3).

25. Федоров Е. Оцінка економічних ризиків безпекового розвитку України. *Журнал європейської економіки*. 2023. Т. 22. № 2. С. 188-212.

26. Вдовин М. Л., Данилюк Л. Г., Лелик Л. І., Березяк І. Г., Мельник О.-С.М. Моделі та методи оцінювання економічних ризиків у різних функціональних сферах бізнесу: монографія. Львів: АТБ, 2015. 247 с.

27. Економічний ризик: методи оцінки та управління : навч. посіб. для студентів і викладачів екон. спец. ВНЗ / уклад.: Т. А. Васильєва, С. В. Леонов, Я. М. Кривич; ДВНЗ «Укр. акад. банк. справи Нац. банку України». Суми, 2015. 207 с.

28. Вітлінський В.В., Верченко П. І., Сігал А. В., Наконечний Я. С. Економічні ризики: ігрові моделі: навч. посіб. Київ: КНЕУ, 2002. 446 с.

29. Куцик П. О., Васильців Т. Г., Сороківський В. М., Стефаняк В. І., Сороківська М. В., Куцик П. О. Управління фінансовими ризиками: навч. посіб.; Укоопспілка, Львів. торг.-екон. ун-т. Львів : Растр-7, 2016. 317 с.

30. Федулова І. В., Скопенко Н. С. Економічні ризики та методи їх вимірювання: навч. посіб. для студентів екон. спец. Київ: Компринт, 2016. 292 с.

31. Донець Л. І. Економічні ризики та методи їх вимірювання: навч. посіб. Київ: Центр навчальн. літ-ри, 2006. 312 с.

32. Внукова Н. М., Смоляк В. А. Економічна оцінка ризику діяльності підприємств: проблеми теорії та практики: монографія. Харків: ВД «ІНЖЕК», 2006. 184 с.

33. Економічний ризик: практикум / З. Б. Артим-Дрогомирецька, І. Б. Романич; Львів. нац. ун-т ім. І. Франка. Львів: Вид-во Т. Сороки, 2008. 186 с.

34. Верченко П.І. Багатокритеріальність і динаміка економічного ризику (моделі та методи) : монографія; Київ. нац. екон. ун-т ім. В.Гетьмана. Київ, 2006. 272 с.

35. Старостіна А. О., Кравченко А. Ризик-менеджмент теорія і практика: навч. посіб. Київ: ІВЦ «Видавництво «Політехніка», 2009. 200 с.

36. Економіка і управління підприємствами: теорія, методика, практика: колект. монографія / В. М. Антоненко та ін.; Центр фінанс.-екон. наук. дослідж. Полтава: Астроя, 2020. 240 с.

37. Економіка підприємства: підручник / Л. Л. Лазебник, В. Г. Бодров, В. В. Гурочкіна, Г. М. Калач, Г. П. Ляшенко, О. І. Марченко, Г.С. Мельничук, І. В. Минчинська, О. І. Піжук, Н. О. Ружинська, Л. В. Слюсарева, В. В. Ткаченко; ред.: Л. Л. Лазебник; Університет державної фіскальної служби України. Ірпінь: Ун-т ДФС України, 2021. 425 с.

38. Економіка і фінанси підприємства: навч. посіб. / І. М. Метошоп [та ін.]; [за заг. ред. І. М. Метошоп]; Івано-Франків. нац. техн. ун-т нафти і газу, Каф. приклад. економіки, Каф. фінансів. Івано-Франківськ: ІФНТУНГ, 2020. 490 с.

39. Ефективність управління бізнес-процесами підприємства: навч. посіб. / уклад.: О. М. Світовий; Уманський державний педагогічний університет імені Павла Тичини. Умань: Сочінський М. М., 2022. 202 с.

40. Караван Н. А., Чернявська І. М. Економіка та організація виробництва: навч. посіб.; Дніпровський державний технічний університет. Кам'янське: ДДТУ, 2022. 396 с.

41. Куцик В. І., Кліпкова О. І. Економіка і управління підприємствами у схемах і таблицях: навч. посіб.; Центр спілка спожив. т-в України, Львів. торг.-екон. ун-т. Львів: Вид-во Львів. торг.-екон. ун-ту, 2020. 315 с.

42. Основи економіки та підприємництва: навч. посіб. / уклад.: С. А. Жуков; «Ужгородський національний університет», державний вищий навчальний заклад. Ужгород: Говерла, 2021. 398 с.

43. Прикладна економіка: підручник / Б. О. Язлюк, А. І. Гулей, О. О. Красноручський, Т. А. Власенко, А. М. Бутов; ред.: Б. О. Язлюк; Західноукраїнський національний університет. Тернопіль: ЗУНУ, 2021. 373 с.

44. Сментина Н. В., Балджи М. Д., Доброва Н. В., Клевцевич Н. А., Маркітан О. С., Осипова М. М., Однолько В. О., Фіалковська А. А. Економіка та організація підприємницької діяльності: навч. посіб.; ред.: Н. В. Сментина; Одес. нац. екон. ун-т. Київ: Гуляєва В.М., 2019. 320 с.

45. Трегубов О. С., Ахновська І. О., Андронік О. Л., Баглюк Ю. Б., Болгов В. Є., Воронін А. В., Солоненко Ю. В. Економіка підприємства: навч. посіб. [для студентів ВНЗ]; ред.: О. С. Трегубов; Донец. нац. ун-т ім. В. Стуса. Вінниця: ТВОРИ, 2019. 228 с.

46. Шандова Н. В. Мешкова-Кравченко Н. В., Латкіна С. А. Економіка підприємства: навч. посіб. для студентів закл. вищ. освіти; Херсонський національний технічний університет. Херсон: Вишемирський В. С., 2021. 335 с.

47. Концептуальні засади формування фінансово-економічної безпеки: колект. монографія / [Абакуменко О. І. та ін.]; за заг. ред. д-ра екон. наук, проф. Шкарлета Сергія Миколайовича; Черніг. нац. технол. ун-т. Ніжин: Лук'яненко В.В.: Орхідея, 2015. 440 с.

48. Антикризові технології в управлінні економічною безпекою підприємства: монографія / М. М. Караїм, В. В. Мартинів, А. М. Штангрет, Я.В. Котляревський, Л. Є. Сухомлин, Ю. В. Ратушняк; ред.: А. М. Штангрет; Укр. акад. друкарства. Львів: Укр. акад. друкарства, 2021. 249 с.

49. Новик І. В. Проблеми та перспективи забезпечення економічної безпеки підприємства в Україні. *Інфраструктура ринку*. 2020. Вип. 43. С. 229-233.

50. Мостенська Т. Л., Білан Ю. В., Мостенська Т. Г. Ризик-менеджмент як чинник забезпечення економічної безпеки підприємств. *Актуальні проблеми економіки*. 2015. № 8. С. 193-203.

51. Черняк О. Л., Чакалов Р. К., Зачосова Н. В. Засади використання ризик-менеджменту у системі управління фінансово-економічною безпекою в умовах економіки воєнного часу. *Підприємництво та інновації*. 2023. Вип. 27. С. 73-78.

52. Гриценко Л. Л., Кожушко І. О., Чепурко В. О., Перепеліцин Г. Б. Ризик-орієнтоване управління в системі економічної безпеки корпоративного підприємства. *Бізнес Інформ*. 2023. № 8. С. 281-288.

53. Polozova T., Cherkashina M., Shapoval O., Romanchik T., Alzoubi Laith Abdel Karim Mohammad. Assessment of risks in conditions of provision of security of economic activities of organizations. *Journal of security and sustainability issues*. 2019. № 8 (4). С. 705-714.

54. Polozova T., Musiienko V., Storozhenko O., Peresada O., Geseleva N. Modeling of energy-saving processes in the context of energy safety and security. *Journal of security and sustainability issues*. 2019. № 8 (3). С. 387-397.

55. Нестеренко В. Ю., Горовий Д. А. Оцінка ризику рейдерського захоплення підприємства. *Вісник Національного технічного університету «Харківський політехнічний інститут»*. Збірник наукових праць. Тематичний випуск: *Технічний прогрес і ефективність виробництва*. Харків: НТУ «ХПІ». 2009. № 5. С. 26-34.

56. Нестеренко В. Ю. Методика оцінки слабких сторін підприємства, що сприяють його рейдерському захопленню. *Коммунальное хозяйство городов. Научно-технический сборник. Серия: Экономические науки*. Київ: «Техніка». 2008. № 85. С. 344-349.

57. Дмитрієв І. А., Нестеренко В. Ю. Визначення потенційних методів рейдерського захоплення автотранспортних підприємств. *Економіка транспортного комплексу: Збірник наукових праць*. Харків: ХНАДУ. 2011. Вип.16. С. 33-42.

58. Горовий Д. А., Нестеренко В. Ю. Основні фактори, що впливають на настання ризику рейдерського захоплення підприємства. *Вісник Дніпропетровської державної фінансової академії. Науково-теоретичний журнал*. Дніпропетровськ: ДДФА, 2007. № 2(18). С. 18-23.

59. Шейко І. А., Петренко Д. А., Кондрашов І. Є. Кіберстійкість для підвищення економічної безпеки підприємств. *Сучасні стратегії економічного розвитку: наука, інновації та бізнес-освіта. Матеріали IV Міжнародної науково-практичної конференції* (м. Харків, 1 листопада 2023 р.) / За заг. ред. д.е.н., проф. Т.В. Полозової. Харків. ХНУРЕ. 2023. С. 223-225.

60. Шейко І. А., Степаненко Р.Д., Кондрашов І.Є. Аналіз методичних підходів до управління ризиками підприємства в умовах цифрового розвитку. Функціонування соціально-економічних систем в контексті цілей сталого розвитку: колективна монографія / За заг. ред. д.е.н., проф. Т. В. Полозової. Харків: ХНУРЕ, 2023. С. 345-352.