МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ ТА ЗАХИСТОМ ІНФОРМАЦІЇ**

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “МЕТОДИЧНІ ПІДХОДИ ЩОДО ОЦІНКИ ВТРАТ ОРГАНІЗАЦІЇ ВІД ВПЛИВУ ІНФОРМАЦІЙНИХ ЗАГРОЗ”

на здобуття освітнього ступеня магістра
зі спеціальності 125 Кібербезпека
освітньої програми Управління інформаційною та кібернетичною безпекою

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Владислав ДЕЛІКАТНИЙ
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконала: здобувач вищої освіти гр. УБДМ-61

Владислав ДЕЛІКАТНИЙ
Ім’я, ПРІЗВИЩЕ

Керівник: Юрій ЯКИМЕНКО
Ім’я, ПРІЗВИЩЕ

Рецензент: Галина ГАЙДУР
Ім’я, ПРІЗВИЩЕ

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ

ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут кібербезпеки та захисту інформації

Кафедра Управління кібербезпекою та захистом інформації

Ступінь вищої освіти магістр

Спеціальність 125 Кібербезпека

Освітня програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедри УКБЗІ
_____ Світлана ЛЕГОМІНОВА
“____”_____2025 р.

ЗАВДАННЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

ДЕЛІКАТНИЙ Владислав Артурович
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “Методичні підходи щодо оцінки втрат організації від впливу інформаційних загроз”,
Керівник кваліфікаційної роботи Юрій ЯКИМЕНКО, к.в.н., доцент
(Ім’я,, ПРІЗВИЩЕ, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від “30“ жовтня 2025 р. №467.

2. Строк подання кваліфікаційної роботи “ _ ” грудня 2025р.

3. Вихідні дані до кваліфікаційної роботи: *інформаційна інфраструктура організації; дані про інформаційні активи, загрози та інформаційні інциденти, наукова та технічна література.*

4. Перелік питань, які мають бути розроблені:
4.1. Дослідити теоретичні засади забезпечення інформаційної безпеки організацій та роль оцінки втрат у системі управління інформаційними ризиками.
4.2. Провести аналіз інформаційної інфраструктури досліджуваного підприємства, визначити ключові інформаційні активи, вразливості та потенційні ризики.
4.3. Розробити методичний підхід до оцінювання можливих втрат організації від впливу інформаційних загроз з урахуванням прямих і непрямих збитків.

5. Перелік ілюстративного матеріалу: *презентація PowerPoint*

6. Дата видачі завдання “10“ жовтня 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Визначення об’єкта, предмета, мети та завдань дослідження в контексті оцінки втрат від інформаційних загроз.	12.10.2025	
2.	Збір та аналіз наукових, нормативно-правових і технічних джерел з питань інформаційної безпеки, управління ризиками та оцінювання втрат.	15.10.2025	
3.	Дослідження міжнародних стандартів і методологій оцінки ризиків та наслідків інформаційних інцидентів (FAIR, ISO/IEC 27005, NIST).	20.10.2025	
4.	Аналіз інформаційної інфраструктури та системи управління інформаційною безпекою досліджуваної організації.	10.11.2025	
5.	Виявлення інформаційних активів, загроз і вразливостей, а також оцінка відповідних інформаційних ризиків.	12.11.2025	
6.	Розроблення комплексу практичних рекомендацій щодо мінімізації можливих втрат і підвищення рівня стійкості організації до інформаційних загроз.	16.11.2025	
7.	Оформлення роботи.	03.12.2025	
8.	Оформлення презентації.	03.12.2025	
9.	Отримання рецензії на роботу.	07.12.2025	
10.	Захист в ЕК.	__.06.2025	

Здобувач вищої освіти _____ Владислав ДЕЛІКАТНИЙ
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Юрій ЯКИМЕНКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА

на кваліфікаційну магістерську роботу

здобувача вищої освіти Делікатного Владислава Артуровича

на тему “**МЕТОДИЧНІ ПІДХОДИ ЩОДО ОЦІНКИ ВТРАТ ОРГАНІЗАЦІЇ ВІД ВПЛИВУ ІНФОРМАЦІЙНИХ ЗАГРОЗ**”

Рецензент: завідувач кафедри
Систем та технологій кібербезпеки _____ Галина ГАЙДУР

Актуальність.

У сучасних умовах стрімкого розвитку інформаційних технологій та цифрової трансформації бізнесу кількість та складність кібератак постійно зростає, що вимагає адекватних методичних підходів щодо оцінки їхнього впливу на діяльність будь-якої організації. Методичні підходи до оцінки втрат від інформаційних загроз, як правило, дозволяють поєднати кількісні та якісні методи, аналізуючи ймовірність реалізації загроз та потенційний збиток від них. Використання їх на практиці спрямовано на покращення управління ризиками та оцінку впливу кібер-інцидентів на фінансові показники та репутацію, що є критично важливим і актуальним для забезпечення безперервності бізнесу та конкурентоспроможності організації.

Усунення та запобігання інформаційним загрозам різного характеру передбачає побудову ефективної системи економічних, соціальних, техніко-технологічних та інших показників, які повинні базуватися на оцінці інформаційних ризиків та на управлінні захистом інформаційних ресурсів організації, що включає ідентифікацію загроз, оцінку їхнього впливу та розробку методичних підходів для мінімізації збитків.

Позитивні сторони

1. У кваліфікаційній роботі проаналізовано теоретичні засади оцінки втрат від інформаційних загроз, підходи та методи оцінки ризиків і фінансових втрат від інформаційних інцидентів - відповідно до міжнародних стандартів і методологій.

2. Розроблена методика формування моделі оцінювання потенційних втрат і її використання на прикладі організації, що дозволило визначити рекомендації щодо зменшення можливих втрат та підвищення рівня стійкості захисту інформаційних ресурсів від інформаційних загроз і інцидентів. Проведений аналіз отриманих результатів у вигляді показників підтвердив ефективність запропонованих рішень для практичної реалізації.

Робота оформлена відповідно до вимог. Структура роботи забезпечує досягнення поставленої мети. Кваліфікаційна робота засвідчила розуміння студентом проблеми, володіння методами дослідження та здатність вирішувати прикладні завдання.

Недоліки

Доцільно було б приділити більше уваги діяльності керівництва по застосуванню на прикладі по оцінні втрат організації від впливу інформаційних загроз та інцидентів.

Однак, вищезгадані зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Кваліфікаційна робота виконана на високому науково-методичному рівні, заслуговує позитивної оцінки і рекомендується до захисту, а здобувач Делікатний Владислав Артурович заслуговує присвоєння кваліфікації “Магістр з кібербезпеки та захисту інформації за освітньо-професійною програмою Управління інформаційною та кібернетичною безпекою”.

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня магістра

Направляється здобувач Делікатний В.А.до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
Освітньо-професійної програми Управління інформаційною безпекою
(назва)
на тему: “ Методичні підходи щодо оцінки втрат організації від впливу інформаційних загроз”
Кваліфікаційна робота і рецензія додаються.

Директор ННІКБЗІ _____ Євгенія ІВАНЧЕНКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач **ДЕЛІКАТНИЙ Владислав** у кваліфікаційній роботі дослідив теоретичні засади забезпечення інформаційної безпеки організацій та роль оцінки втрат у системі управління інформаційними ризиками, визначив можливі фінансові та нефінансові втрати організації внаслідок реалізації інформаційних загроз і розробив методичний підхід до оцінювання можливих втрат організації від впливу інформаційних загроз з урахуванням прямих і непрямих нанесених збитків. **ДЕЛІКАТНИЙ Владислав** показав розуміння проблеми дослідження та бачення основних теоретичних та практичних напрямів її вирішення, довів уміння самостійного застосування методів наукового дослідження, проявив себе як організований, відповідальний виконавець. Результати дослідження апробовані на науково-практичних конференціях.

Це дозволяє оцінити виконану кваліфікаційну роботу здобувача **ДЕЛІКАТНОГО Владислава** на оцінку “добре” та присвоїти йому кваліфікацію Магістр кібербезпеки за освітньо-професійною програмою “Управління інформаційною безпекою”.

Керівник кваліфікаційної роботи ___ Юрій ЯКИМЕНКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

“____“_____2025 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач **ДЕЛІКАТНИЙ В.А.** допускається до захисту даної роботи в Державній екзаменаційній комісії.

Завідувач кафедрою
Управління кібербезпекою та захистом
інформації _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню методичних підходів до оцінки втрат організації від впливу інформаційних загроз, аналізу інформаційних ризиків та наслідків інформаційних інцидентів.

Робота складається зі вступу, трьох розділів, що містять 7 рисунків, 10 таблиць, висновків та списку використаних джерел із 29 найменувань. Загальний обсяг роботи становить 74 аркушів.

Метою роботи є розробити ефективний підхід до оцінювання можливих втрат організації від інформаційних загроз та сформувати рекомендації щодо мінімізації збитків.

Об'єктом дослідження є інформаційна інфраструктура організації, що зазнає впливу зовнішніх і внутрішніх інформаційних загроз.

Предмет дослідження – методи оцінки втрат від інформаційних інцидентів та підходи до визначення ризиків і їхніх наслідків.

Методи дослідження:

1. Аналіз літературних та технічних джерел – вивчення сучасних підходів до управління інформаційними ризиками, методологій оцінювання втрат (FAIR, ISO/IEC 27005, NIST).
2. Методи системного аналізу та проєктування – формування моделі оцінки збитків, аналіз залежностей між загрозами, активами та потенційними втратами.
3. Експериментальні методи – аналіз IT-інфраструктури підприємства, ідентифікація вразливостей, оцінка критичних ризиків та перевірка ефективності запропонованих заходів.

Ключові слова: ІНФОРМАЦІЙНА БЕЗПЕКА, ПОЛІТИКИ БЕЗПЕКИ, ПРОЦЕДУРИ БЕЗПЕКИ, МІЖНАРОДНІ СТАНДАРТИ, РИЗИК-МЕНЕДЖМЕНТ, АУДИТ БЕЗПЕКИ, ІНФОРМАЦІЙНІ ЗАГРОЗИ

ABSTRACT

The qualification work is devoted to the study of methodological approaches to assessing organizational losses caused by information threats, as well as to the analysis of information risks and the consequences of information incidents.

The work consists of an introduction, three chapters containing 7 figures and 10 tables, conclusions, and a list of references comprising 30 sources. The total volume of the work is 64 pages.

The aim of the study is to develop an effective approach to assessing potential organizational losses resulting from information threats and to formulate recommendations for minimizing damages.

The object of the research is the information infrastructure of an organization exposed to external and internal information threats.

The subject of the research comprises methods for assessing losses from information incidents and approaches to identifying risks and their consequences.

Research methods:

1. Analysis of scientific and technical sources – studying modern approaches to information risk management and loss assessment methodologies (FAIR, ISO/IEC 27005, NIST).

2. System analysis and design methods – development of a loss assessment model and analysis of relationships between threats, assets, and potential losses.

3. Experimental methods – analysis of the enterprise IT infrastructure, identification of vulnerabilities, assessment of critical risks, and verification of the effectiveness of the proposed measures.

Keywords: INFORMATION SECURITY, SECURITY POLICIES, SECURITY PROCEDURES, INTERNATIONAL STANDARDS, RISK MANAGEMENT, SECURITY AUDIT, INFORMATION THREATS

ЗМІСТ

ВСТУП

Актуальність дослідження. В умовах цифровізації діяльності організацій інформаційна інфраструктура стає критично важливим ресурсом, від надійності та захищеності якого залежать безперервність бізнес-процесів і фінансова стабільність підприємства. Зростання кількості інформаційних загроз і кіберінцидентів зумовлює необхідність не лише впровадження технічних засобів захисту, але й застосування обґрунтованих підходів до оцінки можливих втрат, спричинених впливом таких загроз.

Наслідки інформаційних інцидентів проявляються у вигляді прямих фінансових збитків та непрямих втрат, пов’язаних із порушенням функціонування інформаційних систем, зниженням довіри клієнтів і репутаційними ризиками. Водночас у практиці багатьох організацій відсутні формалізовані методики кількісної оцінки таких втрат, що ускладнює прийняття ефективних управлінських рішень у сфері інформаційної та кібернетичної безпеки.

Актуальність даного дослідження полягає у необхідності розроблення та адаптації методичних підходів до оцінювання втрат організації від впливу інформаційних загроз на основі міжнародних стандартів і методологій, що дозволяє підвищити обґрунтованість управління ризиками та рівень стійкості інформаційної інфраструктури організації.

Мета роботи розробити ефективний підхід до оцінювання можливих втрат організації від інформаційних загроз та сформувати рекомендації щодо мінімізації збитків.

Об’єкт дослідження **–** інформаційна інфраструктура організації, що зазнає впливу зовнішніх і внутрішніх інформаційних загроз.

Предмет дослідження – методи оцінки втрат від інформаційних інцидентів та підходи до визначення ризиків і їхніх наслідків.

Для досягнення цієї мети в роботі необхідно виконати наступні завдання:

1. Дослідити теоретичні засади забезпечення інформаційної безпеки

організацій та роль оцінки втрат у системі управління інформаційними ризиками.

2. Провести аналіз інформаційної інфраструктури досліджуваного підприємства, визначити ключові інформаційні активи, вразливості та потенційні ризики.

3. Розробити методичний підхід до оцінювання можливих втрат організації від впливу інформаційних загроз з урахуванням прямих і непрямих збитків.

4. Сформувати рекомендації щодо зменшення можливих втрат та підвищення рівня стійкості організації до інформаційних загроз.

Методи дослідження. Для вирішення поставлених у роботі наукових завдань використано комплекс загальнонаукових і спеціальних методів дослідження, зокрема методи аналізу та синтезу – для вивчення теоретичних засад інформаційної безпеки та підходів до оцінки втрат від інформаційних загроз; порівняння та класифікації.до міжнародних стандартів FAIR, ISO/IEC 27005 і рекомендацій NIST.

Практичне значення одержаних результатів. Практичне значення одержаних у роботі результатів полягає в можливості застосування розробленого методичного підходу для оцінювання можливих втрат організації від впливу інформаційних загроз у процесі управління інформаційною та кібернетичною безпекою.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ІБ – інформаційна безпека

ІТ – інформаційні технології

ІС – інформаційна система

СУІБ – система управління інформаційною безпекою

ІЗ – інформаційна загроза

ІР – інформаційний ризик

FAIR (Factor Analysis of Information Risk) – методологія кількісної оцінки інформаційних ризиків

ISO/IEC 27005 – міжнародний стандарт управління ризиками інформаційної безпеки

NIST – Національний інститут стандартів і технологій США

IDS (Intrusion Detection System) – система виявлення вторгнень

IPS (Intrusion Prevention System) – система запобігання вторгненням

LEF (Loss Event Frequency) – частота виникнення подій втрат

LM (Loss Magnitude) – величина втрат

ALE (Annualized Loss Expectancy) – очікувані річні втрати

BCP (Business Continuity Plan) – план забезпечення безперервності діяльності

CIA (Confidentiality, Integrity, Availability) – тріада цілей інформаційної безпеки

РОЗДІЛ 1 ТЕОРЕТИЧНІ ЗАСАДИ ОЦІНКИ ВТРАТ ВІД ІНФОРМАЦІЙНИХ ЗАГРОЗ

1.1 Інформаційна безпека як складник діяльності сучасних організацій

У сучасних умовах активної цифровізації економіки та широкого використання інформаційних технологій у діяльності підприємств інформаційна безпека поступово перетворюється на один із визначальних чинників стабільного функціонування організацій. Інформаційні ресурси, інформаційні системи та дані сьогодні є не лише засобом підтримки бізнес-процесів, але й стратегічним активом, від якого залежить ефективність управління, фінансова стійкість і конкурентні позиції організації на ринку. У зв’язку з цим питання забезпечення інформаційної безпеки виходить за межі суто технічних рішень і набуває комплексного управлінського характеру [1].

Розглядаючи інформаційну безпеку як управлінську функцію, доцільно підкреслити, що вона передбачає систематичну та цілеспрямовану діяльність керівництва, спрямовану на створення умов для захисту інформаційних активів від внутрішніх і зовнішніх загроз. Така діяльність охоплює не лише впровадження технічних засобів захисту, а й формування політик, процедур і правил, які регламентують роботу з інформацією на всіх рівнях організації. Саме управлінський підхід дозволяє забезпечити узгодженість дій персоналу, технічних підсистем і організаційних механізмів у процесі захисту інформації.

Планування полягає у визначенні цілей захисту інформації з урахуванням стратегічних завдань організації та допустимого рівня ризику. На основі цього здійснюється організація системи інформаційної безпеки, що передбачає розподіл відповідальності між структурними підрозділами, визначення ролей і повноважень, а також створення механізмів взаємодії між управлінськими та технічними компонентами. Контроль у сфері інформаційної безпеки реалізується через постійний моніторинг стану захищеності інформаційної

інфраструктури, проведення аудитів і оцінку ефективності впроваджених заходів.

З огляду на зростання кількості та складності інформаційних загроз особливої актуальності набуває взаємозв'язок інформаційної безпеки з процесами управління ризиками. Керівництво організації змушене приймати рішення щодо вибору заходів захисту, враховуючи можливі наслідки інформаційних інцидентів і потенційні втрати. У цьому контексті інформаційна безпека виступає інструментом зменшення негативного впливу загроз на діяльність організації та забезпечення прийнятного співвідношення між витратами на захист і рівнем ризику.

Інформаційна безпека як складник діяльності сучасних організацій є невід'ємною частиною системи управління, що поєднує стратегічні, організаційні та економічні аспекти [2]. Її ефективна реалізація створює передумови для підвищення рівня стійкості організації до інформаційних загроз і формує основу для подальшої оцінки можливих втрат, пов'язаних з реалізацією інформаційних ризиків.

Сучасні підприємства значною мірою залежать від інформаційних систем, що забезпечують планування, облік, комунікацію, обслуговування клієнтів і прийняття управлінських рішень. Порушення конфіденційності, цілісності або доступності інформації безпосередньо впливає на виконання цих процесів, призводячи до збоїв у роботі, зниження продуктивності персоналу та погіршення якості управління. Таким чином, рівень інформаційної безпеки визначає надійність функціонування бізнес-процесів і їх здатність забезпечувати досягнення стратегічних цілей організації.

У свою чергу, стан бізнес-процесів впливає на вимоги до інформаційної безпеки, оскільки кожен процес характеризується різним рівнем критичності інформаційних активів і допустимими ризиками. Критичні процеси, пов'язані з фінансовими операціями, обробкою персональних даних або управлінням виробничими ресурсами, потребують підвищеного рівня захисту та постійного контролю. Це зумовлює необхідність інтеграції інформаційної безпеки у систему

управління бізнес-процесами, що дозволяє враховувати ризики на етапі їх проєктування та експлуатації.

Взаємозв’язок інформаційної безпеки з фінансовою стабільністю організації проявляється через економічні наслідки інформаційних інцидентів. Реалізація інформаційних загроз може спричинити як прямі фінансові втрати, пов’язані з відновленням інформаційних систем, простоєм бізнес-процесів і штрафними санкціями, так і непрямі збитки у вигляді репутаційних втрат, зниження довіри клієнтів і втрати ринкових позицій. У цьому контексті інвестиції в інформаційну безпеку розглядаються не лише як витрати, а як засіб забезпечення фінансової стійкості та зниження ймовірності значних економічних втрат.

Інформаційна безпека виступає інтегруючим елементом між бізнес-процесами та фінансовими результатами діяльності організації. Належний рівень захисту інформації забезпечує безперервність і ефективність бізнес-процесів, що, у свою чергу, позитивно впливає на фінансову стабільність підприємства та зменшує ризик виникнення критичних втрат від інформаційних загроз.

З метою наочного відображення взаємозв’язку між інформаційною безпекою, бізнес-процесами та фінансовою стабільністю організації доцільно подати відповідну структурну схему. Представлена схема ілюструє, яким чином рівень захищеності інформаційних активів впливає на стійкість функціонування основних бізнес-процесів, а також як порушення інформаційної безпеки може призводити до фінансових втрат і необхідності перегляду підходів до інвестування в заходи захисту (рис. 1.1). Використання такого графічного подання дозволяє комплексно відобразити управлінський характер інформаційної безпеки та її роль у забезпеченні стабільного розвитку організації.

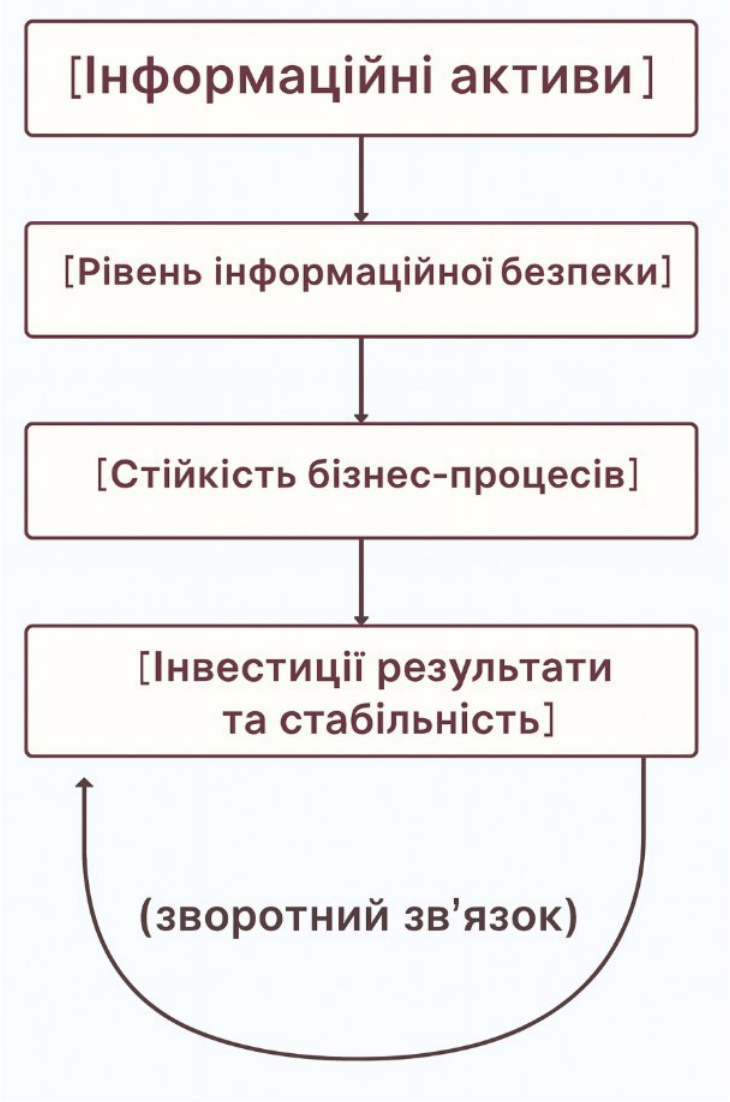

Рис 1.1 Взаємозв'язок інформаційної безпеки, бізнес-процесів та фінансової стабільності організації

У контексті управлінського підходу до забезпечення інформаційної безпеки її основні цілі традиційно визначаються через забезпечення конфіденційності, цілісності та доступності інформації (рис. 1.2). Зазначені складові утворюють концептуальну основу системи інформаційної безпеки та визначають напрями формування заходів захисту інформаційних активів організації.

Рис. 1.2. Тріада цілей інформаційної безпеки

Конфіденційність інформації передбачає обмеження доступу до даних виключно для уповноважених користувачів і запобігання несанкціонованому розкриттю відомостей. Порушення конфіденційності може призвести до витоку комерційної таємниці, персональних даних або іншої чутливої інформації, що, у свою чергу, спричиняє як прямі фінансові втрати, так і репутаційні ризики для організації. З управлінської точки зору забезпечення конфіденційності потребує чіткого регламентування прав доступу, впровадження політик контролю доступу та формування культури відповідального поводження з інформацією серед персоналу [3].

Цілісність інформації полягає у забезпеченні її точності, повноти та незмінності протягом усього життєвого циклу обробки. Порушення цілісності даних може мати критичні наслідки для прийняття управлінських рішень, функціонування фінансових систем і виконання бізнес-процесів. Несанкціонована модифікація або знищення інформації здатна призвести до помилок у звітності, фінансових втрат і зниження довіри до інформаційних систем організації. Тому забезпечення цілісності інформації є важливим елементом управління ризиками та потребує впровадження механізмів контролю змін, резервного копіювання та моніторингу.

Доступність інформації означає забезпечення своєчасного та безперешкодного доступу до інформаційних ресурсів для авторизованих

користувачів у процесі виконання службових обов’язків. Порушення доступності, зокрема внаслідок відмов у обслуговуванні або збоїв інформаційних систем, безпосередньо впливає на безперервність бізнес-процесів і може спричинити суттєві економічні втрати через простої та невиконання зобов’язань. У цьому аспекті інформаційна безпека тісно пов’язана з питаннями забезпечення надійності та стійкості інформаційної інфраструктури.

Тріада КЦД виступає взаємопов’язаними цілями інформаційної безпеки, порушення будь-якої з яких може негативно вплинути на діяльність організації. Забезпечення балансу між цими складовими є ключовим завданням управління інформаційною безпекою та створює основу для подальшої оцінки ризиків і можливих втрат від впливу інформаційних загроз.

У сучасних умовах функціонування організацій втрати від інформаційних загроз мають критичне значення, оскільки вони безпосередньо впливають на стабільність діяльності підприємства та його фінансові результати. Зростаюча залежність бізнес-процесів від інформаційних технологій призводить до того, що будь-яке порушення інформаційної безпеки здатне спричинити збої у роботі ключових інформаційних систем, порушити безперервність операційної діяльності та негативно позначитися на виконанні фінансових і договірних зобов’язань [4]. У результаті навіть локальні інформаційні інциденти можуть трансформуватися у суттєві економічні втрати для організації.

Критичність втрат від інформаційних загроз посилюється тим, що наслідки таких інцидентів, як правило, не обмежуються лише технічними аспектами. Порушення конфіденційності, цілісності або доступності інформації супроводжується необхідністю залучення додаткових фінансових ресурсів на відновлення інформаційних систем, усунення наслідків інцидентів, виконання регуляторних вимог і сплату можливих штрафних санкцій. Водночас організація може зазнавати непрямих збитків, пов’язаних зі зниженням рівня довіри клієнтів, погіршенням ділової репутації та втратою конкурентних переваг, що негативно впливає на фінансові показники у середньо- та довгостроковій перспективі.

У такому контексті кібербезпека набуває чітко вираженого економічного виміру, оскільки управління інформаційною безпекою фактично стає складовою системи управління фінансовими ризиками організації. Рішення щодо впровадження заходів захисту інформації повинні прийматися з урахуванням співвідношення між витратами на безпеку та можливими втратами від реалізації інформаційних загроз. Відсутність кількісної оцінки потенційних збитків ускладнює процес прийняття управлінських рішень і може призвести до неефективного розподілу ресурсів, коли рівень захисту або не відповідає реальним ризикам, або є економічно необґрунтованим.

Отже, втрати від інформаційних загроз є критичними для організацій саме через їх комплексний вплив на бізнес-процеси, фінансову стабільність і стратегічний розвиток підприємства, що зумовлює необхідність системного підходу до оцінки таких втрат і формування економічно обґрунтованих рішень у сфері кібербезпеки.

1.2 Класифікація інформаційних загроз та їх вплив на функціонування підприємства

У процесі забезпечення інформаційної безпеки організації важливим етапом є ідентифікація та систематизація інформаційних загроз, оскільки саме характер і джерела загроз визначають рівень ризиків та можливі втрати від інформаційних інцидентів. Різноманіття загроз, з якими стикаються сучасні організації, зумовлює необхідність їх класифікації за кількома ознаками, що дозволяє більш обґрунтовано оцінювати наслідки їх реалізації та формувати адекватні заходи протидії [5]. З метою узагальнення впливу інформаційних загроз на діяльність організації доцільно розглянути логічний взаємозв’язок між інформаційною загрозою, інформаційним інцидентом та можливими втратами. Такий підхід дозволяє наочно відобразити трансформацію потенційної загрози у конкретні економічні та нефінансові наслідки для підприємства.

Зовнішні загрози пов’язані з впливом факторів, що знаходяться поза межами організації, зокрема кібератаками з боку зловмисників, діяльністю конкурентів, впливом шкідливого програмного забезпечення або порушеннями з боку третіх сторін. Внутрішні загрози, у свою чергу, виникають у межах самої організації та пов’язані з діями або бездіяльністю персоналу, помилками в управлінні інформаційними ресурсами, а також недоліками внутрішніх процедур і контролю. Практика свідчить, що внутрішні загрози нерідко є не менш небезпечними, ніж зовнішні, оскільки пов’язані з наявністю легітимного доступу до інформаційних активів.

Технічні загрози зумовлені недоліками програмного забезпечення, апаратних засобів або мережевої інфраструктури, що можуть призводити до відмов у роботі систем, витоку або спотворення даних. Організаційні загрози виникають унаслідок недосконалості управлінських рішень, відсутності або формального характеру політик і процедур інформаційної безпеки, недостатнього контролю за їх дотриманням. Людський чинник проявляється у вигляді помилок персоналу, недостатнього рівня обізнаності з питань інформаційної безпеки або нехтування встановленими правилами, що значно підвищує ймовірність реалізації інформаційних інцидентів.

Навмисні загрози пов’язані з цілеспрямованими діями зловмисників, спрямованими на отримання вигоди або завдання шкоди організації, зокрема шляхом крадіжки даних, саботажу або порушення доступності інформаційних ресурсів. Випадкові загрози, навпаки, виникають без умислу і є результатом помилок персоналу, технічних збоїв або непередбачуваних обставин. Незважаючи на відсутність злочинного наміру, наслідки випадкових загроз можуть бути не менш значними з точки зору фінансових і операційних втрат [6].

Класифікація інформаційних загроз за джерелом виникнення, характером впливу та наявністю умислу дозволяє комплексно оцінити потенційні ризики для організації. Такий підхід створює основу для подальшого аналізу впливу інформаційних загроз на функціонування підприємства та визначення можливих

втрат, що є необхідним етапом у формуванні ефективної системи управління інформаційною безпекою.

Наявність інформаційної загрози сама по собі ще не означає виникнення збитків для організації. Інформаційна загроза є потенційним джерелом негативного впливу, реалізація якого залежить від рівня захищеності інформаційної інфраструктури, ефективності організаційних і технічних заходів безпеки, а також своєчасності управлінських рішень [7]. Лише у разі трансформації загрози в інформаційний інцидент вона може призвести до порушення конфіденційності, цілісності або доступності інформації, що, у свою чергу, зумовлює виникнення фінансових і нефінансових втрат. Таким чином, загроза слід розглядати як фактор ризику, який за певних умов здатний спричинити збитки, але не є тотожним самим втратам.

1.2 Методології аналізу наслідків кібератак (FAIR, NIST, ISO/IEC 27005), питання безпеки та обмеження IDS/IPS-систем

У процесі управління інформаційною та кібернетичною безпекою важливе значення має застосування формалізованих методологій, які дозволяють системно оцінювати інформаційні ризики та наслідки реалізації кібератак. У міжнародній практиці найбільш поширеними підходами до аналізу ризиків і втрат від інформаційних інцидентів є методологія FAIR, рекомендації NIST у межах Risk Management Framework, а також стандарт ISO/IEC 27005. Кожна з цих методологій має власну концептуальну основу, рівень формалізації та орієнтацію на економічні аспекти інформаційної безпеки.

Методологія FAIR (Factor Analysis of Information Risk) орієнтована на кількісну оцінку інформаційних ризиків і базується на представленні ризику як поєднання частоти реалізації інциденту та величини можливих втрат. Ключовою особливістю FAIR є використання грошового виміру для оцінки наслідків інформаційних інцидентів, що дозволяє безпосередньо пов’язати рівень ризику з фінансовими показниками діяльності організації [10]. У межах цієї методології

детально аналізуються фактори, що впливають на ймовірність виникнення інцидентів, а також розраховуються можливі прямі й непрямі збитки. Завдяки цьому FAIR є ефективним інструментом для обґрунтування управлінських рішень щодо інвестування в заходи інформаційної безпеки з урахуванням потенційних економічних втрат.

Підхід NIST Risk Management Framework спрямований на побудову комплексної системи управління інформаційними ризиками протягом усього життєвого циклу інформаційних систем. Основна увага в цій методології приділяється ідентифікації загроз, оцінці ризиків, вибору та впровадженню заходів безпеки, а також постійному моніторингу їх ефективності. Хоча NIST не зосереджується безпосередньо на кількісній оцінці фінансових втрат, він забезпечує високий рівень формалізації процесів управління ризиками та створює основу для системного підходу до забезпечення інформаційної безпеки в організації. Економічні аспекти в рамках NIST розглядаються опосередковано, через пріоритетність захисту активів і допустимі рівні ризику.

Стандарт ISO/IEC 27005 є складовою міжнародної серії стандартів ISO/IEC 27000 і визначає загальні принципи управління ризиками інформаційної безпеки. Він орієнтований на ідентифікацію активів, загроз і вразливостей, оцінку ризиків та вибір відповідних заходів їх обробки. ISO/IEC 27005 забезпечує універсальний і гнучкий підхід, який може бути адаптований до організацій різного масштабу та галузевої специфіки [11]. Водночас стандарт не містить жорстко визначених методів кількісної оцінки втрат, залишаючи вибір конкретних інструментів на розсуд організації, що обмежує його застосування для прямого фінансового аналізу наслідків кібератак.

Порівняльний аналіз зазначених методологій свідчить, що вони відрізняються підходом до оцінки ризиків, рівнем формалізації та орієнтацією на фінансові втрати. FAIR забезпечує високий рівень деталізації економічних наслідків і дозволяє кількісно оцінювати втрати у грошовому вимірі, що є особливо важливим у контексті прийняття управлінських рішень. У свою чергу, NIST Risk Management Framework та ISO/IEC 27005 формують методологічну

основу для побудови системи управління інформаційними ризиками, забезпечуючи структурований і стандартизований підхід до процесів ідентифікації, аналізу та мінімізації загроз.

Методологія FAIR є найбільш придатною для оцінювання втрат від інформаційних інцидентів у фінансовому вимірі, тоді як стандарти NIST і ISO/IEC 27005 доцільно розглядати як фундамент системи управління інформаційними ризиками (табл. 1.1).

Таблиця 1.1.

Порівняльна характеристика методологій FAIR, NIST та ISO/IEC 27005

Критерій порівняння	**FAIR**	**NIST Risk Management Framework**	**ISO/IEC 27005**
Основна мета	Кількісна оцінка інформаційних ризиків і втрат	Побудова комплексної системи управління ризиками	Управління ризиками інформаційної безпеки
Підхід до ризику	Ризик як поєднання ймовірності інциденту та величини втрат	Ризик як загроза для активів у межах життєвого циклу систем	Ризик як комбінація загроз, вразливостей і наслідків
Тип оцінки	Кількісна	Переважно якісна або напівкількісна	Переважно якісна
Рівень формалізації	Високий (чіткі фактори та розрахункова логіка)	Високий (регламентовані процеси і етапи)	Середній (гнучкий стандарт, адаптація організацією)
Орієнтація на фінансові втрати	Пряма, у грошовому вимірі	Опосередкована	Обмежена
Можливість оцінки прямих і непрямих збитків	Так	Частково	Обмежено
Підтримка управлінських рішень	Висока (економічне обґрунтування інвестицій)	Висока (стратегічне управління ризиками)	Середня
Гнучкість застосування	Висока, але потребує даних	Висока, масштабована	Висока

Продовження таблиці 1.1.

Основні переваги	Фінансова прозорість, кількісна оцінка	Системність, повний цикл управління	Відповідність міжнародним стандартам
Основні обмеження	Складність впровадження, потреба в даних	Відсутність прямої грошової оцінки	Відсутність формалізованих розрахунків

Наведене порівняння свідчить, що методологія FAIR найбільш придатна для оцінювання втрат від інформаційних інцидентів у фінансовому вимірі, оскільки забезпечує кількісне обґрунтування ризиків. Водночас підходи NIST та ISO/IEC 27005 формують методологічну основу управління інформаційними ризиками та забезпечують системність і стандартизований характер процесів інформаційної безпеки. Це зумовлює доцільність поєднання зазначених підходів при розробленні методичних підходів до оцінки втрат організації від впливу інформаційних загроз.

Приклад застосування методологій на основі реальних кейсів

Практика доводить ефективність зазначених методологій. Наприклад, у кейсі [Capital One (2019)], де внаслідок вразливості у хмарній конфігурації були скомпрометовані дані понад 100 млн клієнтів, оцінка втрат згідно FAIR дозволила банку спрогнозувати прямі збитки ($300+ млн), включаючи штрафи, компенсації та репутаційні втрати.

У випадку кібератаки на Equifax (2017), де було викрадено персональні дані понад 147 млн осіб, аналіз згідно з NIST RMF виявив критичні недоліки у життєвому циклі управління патчами та контролю доступу. Це призвело до перегляду політик безпеки та запровадження регламентованих процедур управління ризиком.

За підходом ISO/IEC 27005, прикладом адаптивного управління ризиками є кейс Sony Pictures (2014), де було використано якісну модель оцінки ризиків у відповідь на атаку типу APT. Результатом стала розробка індивідуальної політики реагування, незважаючи на відсутність повної фінансової оцінки.

Ці приклади доводять, що для обґрунтованого реагування на інциденти важливо поєднувати якісні методології управління (NIST, ISO/IEC 27005) з кількісними підходами оцінки збитків (FAIR), особливо у сфері економічного аналізу наслідків атак.

Приклад застосування методологій на основі реальних кейсів

Практика доводить ефективність зазначених методологій. Наприклад, у кейсі [Capital One (2019)], де внаслідок вразливості у хмарній конфігурації були скомпрометовані дані понад 100 млн клієнтів, оцінка втрат згідно FAIR дозволила банку спрогнозувати прямі збитки ($300+ млн), включаючи штрафи, компенсації та репутаційні втрати.

У випадку кібератаки на Equifax (2017), де було викрадено персональні дані понад 147 млн осіб, аналіз згідно з NIST RMF виявив критичні недоліки у життєвому циклі управління патчами та контролю доступу. Це призвело до перегляду політик безпеки та запровадження регламентованих процедур управління ризиком.

За підходом ISO/IEC 27005, прикладом адаптивного управління ризиками є кейс Sony Pictures (2014), де було використано якісну модель оцінки ризиків у відповідь на атаку типу APT. Результатом стала розробка індивідуальної політики реагування, незважаючи на відсутність повної фінансової оцінки.

Ці приклади доводять, що для обґрунтованого реагування на інциденти важливо поєднувати якісні методології управління (NIST, ISO/IEC 27005) з кількісними підходами оцінки збитків (FAIR), особливо у сфері економічного аналізу наслідків атак.

Зазначені методології (FAIR, NIST, ISO/IEC 27005) передбачають наявність джерел подій безпеки для побудови моделей ризиків. Одним із ключових таких джерел є IDS/IPS-системи, які фіксують факт реалізації загроз – інформаційних інцидентів.

Після розгляду методологій оцінки інформаційних ризиків та фінансових втрат (FAIR, NIST, ISO/IEC 27005), логічним є перехід до аналізу інструментів, які дозволяють виявляти інформаційні інциденти, що формують основу таких

оцінок. Одним із ключових елементів у системі захисту є системи виявлення та запобігання вторгненням (IDS/IPS).

У сучасних системах забезпечення інформаційної безпеки важливу роль відіграють технічні засоби виявлення та запобігання атакам, зокрема системи виявлення вторгнень (IDS) і системи запобігання вторгненням (IPS). Їх основним призначенням є моніторинг мережевого трафіку та подій у інформаційних системах з метою виявлення ознак несанкціонованої діяльності, порушень політик безпеки або спроб реалізації кібератак. Завдяки використанню сигнатурних, поведінкових і гібридних методів аналізу такі системи дозволяють своєчасно реагувати на загрози та знижувати ймовірність успішної реалізації атак.

Основні обмеження IDS/IPS-систем

1. Відсутність економічної оцінки. IDS/IPS не надають інформації про масштаби можливих збитків чи бізнес-наслідки інцидентів. Усі події класифікуються з технічної точки зору (тип атаки, IP-адреса, порт, сигнатура), але не з позиції впливу на фінанси або репутацію.

Це унеможливлює безпосереднє застосування даних IDS/IPS у рамках методології FAIR без додаткових аналітичних шарів.

2. Фокус на зовнішніх загрозах. Більшість IDS/IPS орієнтовані на зовнішні атаки (DDoS, сканування, експлойти). Вони погано працюють із внутрішніми інцидентами, такими як:

- помилки персоналу,
- зловживання правами доступу,
- витік даних через легальні канали (наприклад, електронну пошту).

Такі події часто не фіксуються технічними системами безпеки, але мають серйозні наслідки.

3. Потреба в налаштуванні та аналізі. IDS/IPS генерують велику кількість подій, які вимагають експертної обробки (аналіз логів, кореляція подій, фільтрація false positive). У разі неправильного налаштування – можливе пропущення атак або надлишкове сповіщення, що призводить до

інформаційного перевантаження. Це знижує ефективність реагування та ускладнює інтеграцію в бізнес-процеси.

4. Відсутність інтеграції з економічною аналітикою IDS/IPS зазвичай не інтегруються з системами управлінського обліку або бізнес-аналітики, що унеможливлює оцінку непрямих втрат (наприклад, втрат клієнтів або падіння виручки після атаки).

Разом з тим функціональні можливості IDS/IPS-систем обмежуються переважно технічним рівнем захисту та зосереджені на факті виявлення або блокування атаки. Хоча ці системи здатні фіксувати інформаційні інциденти та генерувати відповідні події безпеки, вони не забезпечують оцінювання економічних наслідків таких інцидентів. Інформація, що надається IDS/IPS, як правило, не містить даних про масштаб можливих фінансових втрат, вплив інциденту на бізнес-процеси або довгострокові репутаційні наслідки для організації [12]. У результаті управлінські рішення приймаються на основі технічних показників, без урахування повного економічного ефекту від реалізації інформаційних загроз.

Крім того, слід враховувати, що не всі інформаційні інциденти можуть бути виявлені виключно технічними засобами захисту. Значна частина інцидентів пов’язана з внутрішніми загрозами, помилками персоналу, порушенням організаційних процедур або зловживанням легітимними правами доступу, що часто не фіксується IDS/IPS-системами. Такі інциденти можуть мати суттєві наслідки для організації, зокрема витік конфіденційної інформації або спотворення даних, однак залишаються поза межами автоматизованого технічного контролю.

Технічні системи безпеки, включаючи IDS/IPS, не можуть розглядатися як самодостатній інструмент забезпечення інформаційної безпеки. Вони є необхідним, але не достатнім елементом системи захисту, оскільки не враховують економічний вимір інформаційних інцидентів. Ефективне управління інформаційною безпекою потребує доповнення технічних засобів формалізованими методиками оцінки наслідків і втрат від реалізації

інформаційних загроз, що дозволяє перейти від суто технічного реагування до обґрунтованого управління ризиками та фінансовими наслідками для організації.

Висновки до розділу 1

У першому розділі кваліфікаційної роботи було досліджено теоретичні засади оцінки втрат від впливу інформаційних загроз та визначено місце інформаційної безпеки у системі управління сучасною організацією. Показано, що інформаційна безпека в умовах цифровізації перестає бути виключно технічним завданням і набуває характеру комплексної управлінської функції, тісно пов’язаної з бізнес-процесами та фінансовою стабільністю підприємства.

У ході аналізу встановлено, що інформаційні загрози мають різну природу та джерела виникнення, що зумовлює необхідність їх класифікації за низкою ознак, зокрема за походженням, характером впливу та наявністю умислу. Обґрунтовано, що сама по собі інформаційна загроза не є тотожною збиткам, однак у разі її реалізації через інформаційний інцидент може призвести до суттєвих фінансових і нефінансових втрат для організації.

РОЗДІЛ 2 ОЦІНКА ФУНКЦІОНУВАННЯ ТА ВРАЗЛИВОСТЕЙ ТОВ «ІНФОТЕХ СОЛЮШНС»

2.1 Загальна характеристика діяльності підприємства

Досліджуване підприємство здійснює діяльність у сфері проєктування, будівництва та введення в експлуатацію промислових енергетичних об’єктів за принципом «під ключ». Такий формат діяльності передбачає повний цикл робіт – від розроблення техніко-економічного обґрунтування та проєктної документації до монтажу обладнання, пусконалагоджувальних робіт і передачі об’єкта замовнику [13]. Компанія функціонує в умовах високої технологічної складності, значних фінансових обсягів проєктів та підвищених вимог до надійності, безпеки й дотримання нормативних стандартів.

Основні бізнес-процеси підприємства охоплюють управління проєктами, інженерно-технічне проєктування, закупівлю обладнання та матеріалів, координацію підрядних організацій, будівельно-монтажні роботи, контроль якості, фінансове планування та взаємодію з замовниками й регуляторними органами. Зазначені процеси є взаємопов’язаними та потребують постійного обміну достовірною інформацією між структурними підрозділами компанії, що зумовлює високі вимоги до ефективності інформаційного забезпечення діяльності підприємства.

Ключову роль у забезпеченні функціонування бізнес-процесів відіграють інформаційні системи, які використовуються для планування та управління проєктами, ведення фінансового та управлінського обліку, зберігання проєктної документації, контролю виконання робіт і комунікації з контрагентами. Інформаційні системи забезпечують централізований доступ до даних, підтримують прийняття управлінських рішень і дозволяють оперативно реагувати на зміни в процесі реалізації проєктів [14]. Втрата доступу до таких систем або порушення цілісності даних може призвести до затримок у виконанні робіт, фінансових втрат і порушення договірних зобов’язань.

Діяльність підприємства значною мірою залежить від надійності та безперервності функціонування IT-інфраструктури, яка включає серверне обладнання, мережеві ресурси, спеціалізоване програмне забезпечення, засоби зберігання даних і канали зв’язку. IT-інфраструктура є основою для реалізації більшості управлінських і виробничих процесів, тому її уразливість до інформаційних загроз створює потенційні ризики для стабільності діяльності компанії. З огляду на масштаб і вартість енергетичних проєктів навіть короткочасні збої в роботі інформаційних систем можуть мати суттєві економічні наслідки.

Таким чином, специфіка діяльності підприємства, що реалізує промислові енергетичні об’єкти «під ключ», зумовлює високу залежність бізнес-процесів від інформаційних систем та IT-інфраструктури. Це підкреслює актуальність аналізу рівня інформаційної безпеки, виявлення потенційних ризиків і подальшої оцінки можливих втрат від впливу інформаційних загроз, що є предметом подальшого дослідження у межах даної роботи.

Для наочного відображення системи управління та розподілу функціональних обов’язків на підприємстві доцільно розглянути його організаційну структуру (рис. 2.1).

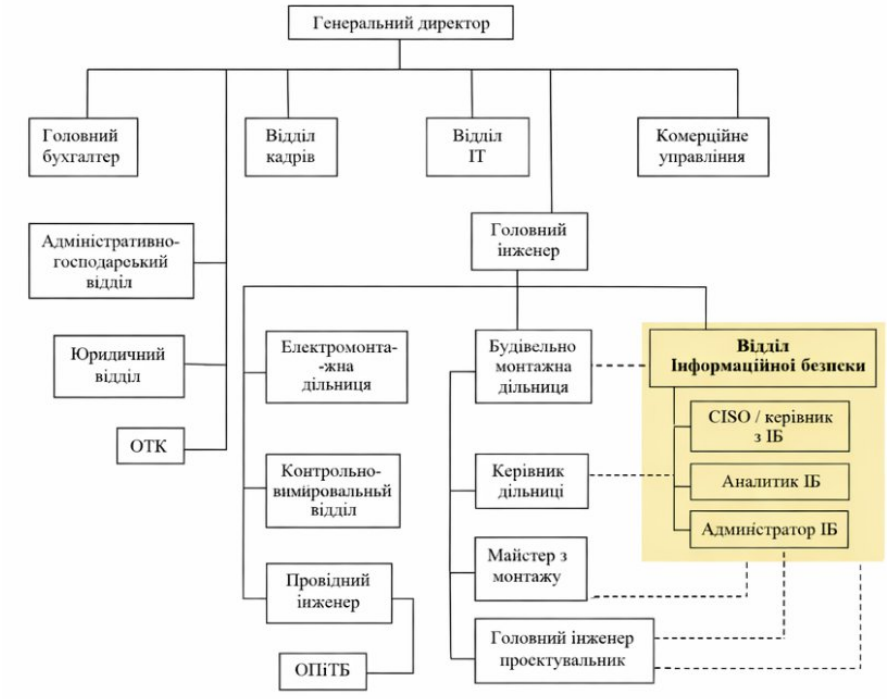

Рис. 2.1. Організаційна структура управління підприємством

Представлена організаційна структура підприємства відображає ієрархію управління та функціональні підрозділи, які забезпечують реалізацію ключових бізнес-процесів. Удосконалення структури передбачає включення служби інформаційної безпеки (ІБ), яка відповідає за розробку політик безпеки, моніторинг інцидентів, управління інформаційними ризиками, а також забезпечення відповідності вимогам законодавства у сфері захисту даних.

Служба ІБ має міжпідроздільні зв’язки з відділом кадрів (з питань доступу персоналу), юридичним відділом (з питань відповідності), ОПіТБ (з питань технічного захисту) та проєктним і технічним підрозділами. Така інтеграція гарантує узгодженість заходів інформаційної безпеки з операційною діяльністю організації.

Таким чином, включення функції інформаційної безпеки в організаційну структуру підприємства забезпечує не лише захист інформаційних ресурсів, а й підвищує надійність і безперервність бізнес-процесів, створюючи єдину систему управління ризиками на всіх рівнях.

2.1.1 Аналіз структури інформаційних ресурсів та ІТ-інфраструктури

У результаті аналізу організаційної структури підприємства, що реалізує енергетичні проєкти, встановлено, що його управлінська модель має ієрархічно-функціональну побудову, яка сприяє ефективному розподілу повноважень між виробничими, адміністративними та комерційними блоками. Однак виявлено, що в наявній структурі не передбачено окремого підрозділу, відповідального за інформаційну безпеку, що створює потенційні ризики в контексті збереження конфіденційних, технічних та фінансових даних.

Функції підтримки ІТ-інфраструктури та частково захисту інформаційних ресурсів покладено на ІТ-відділ, який виконує адміністрування серверного обладнання, мережевого середовища, систем резервного копіювання та обслуговування програмного забезпечення. Однак фахівці цього відділу не

мають чітко визначених обов’язків у сфері кібербезпеки, що підтверджено аналізом внутрішньої документації. Це свідчить про відсутність централізованого управління політиками ІБ та недооцінку ризиків, пов’язаних із загрозами внутрішнього та зовнішнього походження.

Інформаційні ресурси підприємства поділяються за критичністю на:

- високої важливості – технічна документація, проєкти, кошториси, договори, комерційні пропозиції;
- середньої важливості – фінансові та кадрові дані;
- низької важливості – службова кореспонденція, план-графіки, оперативні звіти.

Встановлено, що більшість документів циркулює як у цифровому, так і в паперовому вигляді. Частина з них зберігається локально на робочих ПК без централізованого контролю доступу чи шифрування, що порушує принципи цілісності та конфіденційності. Крім того, відсутність автоматизованих систем моніторингу доступу (SIEM, DLP, тощо) не дозволяє вчасно виявляти інциденти безпеки або порушення політик доступу до чутливої інформації.

Особливо вразливими виявлено:

- проєктний відділ, де зберігається критична технічна інформація;
- відділ кошторису та договорів, що має доступ до фінансових умов і цінових стратегій;
- кадровий сектор, де обробляються персональні дані.

Не було виявлено нормативних документів (регламентів, політик, процедур), які б регулювали порядок:

- класифікації активів за критичністю;
- періодичної оцінки ризиків;
- реагування на інциденти;
- планів безперервності діяльності (BCP).

З огляду на це, організація не забезпечує повноцінного захисту своїх інформаційних активів відповідно до вимог ISO/IEC 27001 та NIST, що є актуальним у зв’язку з підвищенням кількості кібератак на енергетичний сектор.

Таким чином, у межах цього підрозділу було виявлено:

- відсутність окремого підрозділу ІБ або відповідального фахівця;
- відсутність політик та системного підходу до захисту інформаційних ресурсів;
- наявність високоризикових інформаційних точок без контролю доступу;
- слабкий зв’язок між управлінням бізнес-процесами та управлінням інформаційною безпекою.

Це формує підґрунтя для подальшого обґрунтування необхідності впровадження інформаційно-аналітичної моделі захисту, яку буде розглянуто в наступних підрозділах.

Виявлена відсутність інтегрованої системи управління інформаційною безпекою (СУІБ) створює потенційні передумови для виникнення таких інцидентів:

- витоку конфіденційної інформації, особливо у процесах тендерних пропозицій та проєктування;
- втрати технічної документації внаслідок відсутності резервного копіювання з географічною диверсифікацією;
- несанкціонованого доступу до даних через недостатній контроль прав доступу;
- використання застарілого ПЗ або відсутність регулярного патч-менеджменту, що робить систему вразливою до шкідливого ПЗ.

У практиці сучасного кіберзахисту поширеним підходом є орієнтація на принцип «Zero Trust», який передбачає перевірку будь-якого доступу незалежно від його джерела. У випадку досліджуваного підприємства, ця парадигма не реалізується, що збільшує ризики інсайдерських загроз, особливо в умовах віддаленої роботи, яка частково застосовується у проєктному відділі.

З метою кількісної оцінки рівня ризику доцільним є застосування методології FAIR, що дозволяє розраховувати очікувані збитки від імовірних інформаційних інцидентів. Наприклад, витік контрактної інформації може

призвести до втрати тендеру з очікуваним прибутком у десятки мільйонів гривень, що створює прямий економічний ризик для компанії.

У зв’язку з викладеним, доцільно розглянути такі практичні заходи:

1. Створення відділу інформаційної безпеки або введення посади CISO (Chief Information Security Officer) з підпорядкуванням напряму керівництву.
2. Розробка політик ІБ, зокрема:
   - політика контролю доступу;
   - політика захисту персональних даних;
   - інструкція реагування на інциденти.
3. Впровадження системи моніторингу подій безпеки (SIEM) та журналювання дій користувачів.
4. Навчання персоналу основам кібергігієни, з обов’язковою сертифікацією на критичних посадах.
5. Застосування DLP-систем для запобігання витоку даних та контролю роботи з носіями.

Організаційна структура підприємства є ефективною з точки зору реалізації інжинірингових проєктів, однак суттєво вразливою в інформаційній площині. Відсутність фахово організованої інформаційної безпеки загрожує не лише безперервності бізнес-процесів, але й репутаційним та фінансовим втратам. Це обґрунтовує необхідність впровадження системного підходу до ІБ як невід’ємної частини стратегії цифрової трансформації підприємства.

2.1.2 Діагностика зовнішніх та внутрішніх факторів, що впливають на рівень інформаційної безпеки

Рівень інформаційної безпеки підприємства формується під впливом сукупності внутрішніх і зовнішніх факторів, які визначають як імовірність виникнення інформаційних інцидентів, так і масштаб можливих втрат. Для підприємства, що здійснює будівництво промислових енергетичних об’єктів «під ключ», діагностика таких факторів є особливо важливою з огляду на

складність бізнес-процесів, значний обсяг критичної інформації та залучення великої кількості персоналу і контрагентів.

До внутрішніх факторів впливу належать насамперед кадрові, організаційні та процесні аспекти діяльності підприємства. Рівень обізнаності персоналу з питань інформаційної безпеки, дотримання встановлених політик і процедур, а також розподіл ролей і відповідальності безпосередньо впливають на захищеність інформаційних ресурсів [16]. Недостатня регламентація процесів обробки інформації, формальний характер політик безпеки або відсутність регулярного контролю створюють передумови для виникнення внутрішніх інцидентів, пов’язаних з помилками або зловживаннями з боку працівників.

Зовнішні фактори впливу на інформаційну безпеку підприємства зумовлені передусім активністю кіберзагроз у сучасному цифровому середовищі, а також вимогами регуляторних і наглядових органів. Підприємство може зазнавати кібератак, спрямованих на отримання доступу до проєктної документації, фінансових даних або комерційної інформації. Окрім цього, важливу роль відіграють контрагенти та підрядні організації, які мають доступ до окремих інформаційних ресурсів або інформаційних систем, що підвищує ризик реалізації загроз через ланцюг постачання.

Окрему групу ризиків становлять загрози, пов’язані з людським чинником, який може виступати як внутрішнім, так і зовнішнім фактором впливу. Помилки персоналу, недбале поводження з інформацією, використання слабких паролів або нехтування правилами безпеки значно підвищують імовірність реалізації інформаційних інцидентів [17]. Навіть за наявності сучасних технічних засобів захисту людський чинник часто залишається найвразливішою ланкою системи інформаційної безпеки та може призводити до суттєвих фінансових і нефінансових втрат.

З урахуванням наведеного доцільно узагальнити результати діагностики внутрішніх і зовнішніх факторів впливу на рівень інформаційної безпеки підприємства у вигляді табл. 2.1.

Таблиця 2.1.

Діагностика внутрішніх та зовнішніх факторів впливу на інформаційну безпеку підприємства

Група факторів	**Фактор впливу**	**Характер впливу**	**Потенційні наслідки**
Внутрішні	Рівень підготовки персоналу	Недостатня обізнаність з ІБ	Помилки, витік інформації
Внутрішні	Політики та процедури ІБ	Формальний або неповний характер	Порушення правил обробки даних
Внутрішні	Бізнес-процеси	Відсутність контролю на окремих етапах	Порушення цілісності та доступності
Внутрішні	Розподіл доступів	Надмірні або некоректні права	Несанкціонований доступ
Зовнішні	Кібератаки	Цілеспрямований зловмисний вплив	Фінансові та репутаційні втрати
Зовнішні	Регуляторні вимоги	Невідповідність вимогам	Штрафи, санкції
Зовнішні	Контрагенти	Доступ третіх сторін до ІС	Загрози через ланцюг постачання
Людський чинник	Помилки персоналу	Випадкові дії	Інформаційні інциденти
Людський чинник	Зловживання доступом	Навмисні дії	Значні збитки

Результати діагностики свідчать, що найбільший вплив на рівень інформаційної безпеки підприємства мають внутрішні фактори та загрози, пов’язані з людським чинником, оскільки саме вони є найменш формалізованими та складними для контролю. Це підтверджує доцільність подальшого аналізу інформаційних активів і ризиків, а також необхідність кількісної оцінки можливих втрат від реалізації інформаційних загроз.

2.2 Оцінка фінансових, технічних та організаційних ресурсів підприємства

Для оцінювання поточного стану підприємства виконаємо аналіз фінансово-економічних показників діяльності ТОВ «Інфотех Солюшнс» та структури його активів. З цією метою проведено групування однорідних за

економічним змістом статей балансу, що дозволяє визначити склад майна підприємства та оцінити його структурні пропорції. Узагальнені результати систематизації наведено в табл. 2.2 [18].

Таблиця 2.2

Аналіз складу та структури активів ТОВ «Інфотех Солюшнс» за 2023–2025 роки, тис. грн

Показник	Роки	2024/2023	2025/2024
	2023	2024	2025
Усього майна	92 500	41 320	168 740
Необоротні активи	215	172	148
Оборотні активи	92 285	41 148	168 592
Запаси	9 120	4 630	28 750
Дебіторська заборгованість	61 840	6 850	90 260
Кошти та їх еквіваленти	8	27 880	41 520

На основі даних таблиці 2.2 можна зробити висновок, що загальна вартість активів ТОВ «Інфотех Солюшнс» у 2024 році порівняно з 2023 роком суттєво знизилася. Так, загальний обсяг майна скоротився приблизно на 51 млн грн – з 92,5 млн грн до 41,3 млн грн. Відповідне зниження становить близько 44,67%, що свідчить про різке падіння активів у зазначений період [18].

У 2025 році ситуація кардинально змінилася: вартість активів підприємства зросла більш ніж утричі – зі 41,3 млн грн до 168,7 млн грн (приріст 127,4 млн грн, або 308,38%) [18]. Однією з можливих причин такого стрімкого відновлення є суттєве збільшення обсягу грошових коштів та їх еквівалентів, що може свідчити про покращення ліквідності та імплементацію ефективних фінансових рішень.

Щодо оборотних активів, то їх динаміка загалом повторює рух загальної вартості майна. У 2024 році обсяг оборотних активів скоротився з 92,3 млн грн до 41,1 млн грн, тобто на 44,77%. Проте вже у 2025 році спостерігається значне

збільшення – до 168,6 млн грн, що відповідає приросту приблизно 309,69% порівняно з 2024 роком [18].

Необоротні активи за 2023–2025 роки демонструють протилежну тенденцію: протягом аналізованого періоду відбувається поступове зниження їхнього обсягу. Так, вартість необоротних активів у 2023 році становила 215 тис. грн, у 2024 році – 172 тис. грн, а у 2025 році – 148 тис. грн. Така динаміка може свідчити про відсутність інвестицій у довгострокові активи або про їх часткове списання[19].

Особливо помітною є зміна показника «грошові кошти та їх еквіваленти». У 2023 році підприємство володіло лише 8 тис. грн, проте вже у 2024 році ця величина різко зросла до 27,88 млн грн. У 2025 році обсяг коштів збільшився до 41,52 млн грн, що становить приріст 48,92% порівняно з попереднім роком. Така динаміка відображає істотне покращення платоспроможності ТОВ «Інфотех Солюшнс»[19].

Отримані дані свідчать про значні коливання активів підприємства протягом аналізованого періоду. Для більш точної оцінки фінансової стійкості проведемо додаткові розрахунки основних показників майнового стану та внесемо їх до табл. 2.3.

На основі даних табл. 2.3 можна надати розширену характеристику окремих показників майнового стану підприємства. Оскільки динаміку вартості всього майна ми вже детально розглянуто за підсумками аналізу табл. 2.2, повторно зупинятися на ній немає потреби. Натомість перейдемо до оцінювання інших ключових складових активів ТОВ «Інфотех Солюшнс».

Таблиця 2.3

Аналіз показників майнового стану ТОВ «Інфотех Солюшнс» за 2023–2025 роки

Показник	Роки	2024/2023	2025/2024
Вартість усього майна, тис. грн	2023	2024	2025
Власний капітал, тис. грн	92 500	41 320	168 740
Власні оборотні кошти (робочий капітал), тис. грн	2 950	3 780	4 290
Коефіцієнт зносу	-2 820	3 540	3 980
Коефіцієнт придатності	0,81	0,86	0,88
Коефіцієнт придатності	0,19	0,14	0,12

Вартість власного капіталу підприємства демонструє позитивну тенденцію. Як свідчать дані таблиці, у 2024 році порівняно з 2023 роком власні кошти збільшилися приблизно на 830 тис. грн, зростаючи з 2 950 тис. грн до 3 780 тис. грн. Темп приросту при цьому становив 128,14%, що свідчить про зміцнення фінансової бази компанії. Аналогічна динаміка спостерігається і у 2025 році: власний капітал зріс ще на 510 тис. грн, досягнувши 4 290 тис. грн. Такий поступовий приріст вказує на покращення результатів діяльності й підвищення частки власних ресурсів у структурі фінансування [20].

Власні оборотні кошти (робочий капітал) – це один із ключових індикаторів здатності підприємства забезпечувати операційну діяльність без зовнішнього фінансування. Згідно з таблицею, у 2023 році робочий капітал мав від’ємне значення, однак у 2024 році показник суттєво покращився і становив уже 3 540 тис. грн. У 2025 році спостерігається подальше зростання – до 3 980 тис. грн, що свідчить про стабілізацію обігових ресурсів і зниження ризику залежності від кредитних коштів. У цілому за період 2023–2025 років приріст робочого капіталу становив понад 6 млн грн, що є вагомим показником фінансового оздоровлення підприємства [20].

Коефіцієнт зносу основних засобів також демонструє стабільне зростання – з 0,81 у 2023 році до 0,88 у 2025 році. Попри незначне підвищення, така динаміка загалом свідчить про поступове старіння матеріально-технічної бази. Зростання зносу є сигналом необхідності оновлення основних засобів, щоб уникнути підвищення витрат на ремонти та зниження ефективності виробничих процесів.

Коефіцієнт придатності, навпаки, має тенденцію до зниження: від 0,19 у 2023 році він зменшився до 0,12 у 2025 році. Хоча нормативним вважається значення не нижче 0,5, показники ТОВ «Інфотех Солюшнс» поки не перетинають критичної межі, проте їх зниження вказує на поступове погіршення технічного стану основних засобів [19].

Наступним етапом аналізу є оцінювання фінансової стійкості підприємства, результати якого подано в табл. 2.4.

Таблиця 2.4

Аналіз фінансової стійкості ТОВ «ІІнфотех Солюшнс» за 2023–2025 роки

Показник	Роки	2024/2023	2025/2024	Динаміка значень
	2023	2024	2025	+/-
1) Коефіцієнт автономії	0,032	0,091	0,025	+0,059
2) Коефіцієнт маневреності власних коштів	1,05	0,93	0,88	-0,12
3) Коефіцієнт концентрації залученого капіталу	1,02	0,90	0,98	-0,12
4) Показник заборгованості кредиторам	0,97	0,76	0,59	-0,21
5) Коефіцієнт покриття запасів (Кпз)	–	-0,64	0,15	–

На основі результатів аналізу фінансової стійкості, відображених у таблиці 2.4, можна сформулювати такі узагальнені висновки:

1. Коефіцієнт автономії.

Візуальний огляд значень свідчить, що найкращий показник спостерігався у 2024 році, коли його значення наблизилося до нормативного. Натомість у 2023 та 2025 роках коефіцієнт був значно нижчим за рекомендований рівень, що свідчить про обмежену частку власного капіталу в структурі фінансових ресурсів.

2. Коефіцієнт маневреності власних коштів.

Протягом 2023–2025 років значення даного показника поступово знижувалося. Незважаючи на спад, коефіцієнт зберігає позитивну динаміку відносно нормативу, оскільки залишається більшим за нуль. Це означає, що підприємство все ще має певний рівень мобільності у використанні власних фінансових ресурсів.

3. Коефіцієнт концентрації залученого капіталу.

У 2024 році порівняно з 2023 роком зафіксовано суттєве зниження на 0,12, що характеризує позитивну тенденцію – частка позикових ресурсів зменшилася. Проте у 2025 році коефіцієнт знову зріс на 0,08. Підвищення цього показника означає, що частка залучених коштів знову стала домінувати, а це підвищує фінансові ризики, оскільки боргове навантаження зростає швидше, ніж активи.

4. Показник заборгованості кредиторам.

Динаміка протягом періоду є стабільно позитивною: у 2024 році значення скоротилося на 0,21, а у 2025 році – ще на 0,17. Зменшення цього коефіцієнта свідчить про зниження залежності підприємства від кредиторів, що є важливою умовою підвищення фінансової стійкості.

Отже, загалом можна зазначити, що частина показників демонструє позитивні зміни (зменшення боргового навантаження), проте існують проблеми, пов’язані зі складом капіталу та низькою часткою власних коштів. Це вимагає

подальшого аналізу прибутковості діяльності підприємства, дані щодо якої наведені в табл. 2.5 [19, 20].

Таблиця 2.5

Аналіз прибутковості ТОВ «Інфотех Солюшнс» за 2023–2025 роки

Показник	Роки	2024/2023	2025/2024	Динаміка значень
	2023	2024	2025	+/-
1) Рентабельність продажів, %	0,32	9,85	0,41	+9,53
2) Рентабельність операційної діяльності, %	0,30	10,14	0,39	+9,84
3) Рентабельність діяльності до оподаткування, %	0,22	19,70	0,51	+19,48
4) Рентабельність власного капіталу, %	6,10	185,00	12,40	+178,90

Виходячи з результатів, поданих у таблиці 2.4, можна сформулювати такі узагальнення щодо динаміки прибутковості ТОВ «Інфотех Солюшнс» у 2023–2025 роках. Найвищі значення більшості показників прибутковості спостерігалися у 2024 році, коли підприємство демонструвало різке зростання доходності та суттєве перевищення нормативних меж. Найнижчі значення, навпаки, зафіксовано у 2023 році, що свідчить про слабку ефективність операційної та загальної діяльності на початку аналізованого періоду [21].

Для візуалізації структури можливих збитків від реалізації інформаційних ризиків та аналізу динаміки їх зростання в умовах зростаючої кіберзагрози доцільно використати узагальнену інфографіку (рис. 2.2), яка відображає основні компоненти втрат і тенденції ризиків у часі.

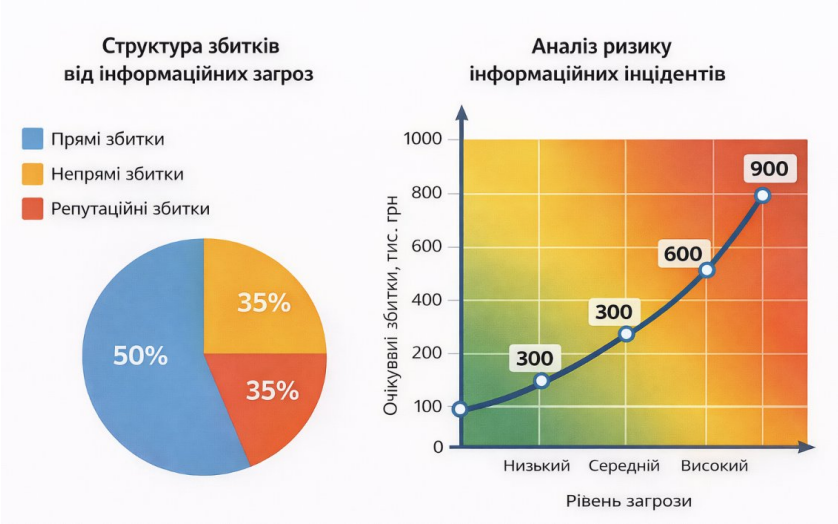

Рис. 2.2 Структура інформаційних збитків та динаміка ризику

Серед усіх показників слід виділити рентабельність діяльності до оподаткування та рентабельність власного капіталу, які у 2024 році суттєво перевищили порогові орієнтири (20 % та 16 % відповідно). Це вказує на те, що саме у цей рік підприємство досягло найбільшої фінансової результативності та ефективності використання власних ресурсів.

У 2025 році спостерігається різке зниження всіх показників прибутковості порівняно з 2024 роком. Такий спад може свідчити про погіршення рентабельності основної діяльності, зміну ринкових умов або зростання витратної частини. Водночас рентабельність власного капіталу зберегла найвищий рівень у межах року порівняно з іншими показниками, що вказує на відносно ефективне використання залучених інвестицій та внутрішніх ресурсів.

Загалом динаміка прибутковості за трирічний період демонструє контрастний характер: різке зростання у 2024 році та помітне падіння у 2025 році, що потребує додаткового аналізу причин та розроблення коригувальних управлінських рішень.

2.2.1 Визначення потенційних ризиків та можливих втрат від інформаційних загроз

Інформаційне середовище сучасного підприємства може містити широкий спектр потенційних вразливостей, які зловмисники здатні використати для отримання несанкціонованого доступу до конфіденційних даних або порушення

стабільності бізнес-процесів. Найбільш поширені типи вразливостей інформаційної інфраструктури включають:

1. Кібератаки різної природи.

Порушники можуть застосовувати різні тактики та інструменти, зокрема DDoS-атаки, фішинг, шкідливе програмне забезпечення та інші засоби, що дозволяють проникнути до корпоративних систем, викрасти інформацію або завдати шкоди їхній роботі.

2. Використання застарілого програмного забезпечення.

Невстановлені оновлення та патчі для операційних систем або прикладних програм створюють вразливості, які з часом стають відомими широкому колу зловмисників. Регулярна актуалізація програмного забезпечення є критичною умовою підтримання належного рівня захисту.

3. Недостатній рівень автентифікації та слабкі паролі.

Прості або повторювані паролі, а також відсутність механізмів багатофакторної аутентифікації значно підвищують ризик компрометації облікових записів і доступу до інформаційних ресурсів [21].

4. Успішні атаки соціальної інженерії.

Шахрайські техніки, спрямовані на маніпуляцію співробітниками, можуть використовуватися для отримання доступу до інформаційних систем. Недостатня обізнаність персоналу створює сприятливі умови для таких загроз.

5. Внутрішні ризики та інсайдерські загрози.

До потенційних порушень належать як навмисні дії недобросовісних співробітників, так і ненавмисні помилки персоналу, які можуть призвести до витоку даних або порушення роботи підприємства.

6. Пересилання даних без шифрування.

Передавання інформації у відкритому вигляді робить її вразливою до перехоплення, аналізу або модифікації третіми особами.

7. Відсутність належної системи резервного копіювання.

У разі втрати, пошкодження або шифрування даних внаслідок кібератаки брак резервних копій може спричинити важкі функціональні та фінансові наслідки.

8. Надмірно широкі права доступу.

Надання великій кількості співробітників доступу до конфіденційної інформації збільшує ймовірність ненавмисного витоку або умисного зловживання.

9. Недостатній моніторинг та слабкий контроль безпеки.

Відсутність системного відстеження подій безпеки ускладнює своєчасне виявлення інцидентів, що дозволяє загрозам залишатися непоміченими протягом тривалого часу.

10. Використання застарілої апаратної та програмної інфраструктури.

Обладнання та програмне забезпечення, що давно не оновлювалися, можуть мати численні відомі вразливості, які активно експлуатуються зловмисниками (рис. 2.3).

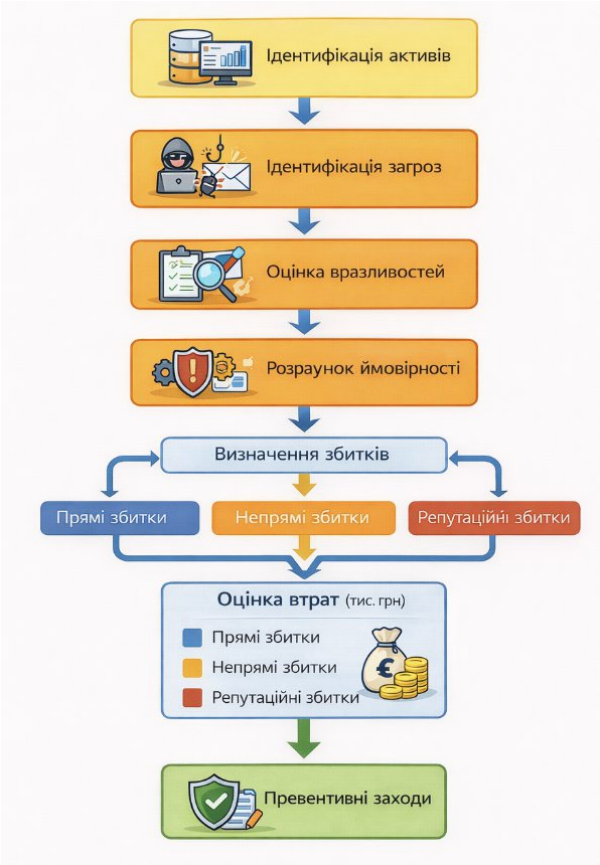

Рис. 2.3 Алгоритм застосування методики оцінки фінансових втрат організації, спричинених інформаційними загрозами

Для ефективного зниження зазначених ризиків підприємству необхідно розробити та реалізувати комплексну стратегію кіберзахисту, що включає технічні та організаційні заходи, регулярне навчання персоналу, належну політику доступу й безперервний моніторинг стану інформаційної безпеки.

2.2.2 Підходи та методи оцінки ризиків і фінансових втрат від інформаційних інцидентів

На відміну від загроз, які мають потенційний характер, ризик відображає ймовірність реалізації загрози та масштаб можливих негативних наслідків. У цьому контексті ризик доцільно розглядати як поєднання ймовірності виникнення інформаційного інциденту та величини збитків, які можуть бути завдані організації в разі його реалізації.

Інформаційний інцидент є практичною формою реалізації інформаційного ризику та проявляється у вигляді порушення встановлених вимог інформаційної безпеки. Такими порушеннями можуть бути несанкціонований доступ до інформації, її витік, модифікація або знищення, а також порушення доступності інформаційних систем [8]. Інформаційні інциденти виникають у результаті дії як зовнішніх, так і внутрішніх загроз і, на відміну від самих загроз, мають конкретні наслідки для функціонування інформаційної інфраструктури та бізнес-процесів організації.

Наслідком інформаційних інцидентів є виникнення збитків, які можуть мати різну природу та масштаб. У практиці управління інформаційною безпекою прийнято розрізняти прямі та непрямі збитки. Прямі збитки пов’язані з безпосередніми фінансовими витратами, що виникають унаслідок інциденту, зокрема витратами на відновлення інформаційних систем, ліквідацію наслідків кібератак, залучення фахівців, а також сплатою штрафів і компенсацій. Такі збитки, як правило, можуть бути кількісно оцінені та відображені у фінансовій звітності організації.

Непрямі збитки мають менш очевидний, але часто більш суттєвий характер і проявляються у довгостроковій перспективі. До них належать репутаційні втрати, зниження довіри клієнтів і партнерів, втрата конкурентних позицій, а також зменшення доходів унаслідок порушення бізнес-процесів. Складність оцінки непрямих збитків полягає в їх відкладеному характері та залежності від зовнішніх факторів, що ускладнює прийняття управлінських рішень без застосування спеціальних методичних підходів.

Оцінка ризиків і фінансових втрат від інформаційних інцидентів базується на чіткому розумінні взаємозв'язку між загрозами, інформаційними інцидентами та збитками [9]. Усвідомлення цієї логіки створює передумови для застосування формалізованих методів оцінки ризиків і втрат, які дозволяють перейти від якісного опису проблеми до кількісного обґрунтування управлінських рішень у сфері інформаційної та кібернетичної безпеки.

У практиці управління інформаційною безпекою для оцінки ризиків застосовуються як якісні, так і кількісні підходи, кожен з яких має власні переваги та обмеження. Для узагальнення відмінностей між зазначеними підходами доцільно здійснити їх порівняльний аналіз (табл. 2.6).

Наведене порівняння свідчить, що якісні підходи, засновані переважно на експертних і суб'єктивних оцінках, не забезпечують достатньої точності для обґрунтованого визначення фінансових втрат від інформаційних інцидентів. У свою чергу, кількісні підходи дозволяють перейти від загальних характеристик ризику до його економічної оцінки, що зумовлює потребу у використанні структурованих методик оцінювання втрат, орієнтованих на підтримку управлінських рішень.

З метою підвищення точності оцінки ризиків та обґрунтування управлінських рішень доцільно використовувати формалізовані методології, зокрема FAIR, NIST SP 800-30 та ISO/IEC 27005.

Таблиця 2.6.

Порівняльна характеристика підходів до оцінки інформаційних ризиків і втрат

Критерій порівняння	**Якісні підходи**	**Кількісні підходи**
Основа оцінювання	Експертні судження, досвід фахівців	Статистичні дані, розрахункові моделі
Форма результату	Описова (низький / середній / високий ризик)	Числові показники (грошові втрати, ймовірності)
Рівень суб’єктивності	Високий	Низький або помірний
Точність оцінки	Обмежена	Вища за умови наявності даних
Можливість фінансового аналізу	Обмежена або відсутня	Повноцінна
Придатність для управлінських рішень	Орієнтовна	Обґрунтована
Основні недоліки	Суб’єктивність, залежність від експерта	Складність реалізації, потреба в даних
Сфера доцільного застосування	Попередній аналіз, невеликі організації	Оцінка втрат, стратегічне управління ризиками

Метод FAIR (Factor Analysis of Information Risk) дозволяє перевести кіберризики у грошовий вимір, оцінюючи частоту інцидентів (Loss Event Frequency) та величину втрат (Loss Magnitude). Це забезпечує кількісну основу для управління ризиками і дає змогу порівнювати альтернативні сценарії впливу.

Методологія NIST SP 800-30, розроблена Національним інститутом стандартів і технологій (США), передбачає етапний підхід до оцінки ризиків, включаючи ідентифікацію загроз, вразливостей, аналіз впливу та визначення рівня ризику. Її гнучкість дозволяє використовувати як якісні, так і кількісні оцінки.

Стандарт ISO/IEC 27005 забезпечує процесуальну основу для управління ризиками в системах інформаційної безпеки, передбачаючи постійне оновлення ризик-аналізу у відповідності до змін у середовищі загроз.

Усі три підходи орієнтовані на практичне застосування результатів оцінки – від бюджетування заходів безпеки до прийняття стратегічних рішень щодо захисту критичних активів.

2.2.3 Оцінювання економічних наслідків виникнення інформаційних інцидентів

Заходи, спрямовані на мінімізацію ризиків та забезпечення належного рівня безпеки в цифровому середовищі, охоплюють широкий спектр технічних та організаційних рішень. Основні з них включають [24]:

1. Використання антивірусних і антиспам-рішень.

Встановлення сучасних антивірусних програмних продуктів та систем фільтрації небажаних повідомлень, а також регулярне їх оновлення, дозволяє своєчасно виявляти шкідливе програмне забезпечення, блокувати спроби вторгнення та зменшувати кількість спам-трафіку.

2. Контроль доступу та удосконалені механізми автентифікації.

Запровадження вимог до складності паролів, а також використання багатофакторної аутентифікації істотно знижують ймовірність несанкціонованого доступу до корпоративних ресурсів.

3. Шифрування даних.

Застосування криптографічних методів захисту інформації як під час її зберігання, так і в процесі передавання забезпечує конфіденційність даних та унеможливлює їх перехоплення чи модифікацію сторонніми особами.

4. Своєчасне оновлення програмних і апаратних компонентів.

Регулярне встановлення патчів та оновлень для операційних систем, прикладного програмного забезпечення й мережевого обладнання є критичним фактором усунення вразливостей, які можуть бути використані зловмисниками.

5. Сегментація мережевої інфраструктури.

Логічне розділення корпоративної мережі на ізольовані сегменти з використанням міжмережевих екранів дозволяє локалізувати потенційні загрози та мінімізувати їх поширення в разі компрометації окремої ділянки.

6. Протидія методам соціальної інженерії.

Регулярне навчання співробітників, підвищення їхньої обізнаності щодо фішингових атак та інших маніпуляційних технік сприяє формуванню безпечної поведінки та знижує ризик людського фактору.

7. Постійний моніторинг і аудит безпеки.

Систематичне проведення аудитів, а також використання інструментів моніторингу подій безпеки дозволяє виявляти аномальні дії та оперативно реагувати на потенційні інциденти.

8. Резервне копіювання та відновлення інформаційних систем.

Формування політики з резервного копіювання, регулярне створення копій важливих даних і тестування процедур відновлення забезпечують безперервність роботи підприємства у випадку кібератаки або технічної аварії.

9. Політики та навчання з кібербезпеки.

Розроблення та впровадження внутрішньої політики кіберзахисту, а також навчання персоналу правилам її дотримання формує основу для створення безпечного інформаційного середовища.

10. Запобігання витоку інформації (DLP).

Застосування систем контролю та обмеження доступу до конфіденційних даних, а також використання рішень для відстеження їх переміщення дозволяє мінімізувати ризики розголошення або втрати інформації [24, 25].

Зазначені заходи забезпечують комплексний підхід до зниження кіберризиків і створюють умови для надійного функціонування інформаційних систем підприємства.

Висновки до розділу 2

У другому розділі кваліфікаційної роботи проведено аналіз функціонування та вразливостей інформаційної інфраструктури досліджуваного підприємства ТОВ «Інфотех Солюшнс». Встановлено, що специфіка діяльності компанії, пов’язаної з реалізацією промислових енергетичних об’єктів «під ключ», зумовлює високу залежність основних бізнес-процесів від інформаційних систем та ІТ-інфраструктури.

У ході дослідження структури інформаційних ресурсів визначено, що підприємство обробляє значні обсяги фінансової, технічної, кадрової та проєктної інформації, яка має різний рівень критичності та конфіденційності. Інтенсивний обмін даними між управлінськими, фінансовими та виробничими підрозділами підвищує ризики порушення конфіденційності, цілісності й доступності інформації у разі реалізації інформаційних загроз.

Діагностика внутрішніх і зовнішніх факторів впливу на рівень інформаційної безпеки показала, що найбільш значущими є внутрішні ризики, пов’язані з людським чинником, організаційними недоліками та рівнем обізнаності персоналу. Водночас зовнішні загрози, зокрема кібератаки, регуляторні вимоги та ризики, пов’язані з контрагентами, створюють додаткові виклики для системи захисту інформації.

РОЗДІЛ 3 РОЗРОБКА МЕТОДИЧНИХ ПІДХОДІВ ДО ОЦІНКИ ВТРАТ ВІД ІНФОРМАЦІЙНИХ ЗАГРОЗ

3.1 Обґрунтування вибору методик та формування моделі оцінювання потенційних втрат

Ефективне управління інформаційною безпекою в сучасних умовах неможливе без ґрунтовної оцінки потенційних втрат від реалізації інформаційних інцидентів. Таке оцінювання дозволяє не лише усвідомити рівень ризику, а й приймати обґрунтовані управлінські рішення щодо інвестування у заходи захисту. Для цього необхідно застосовувати відповідні методичні підходи, що дозволяють перейти від загальних міркувань до формалізованої, у тому числі й кількісної, оцінки ризиків.

У міжнародній практиці найбільш поширеними підходами до аналізу ризиків та втрат є:

˜ FAIR (Factor Analysis of Information Risk) – методика кількісної оцінки інформаційного ризику, що дозволяє обраховувати ймовірність інциденту та фінансові втрати. Її перевага полягає в економічній конкретиці – вона дає можливість прив’язати ризики до фінансових показників.

˜ NIST Risk Management Framework (RMF) – методологія Національного інституту стандартів і технологій США, яка фокусується на комплексному управлінні ризиками протягом усього життєвого циклу IT-систем. Хоча RMF не дає прямого фінансового моделювання, вона забезпечує чіткий процес оцінки та моніторингу ризиків.

˜ ISO/IEC 27005 – міжнародний стандарт, що надає загальні принципи і підходи до управління інформаційними ризиками. Його перевага – у гнучкості та інтеграції з іншими стандартами серії ISO/IEC 27000, проте стандарт сам по собі не містить чіткої методики фінансової оцінки втрат.

Зважаючи на потреби підприємства у кількісному обґрунтуванні заходів з інформаційної безпеки, доцільним є поєднання двох підходів:

˜ Використання методики FAIR як основи для формування кількісної моделі оцінювання потенційних втрат;

˜ Інтеграція структурного підходу ISO/IEC 27005 для ідентифікації активів, вразливостей та загроз, що формують контекст аналізу.

У результаті формується гібридна модель оцінювання втрат, яка включає:

1. Визначення активів та їхньої цінності для підприємства.
2. Ідентифікацію загроз та ймовірності їх реалізації.
3. Аналіз вразливостей, що можуть бути використані.
4. Оцінку потенційних наслідків (прямих і непрямих збитків).
5. Розрахунок очікуваного річного збитку (ALE – Annual Loss Expectancy).

На рис. 3.1 представлено схему, що узагальнює логіку побудови моделі оцінювання потенційних втрат на основі вищезгаданих методик.

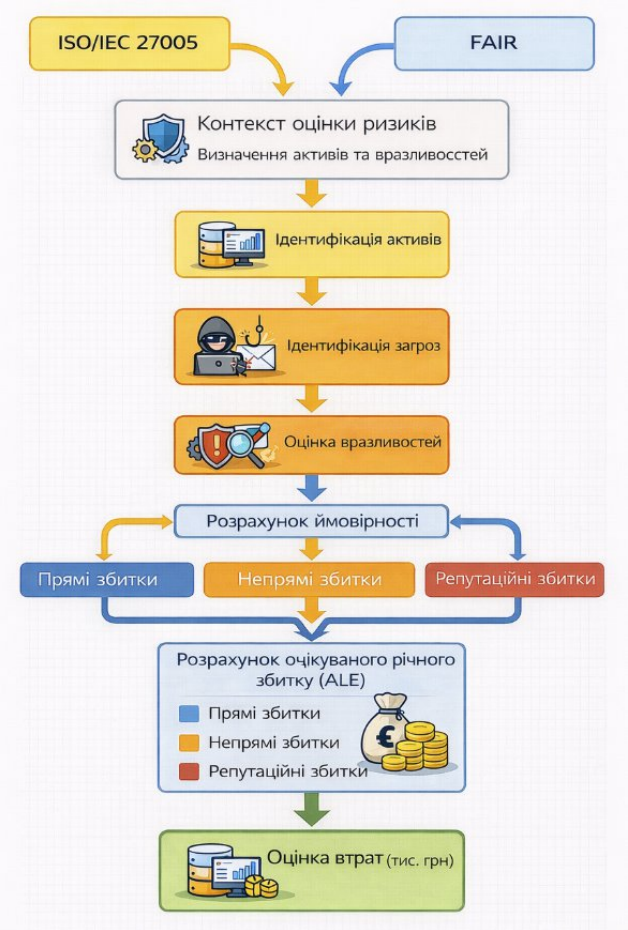

Рис. 3.1. Схема формування моделі оцінювання потенційних втрат на основі підходів FAIR та ISO/IEC 27005.

На основі сформованої моделі підприємство може:

- Визначити пріоритетність захисних заходів.
- Порівнювати потенційні збитки з витратами на безпеку.
- Оцінити рентабельність ІБ-інвестицій (ROI для безпеки).
- Побудувати динамічну систему моніторингу та реагування.

Після формування моделі доцільно перейти до розробки комплексу заходів, спрямованих на мінімізацію визначених ризиків. Такий перелік буде представлено в табл. 3.1, яка узагальнює практичні дії для підвищення кіберстійкості підприємства.

Таблиця 3.1

Комплекс заходів для зниження ризиків і зміцнення інформаційної безпеки

№	Назва заходу	Сутність заходу
1	Аудит і аналіз поточного стану	Проведення комплексного обстеження інформаційних систем, мережевої інфраструктури та бізнес-процесів з метою виявлення вразливостей і визначення пріоритетних напрямів підвищення рівня інформаційної безпеки.
2	Політики та процедури	Формування внутрішніх політик і регламентів з інформаційної безпеки, які визначають правила роботи з конфіденційними даними, вимоги до їх збереження та порядок реагування на інциденти.
3	Освітні програми та навчання	Забезпечення регулярного навчання співробітників щодо принципів кібергігієни, безпечного використання інформаційних ресурсів і сучасних кіберзагроз.
4	Захист мережевої інфраструктури	Впровадження мережевих засобів захисту: міжмережевих екранів, антивірусних систем, IDS/IPS-рішень, а також механізмів централізованого контролю

		доступу до інформаційних ресурсів.

Продовження таблиці 3.1

5	Використання шифрування	Застосування криптографічних засобів для захисту конфіденційних даних під час їх передавання та зберігання, що мінімізує ризики несанкціонованого доступу.
6	Резервне копіювання та відновлення даних	Створення регулярних резервних копій критичних даних і розроблення процедур швидкого відновлення у разі кібератак, технічних збоїв або надзвичайних ситуацій.
7	Моніторинг і аналіз подій	Встановлення систем для безперервного моніторингу, збору та аналізу подій інформаційної безпеки з метою оперативного виявлення аномалій та інцидентів.
8	Фізична безпека	Обмеження фізичного доступу до серверних приміщень, телекомунікаційного обладнання та інших критичних зон з метою запобігання несанкціонованому втручанню.
9	Аутентифікація та авторизація	Використання надійних механізмів підтвердження особи користувачів та чітких правил розмежування їхніх повноважень щодо доступу до інформаційних систем і даних.
10	Управління ризиками	Систематична оцінка ризиків та формування стратегії їх мінімізації шляхом визначення пріоритетних загроз і заходів із їх усунення.
11	Дотримання нормативних вимог	Забезпечення відповідності законодавчим нормам і стандартам інформаційної безпеки, ведення належної звітності та документації.

Продовження таблиці 3.1

12	Тестування та аудит безпеки	Проведення планових перевірок, включно з тестуванням на проникнення та аудитами, що допомагають визначити фактичний рівень захищеності систем.
13	Аналіз трендів у сфері загроз	Постійний моніторинг нових видів кібератак і технологічних ризиків, а також адаптація політик та заходів реагування відповідно до актуальних тенденцій.
14	Постійне вдосконалення системи безпеки	Регулярний перегляд стану інформаційної безпеки та впровадження оновлень, що підвищують стійкість інфраструктури до нових викликів.
15	Захист на рівні постачальників і партнерів	Контроль виконання вимог безпеки зовнішніми підрядниками й партнерами, забезпечення захищеності ланцюгів постачання та взаємодії між організаціями.

Таким чином, у табл. 3.1 представлено узагальнений комплекс заходів, що можуть бути використані для підвищення рівня інформаційної безпеки підприємства. Конкретний набір дій формується з урахуванням результатів проведеного аудиту, особливостей оброблюваних даних, специфіки інфраструктури та низки інших факторів. Стратегія забезпечення інформаційної безпеки повинна мати індивідуальний характер і адаптуватися до потреб, ризиків та операційних особливостей кожного окремого бізнесу.

3.2 Інтерпретація результатів розрахунків та визначення найбільш критичних ризиків

Метою впровадження та експлуатації такої системи є забезпечення постійного контролю за станом клієнтських пристроїв, які функціонують поза межами корпоративної інфраструктури (локальної мережі чи VPN-тунелю). Передусім здійснюється моніторинг актуальності оновлень операційної системи, стану антивірусного захисту, наявності встановленого програмного забезпечення, а також перевірка активності механізму шифрування BitLocker.

Система орієнтована на керування пристроями, що не мають прямого підключення до внутрішньої мережі підприємства. До ключових переваг такого підходу можна віднести [26]:

- повний контроль над серверами та ролями, які забезпечують надання відповідних послуг;
- відсутність залежності від зовнішніх хмарних платформ та сторонніх сервісів;
- можливість функціонування без використання VPN-каналу;
- локалізація всіх витрат у межах внутрішньої інфраструктури підприємства.

Оскільки взаємодія з клієнтськими пристроями відбувається у відкритому мережевому середовищі, підвищені вимоги до безпеки зумовлюють необхідність використання сертифікатів PKI. Такий підхід забезпечує незалежну автентифікацію обох сторін з’єднання, а передавані між сервером та клієнтами дані проходять шифрування, що гарантує їх конфіденційність і цілісність.

Узагальнена схема функціонування системи подана на рис. 3.2.

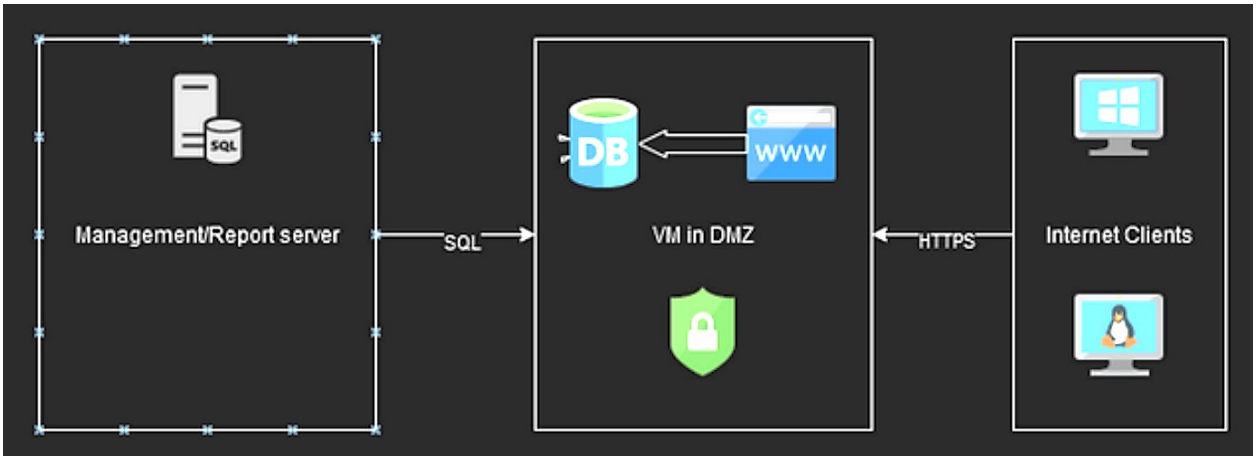

Рис. 3.2 Структурна схема процесу передавання інформації до БД

Інфраструктура системи побудована таким чином, що база даних моніторингу та веб-сайт керування розміщуються в мережі периметра. У цьому ж сегменті функціонує контролер домену в режимі "read-only", який забезпечує автентифікацію користувачів. Між периметровою та внутрішніми мережами встановлений міжмережевий екран, що виконує роль бар'єра безпеки та контролює усі взаємодії [26, 27].

Передавання зібраних клієнтом відомостей здійснюється через захищений протокол HTTPS. Отримавши дані, веб-сайт проводить їх валідацію та заносить у тимчасову базу даних. Далі сервер основної БД та системи керування переміщує інформацію з периметрової, менш захищеної БД, у внутрішнє високозахищене сховище, доступ до якого мають лише співробітники, уповноважені на адміністрування.

Подібна конфігурація є доцільною в кількох практичних сценаріях:

- для клієнтських пристроїв, які не матимуть можливості під'єднання до внутрішньої мережі підприємства, наприклад для техніки у віддалених точках продажу;
- у випадках, коли необхідно обмежити взаємодію клієнта лише одним каналом – HTTPS, що важливо для дотримання жорстких політик безпеки або специфічних вимог брандмауера;
- для централізованого керування робочими станціями у внутрішній інфраструктурі.

В межах захищеної мережі для комплексного адміністрування клієнтських ПК доцільно використовувати безкоштовну платформу Tactical RMM. Це рішення з відкритим вихідним кодом побудоване з використанням Django, Vue та Go, і підтримує встановлення Windows-агента. Система має інтеграцію з платформою MeshCentral, що показано на рис. 3.3.

Tactical RMM надає широкий набір функціональних можливостей, які характерні для професійних RMM-рішень, серед яких:

- дистанційне керування робочими станціями через MeshCentral;
- централізоване встановлення оновлень Windows;
- віддалене виконання команд та запуск скриптів різних типів (PowerShell, batch, Python);
- автоматизований моніторинг стану систем з можливістю надсилання сповіщень електронною поштою або SMS (контроль ЦП, пам’яті, дисків, журналів подій тощо);
- ведення інвентаризації апаратного та програмного забезпечення;
- запуск завдань і скриптів за розкладом;
- віддалене встановлення програмного забезпечення через Chocolatey;
- керування службами операційної системи;
- доступ до інтерактивної віддаленої оболонки в реальному часі.

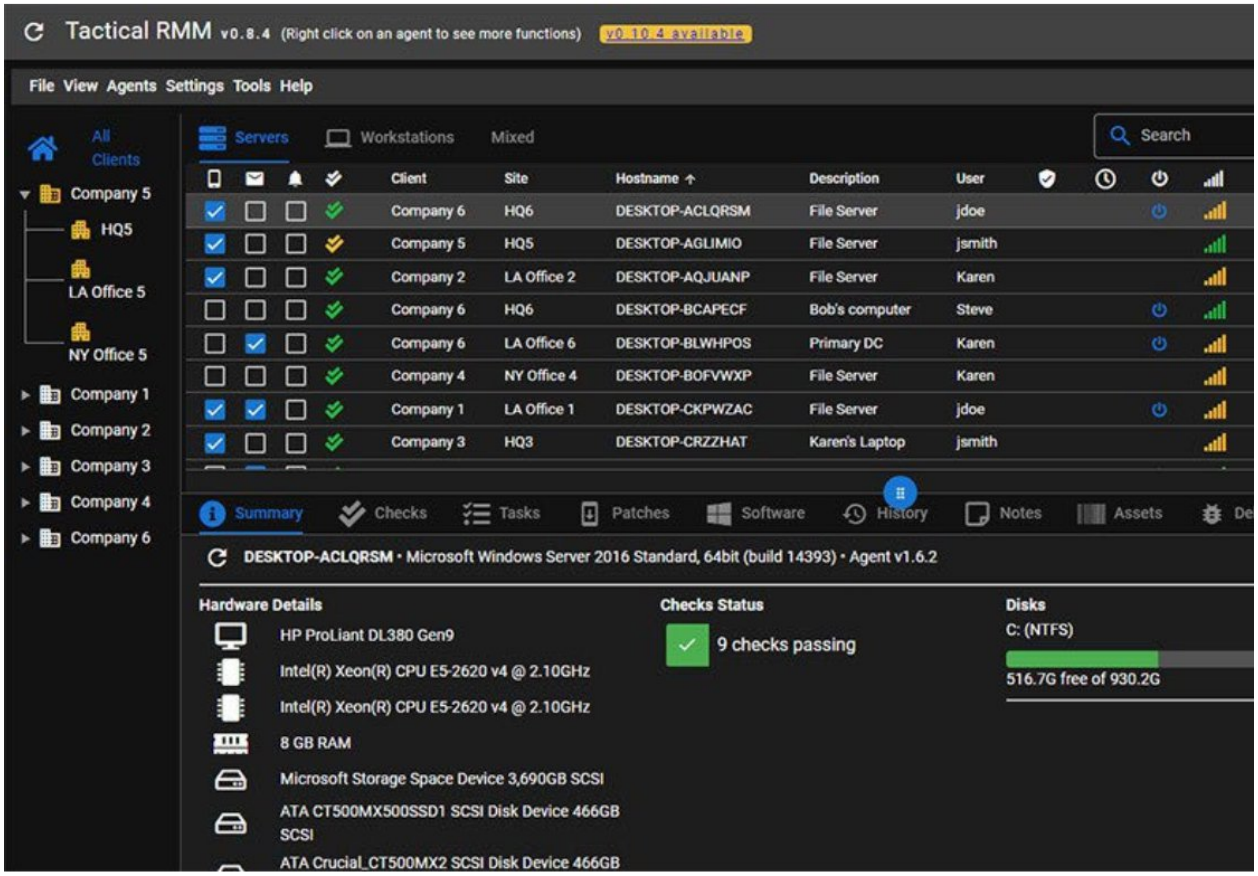

Рис. 3.3 Інтерфейс програмного забезпечення Tactical RMM

Основні переваги впровадження програмного забезпечення Tactical RMM на ТОВ «Інфотех Солюшнс» полягають у наступному [27].

По-перше, із розширенням функціональності комерційних RMM-рішень вони часто стають надмірно складними в експлуатації. Велика кількість інтегрованих можливостей, накопичених роками розвитку таких продуктів, нерідко ускладнює їх освоєння та налаштування, що може створювати додаткові бар'єри для ефективної роботи IT-персоналу. На цьому тлі Tactical RMM вигідно вирізняється більш зрозумілим і раціонально структурованим набором інструментів, який забезпечує виконання ключових завдань без перевантаження інтерфейсу другорядними функціями.

По-друге, вагомою перевагою є те, що Tactical RMM – це сучасне, легке та водночас достатньо потужне рішення. Незважаючи на те, що за кількістю можливостей воно поки що поступається великим пропрієтарним системам, які розвиваються десятиліттями, програма ефективно виконує базові задачі,

необхідні для повноцінного віддаленого управління робочими станціями підприємства.

Оскільки Tactical RMM є продуктом з відкритим програмним кодом, підприємство отримує значно ширший контроль над його розвитком і використанням. Це мінімізує залежність від зовнішніх факторів – таких як зміна політики постачальника, підвищення вартості ліцензій, вилучення функціоналу або продаж продукту іншій компанії. Таким чином, підприємство уникає ризику втрати доступу до ключових можливостей або вимушеної адаптації до небажаних комерційних змін.

Ще однією суттєвою перевагою є можливість повноцінної персоналізації. На практиці індивідуальне налаштування RMM не обмежується зміною логотипів чи оформлення інтерфейсу. Найбільшою цінністю є здатність адаптувати функціональність системи до внутрішніх бізнес-процесів компанії. Завдяки відкритому коду ТОВ «Інфотех Солюшнс» може за потреби модифікувати або форкувати систему під власні робочі сценарії, що недоступно при використанні закритих комерційних платформ.

Таким чином, впровадження Tactical RMM забезпечує підвищення рівня інформаційної безпеки, оптимізацію контролю за IT-інфраструктурою та формує умови для відповідності сучасним вимогам клієнтів і стандартам кіберзахисту в перспективі.

3.3 Розроблення рекомендацій для зменшення можливих втрат і підвищення стійкості організації до інформаційних загроз

У процесі реалізації проекту, спрямованого на встановлення системи контролю за клієнтськими комп’ютерами як у локальних, так і у зовнішніх мережах, передбачається придбання нового сервера вартістю 100 тис. Грн. Для визначення економічної доцільності та ефективності такого проєкту використовуються ключові індикатори інвестиційного аналізу, серед яких: чистий дисконтований дохід (NPV), індекс рентабельності (PI) та період

окупності інвестицій (PP). Зазначені критерії ґрунтуються на принципі дисконтування майбутніх грошових надходжень і є загальноприйнятими у міжнародній практиці як основні показники оцінювання результативності інвестиційних проєктів. Вони дозволяють узагальнити всі вигоди, отримані від упровадження проєкту, та надати структуровану оцінку його економічної ефективності [28].

1. Чистий дисконтований дохід (NPV).

Цей показник відображає абсолютну величину економічного ефекту, яку підприємство може отримати в результаті реалізації проєкту, з урахуванням приведення майбутніх грошових потоків до теперішньої вартості.

$$ЧДД = -К + \frac{\Delta П1}{(1+i)^1} + \frac{\Delta П2}{(1+i)^2} + \frac{\Delta П3}{(1+i)^3}, \quad (3.1)$$

де К – обсяг капітальних інвестицій, грн;

і – ставка дисконтування, що використовується для приведення майбутніх грошових потоків до теперішньої вартості;

ΔП – величина чистого прибутку, грн.

Ставку дисконтування визначають на основі рівняння Фішера, яке використовується для розрахунку реальної норми доходності з урахуванням інфляційних процесів у економіці [29].

$$i = а + в + в * a, \quad (3.2)$$

де а – прогнозований рівень інфляції;

в – номінальна відсоткова ставка за депозитом, що використовується як орієнтир для визначення вартості капіталу.

Відповідно до положень Закону України «Про Державний бюджет України на 2025 рік», прогнозований індекс інфляції на 2025 рік становить 9,7%. Середня

дохідність депозитних вкладів у банківських установах, зокрема в АТ КБ «ПриватБанк», перебуває на рівні 10,5%.

$$I = 0{,}097 + 0{,}105 + 0{,}105 * 0{,}097 = 0{,}212 \quad (3.3)$$

2. Період окупності інвестиційного проєкту визначається за такою формулою:

$$\text{ПО} = \frac{\text{К}}{\text{СГДП}}, \quad (3.4)$$

де К – сума капітальних інвестицій, грн;

СГДП – середньорічний грошовий дохід (грошовий потік), грн.

Середньорічний грошовий потік визначається за такою формулою:

$$\text{СГДП} = \frac{\text{ГП}}{n}, \quad (3.5)$$

де n – тривалість реалізації інвестиційного проєкту, тобто кількість років, протягом яких очікується отримання грошових надходжень [29].

3. Індекс доходності (рентабельності) інвестиційного проєкту визначається за такою формулою:

$$\text{ІД} = \frac{\text{ГП}}{\text{К}}, \quad (3.6)$$

Сумарний обсяг інвестицій, необхідний для впровадження даного проєкту, подано в табл. 3.2.

Таблиця 3.2

Розрахунок інвестицій, необхідних для впровадження проєкту підвищення рівня інформаційної безпеки на ТОВ «Інфотех Солюшнс»

Назва обладнання	Необхідна кількість	Вартість одиниці, тис. грн	Разом, тис. грн
1. Сервер	2	110	220
2. Блок безперебійного живлення для кожного сервера, який забезпечує автономну роботу протягом 4 годин	2	215	430
РАЗОМ	-	-	650

Для оцінювання економічної результативності запропонованого технологічного заходу визначимо очікуваний приріст фінансових надходжень. Зокрема, прогнозована щорічна додаткова виручка, отримана завдяки зростанню довіри клієнтів та відповідності підприємства встановленим вимогам інформаційної безпеки, становить 317 091,25 грн. Цей приріст зумовлений збільшенням кількості укладених контрактів та підвищенням конкурентоспроможності компанії.

$$ЧДД = -650000 + \frac{317091,25}{(1+0,212)^1} + \frac{317091,25}{(1+0,212)^2} + \frac{317091,25}{(1+0,212)^3} + \frac{317091,25}{(1+0,212)^4} + \frac{317091,25}{(1+0,212)^5} = 213901,09 \text{ грн.},$$

$$СГДП = \frac{650000}{5} = 172783,17 \text{ грн.}$$

$$ПО = \frac{650000}{172783,17} = 3,76 \text{ років.}$$

$$ІД = 863903,12 = 1,33 \text{ грн.}$$

Отже, проведені розрахунки дають змогу стверджувати, що запропонований проєкт є економічно доцільним. Чистий дисконтований дохід становить 213 901,09 грн, індекс доходності дорівнює 1,33 грн/грн, а період окупності інвестицій – приблизно 3 роки 9 місяців. Такі показники підтверджують прийнятний рівень інвестиційної привабливості та перспективність реалізації проєкту [30].

Разом із тим, упровадження будь-якого інвестиційного заходу супроводжується певним рівнем ризику, оскільки на нього впливають як внутрішні, так і зовнішні чинники. Щоб мінімізувати невизначеність, необхідно ідентифікувати потенційні ризики та здійснити їхню всебічну оцінку. Найбільш небезпечними вважаються ті види ризиків, на які підприємство практично не може вплинути, тобто зовнішні ризики. Наприклад, зміна інфляційних показників може відчутно позначатися на ефективності інвестицій. Тому їх важливо враховувати під час обґрунтування доцільності впровадження проєкту.

Для аналізу ризиків використано метод експертних оцінок, який передбачає залучення кваліфікованих фахівців для визначення рівня впливу та ймовірності настання кожного виду ризику. На основі попередньо сформованого переліку можливих ризиків було підготовлено анкету, що містила 12 запитань. Експертам пропонувалося оцінити кожен ризик за шкалою від 1 до 10 балів та визначити ймовірність його настання [30].

На підставі зібраних даних було визначено середню ймовірність появи кожного виду ризику як середньоарифметичне значення оцінок експертів, а також розраховано сумарний інтегральний показник ризику з урахуванням середньої вагомості ризикових чинників. Отримані результати подано у табл. 3.3.

Таблиця 3.3

Оцінювання рівня ризикованості запропонованого заходу (перероблений варіант)

№	Види ризику	Середня вагомість ризику	Сумарна оцінка
1	2	3	4
Помилки у прогнозуванні попиту та ринкових тенденцій			20,3
1	Помилки у прогнозуванні попиту та ринкових тенденцій	0,59	12,40
2	Недоліки в етапі планування та формуванні технічного завдання	0,41	7,90
№	Види ризику	Середня вагомість ризику	Сумарна оцінка
Проєктні ризики інвестиційної фази:			17,95
3	Зміна вартості обладнання внаслідок коливання валютного курсу	0,44	9,25
4	Порушення строків постачання обладнання	0,18	2,55
5	Виявлення дефектів або несправностей обладнання	0,27	4,10
6	Відмова постачальників виконувати попередні домовленості	0,16	2,05

Продовження таблиці 3.3

№	Види ризику	Середня вагомість ризику	Сумарна оцінка
Проєктні ризики експлуатаційної фази:			18,75
7	Зростання цін на матеріали та енергоресурси	0,24	4,20
8	Технологічні ризики, пов’язані з нестачею кваліфікованої робочої сили	0,14	2,35
9	Поява додаткових конкурентів на ринку	0,16	3,10
10	Ризики, пов’язані з виробничим браком	0,21	4,15
11	Вихід з ладу обладнання, що відпрацювало нормативний строк	0,09	1,50
12	Коригування державної податкової політики	0,21	3,45

У ролі експертів було залучено провідних фахівців підприємства, управлінський персонал, а також менеджерів середньої та вищої ланки. До експертної групи увійшли керівники та заступники планово-економічного відділу, керівники виробничих підрозділів, головний інженер та інші спеціалісти, які володіють необхідним досвідом та компетенціями для об’єктивного оцінювання ризиків.

Оскільки анкета містить 12 факторів ризику, максимальний можливий інтегральний бал становить 120, мінімальний – 12. Відповідно до методики інтервали оцінювання рівня ризиковості інвестиційного проєкту мають такий вигляд:

- 12–48 балів – низький рівень ризику;
- 49–84 бали – середній рівень ризику;
- 85–120 балів – високий (значний) рівень ризику.

Згідно з розрахунками (табл. 3.4), підсумкова зважена оцінка ризиків становить 56,33, що дає змогу віднести запропонований проєкт до категорії середньоризикових. Такий рівень ризику вважається прийнятним для більшості інноваційних та інвестиційних заходів, за умови реалізації відповідних механізмів управління ризиками.

Для більш наочного відображення впливу окремих ризиків на ефективність реалізації проєкту побудовано діаграму типу “роза ризиків” (рис. 3.4), яка демонструє відносну вагомість кожного фактору та допомагає сформувати пріоритети у процесі управління ризиками [30].

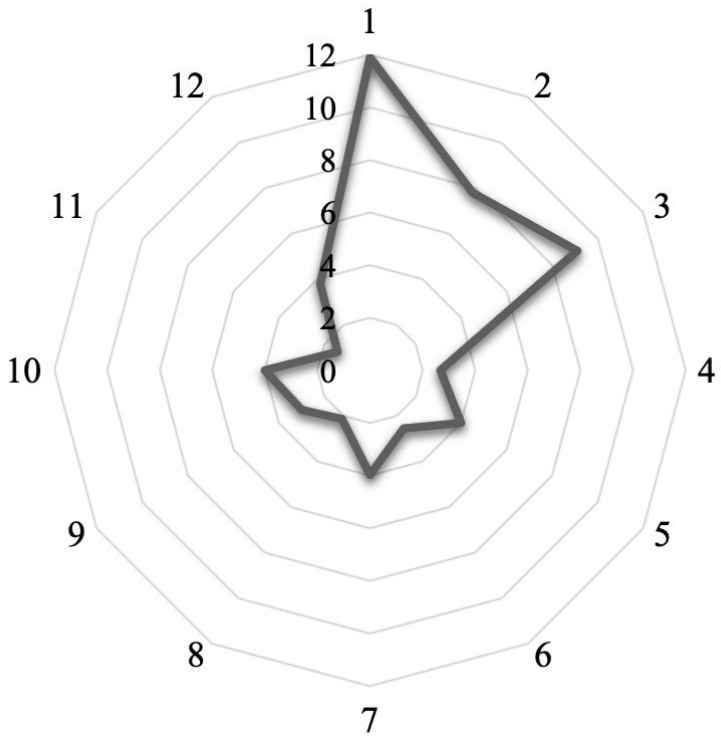

Рис. 3.4 Діаграма типу «роза ризиків», що відображає вплив окремих факторів на реалізацію заходу

Аналіз діаграми на рис. 3.3 дає підстави зробити висновок, що найбільш критичними для успішної реалізації заходу є ризики, пов’язані з точністю прогнозування ринкового попиту та ретельністю планування і проєктування

відповідних дій. Саме ці фактори мають найбільшу вагу та істотно впливають на кінцеві результати впровадження проєкту.

Для зниження рівня ризиковості важливо забезпечити коректне оцінювання потенційної кількості майбутніх контрактів, реалістично визначити можливі обмеження ринку та врахувати зовнішні чинники, що можуть позначитися на динаміці попиту. Зважене та обґрунтоване прогнозування дозволить підвищити точність планування та мінімізувати невизначеність під час реалізації проєкту.

Висновки до розділу 3

У ході дослідження сформовано модель оцінювання потенційних втрат, яка враховує як прямі фінансові збитки, пов’язані з ліквідацією наслідків інформаційних інцидентів, простоєм бізнес-процесів і штрафними санкціями, так і непрямі втрати, зумовлені репутаційними ризиками, зниженням довіри клієнтів і довгостроковими економічними наслідками для організації. Такий підхід дозволяє перейти від суто технічного аналізу інцидентів до їх комплексної економічної оцінки.

У межах розділу здійснено оцінювання економічних наслідків реалізації інформаційних інцидентів для досліджуваної організації, що дало змогу ідентифікувати найбільш критичні ризики та визначити їх вплив на ключові бізнес-процеси й фінансову стабільність підприємства. Інтерпретація результатів розрахунків підтвердила доцільність використання кількісних методів оцінки втрат як інструменту підтримки управлінських рішень у сфері інформаційної та кібернетичної безпеки.

На основі отриманих результатів розроблено комплекс практичних рекомендацій, спрямованих на зменшення можливих втрат і підвищення стійкості організації до інформаційних загроз. Запропоновані заходи охоплюють організаційні, технічні та управлінські аспекти, зокрема

вдосконалення процесів управління інформаційними ризиками, підвищення рівня контролю за критичними інформаційними активами та обґрунтування інвестицій у заходи безпеки з урахуванням потенційних економічних наслідків.

ВИСНОВКИ

У результаті виконання кваліфікаційної роботи досягнуто поставленої мети – розроблено методичний підхід до оцінювання можливих втрат організації від впливу інформаційних загроз та сформовано практичні рекомендації щодо мінімізації збитків і підвищення рівня стійкості інформаційної інфраструктури.

Для досягнення визначеної мети у роботі послідовно виконано та розкрито такі науково-практичні завдання:

1. Досліджено теоретичні засади забезпечення інформаційної безпеки організацій та обґрунтовано роль оцінки втрат як ключового елементу системи управління інформаційними ризиками. Встановлено, що інформаційна безпека має не лише технічний, а й виражений економічний та управлінський вимір, оскільки наслідки інформаційних інцидентів безпосередньо впливають на фінансову стабільність і безперервність бізнес-процесів.

2. Проаналізовано інформаційну інфраструктуру досліджуваного підприємства та визначено ключові інформаційні активи, вразливості й потенційні ризики. Виявлено відсутність централізованої системи управління інформаційною безпекою, формалізованих політик доступу, механізмів реагування на інциденти та планів забезпечення безперервності діяльності, що суттєво підвищує ймовірність виникнення значних прямих і непрямих втрат.

3. Розроблено методичний підхід до оцінювання можливих втрат організації від впливу інформаційних загроз, який ґрунтується на поєднанні кількісної методології FAIR із процесним підходом до управління ризиками відповідно до ISO/IEC 27005 та рекомендацій NIST. Запропонований підхід дозволяє враховувати як частоту виникнення інформаційних інцидентів, так і величину потенційних збитків у фінансовому вимірі, що підвищує обґрунтованість управлінських рішень.

4. Інтерпретовано результати оцінювання ризиків і втрат, що дало змогу виокремити найбільш критичні сценарії реалізації інформаційних загроз для досліджуваного підприємства. Показано, що найбільші потенційні втрати

пов’язані з витоком конфіденційної проєктної та фінансової інформації, порушенням доступності ключових інформаційних систем і помилками персоналу, зумовленими недостатнім рівнем обізнаності у сфері кібербезпеки.

5. Розроблено комплекс практичних рекомендацій, спрямованих на мінімізацію можливих втрат і підвищення стійкості підприємства до інформаційних загроз. Запропоновані заходи охоплюють:

- організаційний рівень – створення функції інформаційної безпеки або введення посади відповідального за ІБ, розроблення політик доступу, реагування на інциденти та планів безперервності діяльності;
- технічний рівень – впровадження систем моніторингу подій безпеки (SIEM), контролю доступу, резервного копіювання та захисту від витоку даних;
- управлінський рівень – інтеграцію оцінки втрат у процеси прийняття управлінських рішень і планування інвестицій у заходи кібербезпеки;
- кадровий рівень – підвищення обізнаності персоналу шляхом навчання та формування культури відповідального поводження з інформацією.

Узагальнюючи результати дослідження, можна зробити висновок, що застосування розробленого методичного підходу дозволяє перейти від фрагментарного технічного реагування на інциденти до системного управління інформаційними ризиками з урахуванням їх економічних наслідків. Запропоновані рекомендації мають практичну цінність і можуть бути використані підприємствами для підвищення рівня інформаційної та кібернетичної безпеки, зменшення потенційних втрат і забезпечення стійкого розвитку в умовах зростання інформаційних загроз.

ПЕРЕЛІК ПОСИЛАНЬ

1. Деркач А. А. Управління інформаційною безпекою : навч. посіб. Харків : ХНЕУ, 2019. 256 с.

2. Коваленко О. П. Кібербезпека: сучасні виклики та загрози : монографія. Львів : ЛНУ імені Івана Франка, 2020. 290 с.

3. Морозов М. М. Основи інформаційної безпеки : підручник. Одеса : ОНПУ, 2017. 310 с.

4. Юдін О. К., Корченко О. Г., Конахович Г. Ф. Захист інформації в мережах передачі даних : підручник. Київ : Інтерсервіс, 2009. 716 с.

5. Корченко О. Г., Казмірчук С. В., Ахметов Б. Б. Системи оцінювання ризиків інформаційної безпеки : монографія. Київ : КОМПРИНТ, 2017. 312 с.

6. Іванченко О. Г. Аналіз загроз інформаційній безпеці в Україні // Інформаційна безпека. 2020. № 2. С. 15–22.

7. Мельник І. В. Управління ризиками в системах інформаційної безпеки // Вісник НТУУ «КПІ». 2021. № 4. С. 67–74.

8. Філатова Т. В., Івченко І. С. Якісні та кількісні методи оцінки ризиків інформаційної безпеки // Вісник Хмельницького національного університету. 2023. № 3. С. 322–329.

9. Цвілій О. О. Безпека інформаційних технологій та сучасний стан стандартів ISO/IEC 27k // Телекомунікаційні та інформаційні технології. 2014. № 2. С. 73–79.

10. Цвілій О. О. Системи управління інформаційною безпекою та їх гармонізація з міжнародними стандартами // Перспективні напрями захисту інформації : зб. наук. праць. Київ, 2015. С. 107–111.

11. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements URL: https://www.iso.org/standard/82875.html (дата звернення: 20.10.2025).

12. ISO/IEC 27002:2022. Information security controls. URL: https://www.iso.org/standard/75652.html (дата звернення: 20.10.2025).

13. ISO/IEC 27005:2018. Information technology – Security techniques – Information security risk management . URL: https://www.iso.org/standard/75281.html (дата звернення: 20.03.2025).

14. ISO/IEC TR 27100:2017. Cybersecurity – Overview and concepts . URL: https://www.iso.org/standard/65633.html (дата звернення: 20.10.2025).

15. NIST SP 800-30 Rev.1. Guide for Conducting Risk Assessments . Gaithersburg : NIST, 2012. URL: https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final (дата звернення: 21.10.2025).

16. NIST SP 800-37 Rev.2. Risk Management Framework for Information Systems and Organizations . Gaithersburg : NIST, 2018. URL: https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final (дата звернення: 21.11.2025).

17. NIST SP 800-53 Rev.5. Security and Privacy Controls for Information Systems and Organizations . Gaithersburg : NIST, 2020. URL: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final (дата звернення: 21.11.2025).

18. Scarfone K., Mell P. Guide to Intrusion Detection and Prevention Systems (IDPS) : NIST SP 800-94 . Gaithersburg : NIST, 2007. URL: https://csrc.nist.gov/publications/detail/sp/800-94/final (дата звернення: 21.11.2025).

19. Freund J., Jones J. Measuring and Managing Information Risk: A FAIR Approach. Oxford : Butterworth-Heinemann, 2014. 432 p.

20. Hubbard D. W., Seiersen R. How to Measure Anything in Cybersecurity Risk. Hoboken : Wiley, 2016. 256 p.

21. Aven T. Risk Assessment and Risk Management. London : Springer, 2015. 310 p.

22. Northcutt S. Network Intrusion Detection. Indianapolis : New Riders, 2016. 480 p.

23. ENISA. Threat Landscape Report 2023. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023 (дата звернення: 22.11.2025).

24. Verizon. Data Breach Investigations Report 2024. URL: https://www.verizon.com/business/resources/reports/dbir/ (дата звернення: 22.03.2025).

25. World Economic Forum. Global Cybersecurity Outlook 2024 [Електронний ресурс]. Geneva : WEF. URL: https://www.weforum.org/reports/global-cybersecurity-outlook-2024 (дата звернення: 22.11.2025).

26. Петров В. В. Захист інформації в комп'ютерних системах. Київ : КНУ імені Тараса Шевченка, 2016. 275 с.

27. Ponemon Institute. Cost of a Data Breach Report 2024. URL: https://www.ibm.com/reports/data-breach (дата звернення: 22.11.2025).

28. OECD. Digital Security Risk Management for Economic and Social Prosperity. Paris : OECD Publishing, 2015. URL: https://www.oecd.org/sti/digital-security-risk-management.htm (дата звернення: 22.11.2025)

29. ISACA. COBIT 2019 Framework: Governance and Management Objectives. URL: https://www.isaca.org/resources/cobit (дата звернення: 22.11.2025).