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: “МЕТОДИ ОЦІНКИ ТА МІНІМІЗАЦІЇ РИЗИКІВ У СИСТЕМІ МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ”

на здобуття освітнього ступеня бакалавра
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

_____ Дмитро ЖЕСТКОВ
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. УБД-42

Дмитро ЖЕСТКОВ
Ім’я, ПРІЗВИЩЕ

Керівник: Іван ОПІРСЬКИЙ
Д.т.н., професор Ім’я, ПРІЗВИЩЕ

Рецензент: _____
_____ 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 бакалавр

Спеціальність 125 Кібербезпека

Освітня програма Управління інформаційною та кібернетичною безпекою

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

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Жесткову Дмитру Ігоровичу
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “Методи оцінки та мінімізації ризиків у системі менеджменту інформаційної безпеки”,
керівник кваліфікаційної роботи ОПІРСЬКИЙ Іван, д.т.н., професор
(ПРІЗВИЩЕ, Ім’я, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від “24“ лютого 2025 р. №56.

2. Строк подання кваліфікаційної роботи “12” травня 2025р.

3. Вихідні дані до кваліфікаційної роботи: *інформаційні ресурси організації, що потребують захисту; методи та підходи до оцінки і мінімізації ризиків; наукова та технічна література, експлуатаційна документація, нормативні документи, міжнародні стандарти.*

4. Перелік питань, які мають бути розроблені:
4.1. Дослідити сутність проблеми управління ризиками в системі менеджменту інформаційної безпеки.
4.2. Проаналізувати основні підходи до оцінки ризиків в інформаційній безпеці.
4.3. Проаналізувати сучасні методи та інструменти мінімізації ризиків.
4.4. Розробити рекомендації щодо вдосконалення методів оцінки та мінімізації ризиків у системі менеджменту інформаційної безпеки

5. Перелік ілюстративного матеріалу: *презентація PowerPoint*

6. Дата видачі завдання “5“ березня 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	18.03.2025	
2.	Збір та аналіз літератури.	29.03.2025	
3.	Аналіз методів та засобів оцінки ризиків у системі менеджменту інформаційної безпеки.	08.04.2025	
4.	Практична реалізація моделі управління ризиками у системі менеджменту інформаційної безпеки.	15.04.2025	
5.	Розроблення рекомендацій щодо застосування методів оцінки та мінімізації ризиків.	22.04.2025	
6.	Формулювання висновків за результатами проведеного дослідження.	29.04.2025	
7.	Оформлення роботи.	06.05.2025	
8.	Оформлення презентації.	09.05.2025	
9.	Отримання рецензії на роботу.	12.06.2025	
10.	Захист в ДЕК.	__.06.2025	

Здобувач вищої освіти _____ Дмитро ЖЕСТКОВ
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Іван ОПІРСЬКИЙ
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

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

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

Направляється здобувач Жестков Д.І. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: "Методи оцінки та мінімізації ризиків у системі менеджменту інформаційної безпеки"

Кваліфікаційна робота і рецензія додаються.

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

Висновок керівника кваліфікаційної роботи

Здобувач ЖЕСТКОВ Дмитро у кваліфікаційній роботі дослідив методи оцінки та мінімізації ризиків у системі менеджменту інформаційної безпеки, проаналізував ключові підходи до ідентифікації, аналізу та оцінки інформаційних ризиків, розглянув їхню структуру та класифікацію. Вивчив сучасні методики управління ризиками, зокрема відповідно до міжнародних стандартів ISO/IEC 27005, ISO 31000, NIST SP 800-30, а також розробив практичні рекомендації щодо вибору оптимальних стратегій мінімізації ризиків з урахуванням актуальних кіберзагроз.

Жестков Д.І. продемонстрував належний рівень обізнаності у сфері інформаційної безпеки, уміння застосовувати як кількісні, так і якісні методи оцінки ризиків, виявив системний підхід до розв'язання поставлених завдань. Результати дослідження апробовані на конференції.

Все це дозволяє оцінити кваліфікаційну роботу здобувача ЖЕСТКОВА Дмитра на оцінку "_____" та присвоїти йому кваліфікацію бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Керівник кваліфікаційної роботи _____ Іван ОПІРСЬКИЙ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"____" _____ 2025 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Жестков Д.І. допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедри
управління кібербезпекою та
захистом інформації _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну бакалаврську роботу

здобувача вищої освіти ЖЕСТКОВА Дмитра
на тему “Методи оцінки та мінімізації ризиків у системі менеджменту інформаційної безпеки”

Актуальність. У сучасному світі питання інформаційної безпеки набувають критичного значення, оскільки кібератаки, витоки даних та інші загрози можуть призвести до значних фінансових втрат, репутаційних ризиків та навіть правових наслідків для організацій. Система менеджменту інформаційної безпеки є фундаментальною складовою стратегічного управління безпекою даних, адже вона допомагає ідентифікувати, оцінювати та контролювати ризики, пов’язані з конфіденційністю, цілісністю та доступністю інформації.

Позитивні сторони.

1. У роботі досліджено сучасні підходи до оцінки та мінімізації ризиків у системі менеджменту інформаційної безпеки, розглянуто класифікацію ризиків, їх структуру та механізми впливу на захищеність інформаційних ресурсів.
2. Кваліфікаційна робота оформлена відповідно до чинних вимог. Структура роботи логічно побудована, матеріал викладено послідовно та аргументовано. Основні результати дослідження наочно представлено у вигляді таблиць, рисунків та схем.
3. Автор опрацював велику кількість джерел, серед яких як сучасні зарубіжні, так і вітчизняні публікації, нормативні документи та міжнародні стандарти. Це дозволило здійснити глибокий аналіз існуючих методів управління ризиками та сформулювати обґрунтовані висновки.
4. У результаті дослідження запропоновано рекомендації щодо вибору оптимальних методів оцінки ризиків та розроблено адаптивні стратегії мінімізації ризиків, що враховують сучасні кіберзагрози та потреби підприємств у сфері інформаційної безпеки.

Недоліки.

Доцільно було б більш глибоко розглянути практичну реалізацію комбінованих методів оцінки ризиків (поєднання кількісних та якісних підходів) та подати більш детальний огляд застосування сучасних технологій управління безпекою (наприклад, SIEM, EDR, XDR) у реальних сценаріях.

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

Висновок: Кваліфікаційна робота виконана на належному науково-методичному рівні та заслуговує оцінки “_____”, а здобувач ЖЕСТКОВ Дмитро заслуговує присвоєння кваліфікації бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Рецензент:
_____ _____ _____
підпис Ім’я, ПРІЗВИЩЕ

РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню методів оцінки ризиків інформаційної безпеки та підвищенню ефективності заходів мінімізації їх впливу в системі менеджменту інформаційної безпеки. Робота складається зі вступу, трьох розділів, що містять 22 рисунки, висновків і списку використаних джерел із 60 найменувань. Загальний обсяг роботи становить 81 аркуш, з яких 8 аркушів займають перелік умовних позначень і скорочень та список використаних джерел.

Метою роботи є дослідження методів оцінки ризиків та розробка рекомендацій щодо підвищення ефективності заходів мінімізації їх впливу в системі менеджменту інформаційної безпеки.

Об'єктом дослідження є процеси управління ризиками в рамках системи менеджменту інформаційної безпеки.

Предмет дослідження – підходи до оцінювання ризиків та способи мінімізації їхнього впливу на стабільність функціонування інформаційної системи підприємства.

Методи дослідження. Для реалізації поставлених завдань у роботі використано аналіз літературних джерел і нормативних документів, якісні та кількісні методи оцінювання ризиків, емпіричні підходи на основі вивчення реальних кейсів, методи моделювання потенційних загроз, а також порівняльний аналіз ефективності різних підходів до управління ризиками в галузі інформаційної безпеки.

Галузь використання. Запропоновані рішення можуть бути використані при побудові та вдосконаленні систем управління інформаційною безпекою підприємств у сфері кібербезпеки.

Ключові слова: ІНФОРМАЦІЙНА БЕЗПЕКА, УПРАВЛІННЯ РИЗИКАМИ, КІБЕРБЕЗПЕКА, ОЦІНКА РИЗИКІВ, СИСТЕМА МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, АНАЛІЗ ЗАГРОЗ ТА ВРАЗЛИВОСТЕЙ, ПОЛІТИКА БЕЗПЕКИ.

ABSTRACT

The qualification work is devoted to the study of methods for assessing information security risks and increasing the effectiveness of measures to minimize their impact in the information security management system. The work consists of an introduction, three chapters containing 22 figures, conclusions and a list of references of 60 titles. The total volume of the work is 81 pages, of which 8 pages are occupied by the list of symbols and abbreviations and the list of references.

The purpose of the study is to investigate risk assessment methods and develop recommendations for improving the effectiveness of measures to minimize their impact in the information security management system.

The object the study is the risk management processes within the information security management system.

The subject of the study is approaches to risk assessment and ways to minimize their impact on the stability of the enterprise information system.

Research methods. To accomplish the tasks set in the work, the analysis of literary sources and regulatory documents, qualitative and quantitative methods of risk assessment, empirical approaches based on the study of real cases, methods of modeling potential threats, as well as a comparative analysis of the effectiveness of various approaches to risk management in the field of information security were used.

Field of application. The proposed solutions can be used in the construction and improvement of enterprise information security management systems in the field of cybersecurity.

Keywords: INFORMATION SECURITY, RISK MANAGEMENT, CYBERSECURITY, RISK ASSESSMENT, INFORMATION SECURITY MANAGEMENT SYSTEM, THREAT AND VULNERABILITY ANALYSIS, SECURITY POLICY.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

ІБ	інформаційна безпека
СМІБ	система менеджменту інформаційної безпеки
GDPR	General Data Protection Regulation (Загальний регламент захисту даних ЄС)
IT	інформаційні технології
SIEM	Security Information and Event Management (система управління інформаційною безпекою і подіями)
SOC	Security Operations Center (центр операцій безпеки)
VPN	Virtual Private Network (віртуальна приватна мережа)
SLA	Service Level Agreement (угода про рівень послуг)
DLP	Data Loss Prevention (система запобігання витоку даних)
ALU	Arithmetic Logic Unit (арифметико-логічний пристрій)
CPU	Central Processing Unit (центральний процесор)
GPGPU	General-Purpose computing on Graphics Processing Units (загального призначення обчислення на GPU)
MIMD	Multiple Instruction, Multiple Data (множинні інструкції, множинні дані)
URL	Uniform Resource Locator (уніфікований локатор ресурсу)
HTML	HyperText Markup Language (мова розмітки гіпертексту)

ВСТУП

Актуальність дослідження. У сучасному цифровому світі питання інформаційної безпеки набувають критичного значення, оскільки кібератаки, витоки даних та інші загрози можуть призвести до значних фінансових втрат, репутаційних ризиків та навіть правових наслідків для організацій. Система менеджменту інформаційної безпеки (СМІБ) є фундаментальною складовою стратегічного управління безпекою даних, адже вона допомагає ідентифікувати, оцінювати та контролювати ризики, пов’язані з конфіденційністю, цілісністю та доступністю інформації. Одним із ключових аспектів ефективного функціонування СМІБ є застосування методів оцінки ризиків, що дозволяє компаніям своєчасно виявляти вразливості та розробляти механізми мінімізації загроз. Стандарти, такі як ISO/IEC 27001, NIST, COBIT, забезпечують організаціям рекомендації щодо ефективного управління ризиками, однак кожна організація повинна адаптувати ці підходи відповідно до своїх потреб і специфіки діяльності.

Оцінка та мінімізація ризиків в інформаційній безпеці є безперервним процесом, що вимагає застосування як класичних методів аналізу (матриця ризиків, аналіз FMEA, DELPHI), так і сучасних технологій, таких як машинне навчання, штучний інтелект та автоматизовані системи моніторингу загроз. З розвитком хмарних технологій, Інтернету речей (IoT) та великих даних (Big Data) зростає кількість потенційних векторів атак, що вимагає вдосконалення підходів до оцінки ризиків та розробки адаптивних методів їхньої мінімізації. Важливість даної теми обумовлена також зростаючими законодавчими вимогами щодо захисту інформації, такими як GDPR та Закон України "Про захист інформації в інформаційно-комунікаційних системах", що вимагає від компаній впровадження ефективних стратегій управління ризиками. Саме тому дослідження методів оцінки та мінімізації ризиків у СМІБ є актуальним і необхідним для забезпечення стійкості та безпеки сучасних інформаційних систем.

Метою роботи є дослідження методів оцінки ризиків та розробка рекомендацій щодо підвищення ефективності заходів мінімізації їх впливу в системі менеджменту інформаційної безпеки.

Об'єктом дослідження виступають процеси управління ризиками в рамках системи менеджменту інформаційної безпеки.

Предмет дослідження – підходи до оцінювання ризиків та способи мінімізації їхнього впливу на стабільність функціонування інформаційної системи підприємства.

Для досягнення цієї мети в роботі необхідно виконати наступні **завдання:**

1. Дослідити сутність проблеми управління ризиками в системі менеджменту інформаційної безпеки;
2. Проаналізувати основні підходи до оцінки ризиків в інформаційній безпеці;
3. Проаналізувати сучасні методи та інструменти мінімізації ризиків;
4. Розробити рекомендації щодо вдосконалення методів оцінки та мінімізації ризиків у системі менеджменту інформаційної безпеки.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використано аналіз літературних джерел та нормативних документів – вивчення міжнародних стандартів (ISO/IEC 27001, NIST, COBIT) та сучасних наукових підходів до управління ризиками; методи якісного та кількісного оцінювання ризиків – аналіз матриці ризиків, методу FMEA (аналіз виду та наслідків відмов), методів DELPHI та аналізу дерева відмов; емпіричні методи – вивчення реальних кейсів впровадження систем менеджменту інформаційної безпеки у компаніях та організаціях; методи моделювання – використання програмних засобів для моделювання загроз та оцінки потенційних ризиків; порівняльний аналіз – зіставлення ефективності різних методів управління ризиками в інформаційній безпеці.

Практичне значення одержаних результатів. Розроблено рекомендації щодо застосування методів оцінки та мінімізації ризиків у системі менеджменту інформаційної безпеки, що дозволяє організаціям ефективніше ідентифікувати,

аналізувати та контролювати інформаційні загрози. Впроваджені підходи сприятимуть підвищенню рівня інформаційної безпеки та зниженню ймовірності реалізації ризиків, пов’язаних із витоками даних, кіберзагрозами та внутрішніми загрозами.

Результати дослідження можуть бути використані фахівцями з кібербезпеки, IT-менеджерами та адміністраторами безпеки для вдосконалення системи управління ризиками в корпоративному середовищі. Розроблені методичні рекомендації допоможуть підприємствам впроваджувати стандартизовані підходи (ISO/IEC 27001, NIST, COBIT) та адаптувати їх до специфічних потреб бізнесу. Крім того, отримані результати можуть бути використані в навчальному процесі для підготовки спеціалістів у сфері інформаційної безпеки та кіберзахисту.

Апробація результатів кваліфікаційної роботи відбулася на Всеукраїнській науково-практичній конференції “Стратегії кіберстійкості: управління ризиками та безперервність бізнесу” 27 лютого 2025 року.

Розділ 1 ТЕОРЕТИЧНІ ЗАСАДИ УПРАВЛІННЯ РИЗИКАМИ У СИСТЕМАХ МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1 Визначення основних компонентів і структури системи менеджменту інформаційної безпеки

Ефективне управління ризиками в СМІБ базується на чітко визначених концептуальних засадах, що забезпечують комплексний підхід до захисту інформаційних активів. Оскільки процеси ідентифікації, оцінки та мінімізації ризиків неможливі без розуміння фундаментальних характеристик ІБ, доцільним є розгляд її сутності, ключових цілей та принципів функціонування. Це створює методологічне підґрунтя для подальшого аналізу механізмів управління ризиками та визначення ефективних стратегій їх мінімізації в межах СМІБ.

ІБ є фундаментальною складовою стійкості сучасних ІС та критично важливим аспектом управління ризиками в організаціях. Вона забезпечує захист інформаційних активів від НСД, модифікації, знищення або витоку, що може призвести до значних фінансових, операційних і репутаційних втрат. В умовах глобальної цифровізації та зростання складності кіберзагроз ІБ перетворюється з локального завдання технічного захисту на стратегічний напрямок управління ризиками, що вимагає системного підходу та інтеграції з бізнес-процесами організації [1].

З концептуальної точки зору ІБ визначається через три ключові характеристики: конфіденційність, цілісність та доступність (CIA-тріада). Конфіденційність передбачає запобігання НСД до інформації, забезпечуючи її доступність лише для авторизованих суб’єктів. Цілісність гарантує збереження достовірності, точності та узгодженості даних у процесі їхнього зберігання, обробки та передачі. Доступність означає безперервну можливість використання інформації та ІС уповноваженими користувачами в межах встановлених політик і процедур. Взаємозв’язок цих характеристик формує основу забезпечення безпеки даних та інформаційної інфраструктури в цілому.

Цілі ІБ спрямовані на створення та підтримку захищеного інформаційного

середовища, здатного протидіяти актуальним загрозам. До основних завдань належать запобігання компрометації інформаційних активів, забезпечення відповідності нормативно-правовим вимогам, зниження ймовірності реалізації загроз та мінімізація потенційних наслідків інцидентів безпеки. Важливою складовою є також забезпечення безперервності бізнес-процесів, що передбачає розробку та реалізацію стратегій резервування, відновлення після інцидентів і адаптивного реагування на змінні загрози [1,2].

Таким чином, ІБ є багаторівневим процесом, що поєднує концептуальні, організаційні та технічні аспекти. Її ефективне забезпечення потребує системного підходу до управління ризиками, дотримання принципів безперервного вдосконалення та інтеграції механізмів захисту у загальну структуру управління інформаційними ресурсами організації.

Система менеджменту інформаційної безпеки (СМІБ) – це комплекс взаємопов’язаних елементів управління, що охоплює політики, процедури, організаційну структуру, процеси, ресурси та технології, спрямовані на забезпечення конфіденційності, цілісності та доступності інформаційних активів (табл. 1.1).

Таблиця 1.1

Основні компоненти СМІБ

Компонент	**Опис**
Політика	Загальні принципи, цілі та підходи до управління ІБ в організації.
Організаційна структура	Визначення відповідальності, повноважень та ролей осіб, що беруть участь в управлінні ІБ.
Процеси	Сукупність дій, що забезпечують реалізацію політики ІБ.
Технології	Технічні засоби та програмне забезпечення, що використовуються для захисту інформаційних активів.
Процедури	Документовані методи виконання операцій чи завдань, пов’язаних з ІБ.
Ресурси	Кадрові, фінансові, технічні та інформаційні засоби, необхідні для впровадження СМІБ.

СМІБ забезпечує розробку, впровадження, моніторинг, періодичний перегляд і вдосконалення заходів з ІБ відповідно до вимог міжнародних стандартів (зокрема ISO/IEC 27001), забезпечуючи таким чином системний підхід до зменшення інформаційних ризиків, відповідність нормативним вимогам і безперервний контроль за станом ІБ в організації [3].

Життєвий цикл СМІБ базується на моделі PDCA (Plan-Do-Check-Act), яка забезпечує безперервне вдосконалення системи, і включає в себе етапи, представлені в таблиці 1.2.

Таблиця 1.2

Завдання, необхідні для функціонування СУІБ в рамках циклу PDCA

Етап	Завдання
PLAN (Планування)	Визначення політики ІБ, цілей, процесів та процедур, необхідних для управління ризиками ІБ. Ідентифікація активів, загроз і вразливостей. Оцінка ризиків та вибір заходів контролю.
DO (Виконання)	Реалізація політики, процедур, заходів захисту. Проведення навчань, впровадження технічних рішень та організаційних заходів.
CHECK (Перевірка)	Оцінювання результатів функціонування СУІБ. Проведення внутрішніх аудитів, моніторинг інцидентів, аналіз відповідності цілям безпеки.
ACT (Поліпшення)	Коригування та вдосконалення СУІБ на основі результатів перевірок. Розробка та впровадження коригувальних і попереджувальних дій.

Для ефективного функціонування СМІБ необхідні чітко визначені політики ІБ, які визначають стратегічні та тактичні підходи до захисту інформації, встановлюючи загальні правила та регламенти управління ІБ і слугують основою для розробки процедур і впровадження технічних заходів захисту. Основні види політик ІБ зведені в таблиці 1.3 [4].

Таблиця 1.3

Типові завдання тематичних політик ІБ

Вид політики	Призначення
Загальна політика ІБ	1. Опис стратегічних цілей та принципів управління ІБ в організації. 2. Визначення підходів до управління ризиками. 3. Встановлення відповідальності керівництва за безпеку.
Політика контролю доступу	1. Визначення рівнів доступу до інформаційних активів. 2. Управління правами користувачів. 3. Регламентування автентифікації та авторизації.
Політика безпеки мереж і систем	1. Забезпечення захисту мережі від несанкціонованого доступу. 2. Впровадження засобів міжмережевого екранування. 3. Використання антивірусного ПЗ та систем виявлення вторгнень.
Політика з резервного копіювання	1. Регламентування періодичності створення резервних копій. 2. Визначення способів та місць зберігання копій. 3. Перевірка відновлення даних із резервних копій.
Політика реагування на інциденти	1. Визначення порядку дій у разі інцидентів ІБ. 2. Призначення відповідальних осіб. 3. Забезпечення реєстрації та аналізу інцидентів для вдосконалення.
Політика управління активами	1. Облік та класифікація інформаційних активів. 2. Визначення відповідальних за активи. 3. Захист активів на всіх етапах їхнього життєвого циклу.

Процеси управління ІБ, в свою чергу, забезпечують реалізацію політик і є основним механізмом підтримки ефективності СМІБ (табл. 1.4).

Таблиця 1.4

Ключові процеси ІБ, що забезпечують підтримку ефективності СМІБ

Процес	**Завдання**
Ідентифікація та оцінка ризиків	1. Виявлення загроз, вразливостей та наслідків порушень ІБ. 2. Визначення рівня ризику. 3. Формування звітів про ризики для прийняття рішень.
Управління ризиками	1. Розробка плану заходів для зменшення ризиків. 2. Впровадження контролів для мінімізації ризиків. 3. Моніторинг залишкових ризиків.
Управління інцидентами	1. Виявлення, реєстрація та класифікація інцидентів ІБ. 2. Реагування на інциденти та мінімізація шкоди. 3. Аналіз та вдосконалення заходів реагування.
Контроль доступу	1. Розмежування прав доступу користувачів. 2. Управління обліковими записами. 3. Періодична перевірка та ревізія доступів.
Розробка політик та процедур	1. Формування нормативної бази ІБ. 2. Регламентування діяльності працівників у сфері ІБ. 3. Перегляд та актуалізація політик.
Управління інфраструктурою ІБ	1. Забезпечення фізичного та логічного захисту активів. 2. Підтримка антивірусного захисту, брандмауерів та IDS/IPS. 3. Оновлення програмного забезпечення.

Для реалізації зазначених політик і процесів ІБ необхідні відповідні технічні, людські та фінансові ресурси (табл. 1.5).

Таблиця 1.5

Ресурси, необхідні для підтримки ефективності СМІБ

Тип ресурсів	**Приклади активів**
Технічні	1. Сервери безпеки (IDS/IPS, проксі, firewall). 2. Мережеве обладнання з підтримкою захисту (маршрутизатори з ACL). 3. Робочі станції з антивірусним ПЗ. 4. Засоби шифрування і VPN. 5. Системи резервного копіювання та відновлення.
Людські	1. Адміністратори ІБ. 2. Інженери з мережевої безпеки. 3. Користувачі, які пройшли навчання з основ ІБ.
Документація	1. Політики та процедури ІБ. 2. Документація з управління ризиками. 3. Звіти з аудиту безпеки.

На рисунку 1.1 представлено загальну структуру СМІБ, яка побудована на основі моделі постійного вдосконалення PDCA (Plan-Do-Check-Act). Схема

відображає ключові компоненти, що забезпечують комплексний підхід до управління ІБ в організації [5].

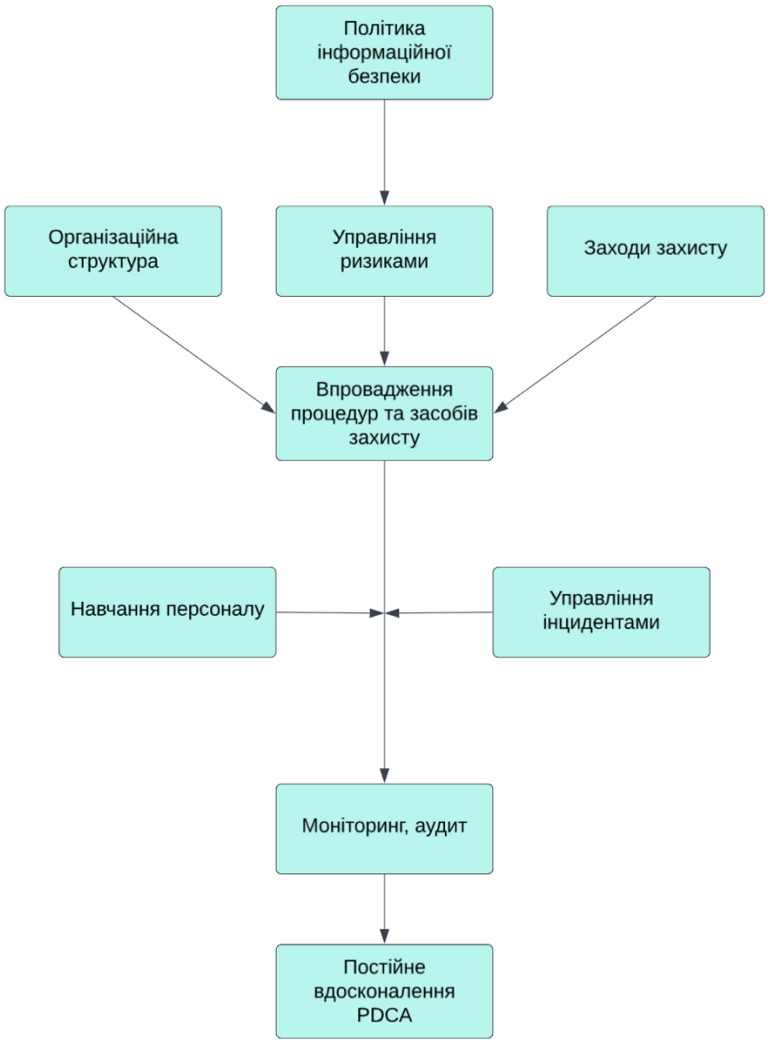

Рис. 1.1. Структура системи менеджменту інформаційної безпеки

Дана структура включає такі взаємопов’язані елементи: політика ІБ, організаційна структура, управління ризиками, заходи захисту, впровадження процедур, навчання персоналу, управління інцидентами, моніторинг і аудит, а також постійне вдосконалення. Всі ці складові інтегруються в єдиний цикл PDCA, що забезпечує безперервне покращення процесів ІБ в організації [5,6].

1.2 Визначення класифікаційних ознак ризиків у контексті інформаційної безпеки

Ризик в ІБ – це ймовірність реалізації загрози, яка здатна завдати шкоди інформаційним активам організації, а також потенційний розмір таких наслідків. Управління ризиками є ключовим елементом функціонування СМІБ, оскільки дозволяє своєчасно виявляти можливі загрози та визначати ефективні заходи їх мінімізації.

Структура ризику в ІБ традиційно включає три основні складові [7]:

1. Загроза – потенційне джерело небажаного впливу, яке може призвести до порушення конфіденційності, цілісності або доступності інформації.
2. Вразливість – слабке місце в системі, що створює можливість для реалізації загрози.
3. Наслідки – негативний результат, що виникає у випадку реалізації загрози через наявну вразливість, що може виражатися у фінансових збитках, порушенні регуляторних вимог, втраті репутації або зниженні операційної ефективності.

Управління ризиками ІБ базується на аналізі та систематизації загроз, які можуть впливати на інформаційні активи організації. Для цього використовується класифікація ризиків за різними ознаками, що дозволяє визначити їхню природу, джерела виникнення та потенційні наслідки. Класифікаційні ознаки ризиків допомагають оцінити рівень загроз, встановити пріоритетність заходів захисту та ефективно розподілити ресурси для їхньої нейтралізації.

Основними класифікаційними ознаками ризиків в ІБ є джерело виникнення, характер впливу, рівень критичності, масштаб загрози та методи управління ризиками (табл. 1.6).

Таблиця 1.6

Класифікація ризиків інформаційної безпеки

Ознака класифікації	**Категорії**
За джерелом	Внутрішні (пов'язані з діяльністю персоналу, процесами всередині організації), Зовнішні (пов'язані з діями сторонніх осіб, кіберзлочинців, постачальників, партнерів)
За природою виникнення	Технічні (відмови технічних засобів, збої в ПЗ), Організаційні (помилки в політиках, процедурах), Людські (помилки персоналу, зловмисні дії співробітників), Фізичні (стихійні лиха, пожежі, крадіжки обладнання)
За наслідками	Фінансові (прямі збитки, штрафи), Репутаційні (втрата довіри клієнтів та партнерів), Регуляторні (невиконання вимог законодавства та стандартів), Операційні (збої у виробничих та бізнес-процесах)
За ймовірністю виникнення	Високий, середній, низький
За критичністю	Критичний, Суттєвий, Незначний

Перша важлива ознака – джерело виникнення ризику, що дозволяє розподілити загрози на внутрішні та зовнішні. Внутрішні ризики виникають в межах організації та пов'язані з людським фактором, помилками персоналу, неналежним адмініструванням або інсайдерськими атаками. Зовнішні ризики спричинені загрозами поза організацією, такими як кібератаки, шкідливе програмне забезпечення, соціальна інженерія або природні катастрофи [9].

Другою ознакою є характер впливу ризику на інформаційну систему. Виходячи з цього критерію, ризики поділяються за впливом на конфіденційність, цілісність та доступність інформації. Конфіденційність може бути порушена через витоки даних або зловмисні атаки. Порушення цілісності відбувається, коли інформація змінюється або пошкоджується несанкціонованим чином. Доступність системи може бути порушена через DDoS-атаки, відмови обладнання або внутрішні технічні збої.

Ще однією важливою класифікаційною ознакою є рівень критичності ризику, який визначається залежно від ймовірності виникнення та масштабу його впливу на організацію. Виділяють високі, середні та низькі ризики. Високий рівень ризику означає значний вплив на функціонування організації, що може призвести до фінансових втрат або компрометації інформації. Середні ризики мають менший вплив і можуть бути контрольовані за допомогою політик

безпеки та технічних засобів. Низькі ризики, як правило, мають мінімальні наслідки, тому можуть бути прийняті без додаткових заходів захисту [10].

Масштаб загрози є ще однією класифікаційною ознакою, що поділяє ризики на локальні та глобальні. Локальні ризики впливають на окремі системи або підрозділи організації, наприклад, зараження одного комп'ютера вірусом або помилка конфігурації сервера. Глобальні ризики мають ширший вплив, який може зачіпати всю організацію або навіть її зовнішніх партнерів, як у випадку масових атак або масштабних витоків даних.

Останньою ключовою ознакою є методи управління ризиками, які визначають можливі стратегії реагування. До основних методів відносяться уникнення ризику, що передбачає відмову від процесів, які можуть спричинити загрозу; зниження ризику, що включає впровадження технічних і організаційних заходів безпеки; передача ризику, коли відповідальність за ризик передається третім сторонам, наприклад, через страхування або аутсорсинг; та прийняття ризику, коли організація погоджується з можливими наслідками, оскільки їхня ймовірність або вплив є незначними [11].

1.3 Аналіз нормативно-правових вимог і стандартів у сфері управління ризиками інформаційної безпеки

Система управління ризиками в ІБ базується на дотриманні міжнародних та національних стандартів, які регламентують принципи, підходи та методи оцінки і мінімізації ризиків. Основним стандартом, який безпосередньо стосується управління ризиками ІБ, є ДСТУ ISO/IEC 27005:2023 «Інформаційна безпека, кібербезпека та захист конфіденційності. Настанова керування ризиками інформаційної безпеки» (ідентичний міжнародному стандарту ISO/IEC 27005:2022). Цей документ визначає процеси управління ризиками ІБ, включаючи їх ідентифікацію, аналіз, оцінку та обробку, а також моніторинг і перегляд.

Стандарт ДСТУ ISO/IEC 27001 регламентує загальні вимоги до СМІБ, при

цьому ризик-орієнтований підхід виступає ключовим елементом цієї системи. ISO/IEC 27001 передбачає, що заходи захисту мають бути визначені на основі результатів оцінки ризиків, що забезпечує їх релевантність та ефективність [11-13].

Слід також відзначити серію стандартів ISO 31000, яка охоплює загальні принципи управління ризиками для всіх типів бізнес-ризиків, включаючи інформаційні. Ця серія є основою для розуміння концепції управління ризиками в більш широкому корпоративному контексті. Додатково в роботі застосовуються рекомендації з методології управління ризиками, викладені в NIST SP 800-30 «Guide for Conducting Risk Assessments», яка містить практичні рекомендації щодо проведення оцінки ризиків ІБ, а також зазначає процедури ідентифікації активів, загроз, вразливостей та потенційних наслідків.

До важливих джерел можна віднести також COBIT (Control Objectives for Information and Related Technologies), який містить окремі положення щодо управління ризиками в рамках загального IT-менеджменту, однак його застосування є доцільним лише в контексті інтеграції з іншими системами управління.

У національному законодавстві України питання управління ризиками в ІБ частково регулюються такими актами, як Закон України «Про основні засади забезпечення кібербезпеки України», а також підзаконними актами, що стосуються критичної інфраструктури та захисту персональних даних. У цьому контексті, відповідно до зазначених нормативів, управління ризиками розглядається не як ізольований процес, а як складова загальної системи кібербезпеки, що включає моніторинг, виявлення інцидентів та реагування на них.

У таблиці 1.7 представлено основні міжнародні стандарти у сфері ІБ та управління ризиками, які відіграють ключову роль у формуванні ефективної СМІБ. Вони визначають підходи до оцінки ризиків, розробки політик, організації процесів безпеки, а також забезпечують правові та методичні рамки для впровадження комплексного захисту інформаційних активів [14].

Таблиця 1.7

Порівняння міжнародних стандартів управління ризиками ІБ

Стандарт	**Тип документа**	**Основне призначення**	**Основні компоненти**	**Сфера застосування**	**Наявність сертифікації**
ISO/IEC 27001	Міжнародний стандарт управління ІБ	Розробка, впровадження та управління СМІБ	Політики безпеки, управління ризиками, контроль доступу, реагування на інциденти	Організації всіх типів, які впроваджують СМІБ	Так, передбачена
ISO/IEC 27005	Міжнародний стандарт управління ризиками в СМІБ	Методичні вказівки щодо управління ризиками у СМІБ	Ідентифікація ризиків, оцінка, аналіз, обробка, моніторинг	Організації, що працюють згідно ISO/IEC 27001	Ні, лише рекомендації
NIST SP 800-30	Методологія оцінки ризиків у сфері кібербезпеки	Оцінка та управління ризиками в ІБ	Ідентифікація активів, загроз, уразливостей, оцінка ризиків, розробка заходів	Організації, що оцінюють ризики ІБ	Ні, методичні рекомендації
COBIT	Модель управління IT-ресурсами	Контроль і управління IT та ІБ відповідно до бізнес-цілей	Контрольні механізми, відповідність цілям, управління IT-інфраструктурою	Бізнес, що використовує IT-ресурси	Ні, рамкова модель
GDPR	Регламент захисту персональних даних	Захист персональних даних, прав користувачів та регулювання обробки	Згода, права, заходи безпеки, звітність про інциденти	Будь-які компанії, що обробляють персональні дані громадян ЄС	Ні, обов'язковий регламент без сертифікації
ISO 31000	Міжнародний стандарт з управління ризиками	Загальні принципи управління ризиками для будь-якої організації	Принципи, структура, процес управління ризиками	Організації будь-якої галузі або типу	Ні, керівний документ

1.4 Аналіз сучасних підходів до ідентифікації, аналізу та оцінки ризиків у системах менеджменту інформаційної безпеки

У сучасній практиці побудови СМІБ значну увагу приділяють аналізу ризиків як базовому елементу прийняття рішень щодо впровадження заходів захисту. Міжнародні стандарти з управління ІБ пропонують різні методології

оцінки ризиків, які відрізняються за глибиною аналізу, орієнтацією на технічні чи організаційні аспекти, а також рівнем деталізації процедур [14,15]. Основні характеристики відповідних нормативно-методичних документів наведено в таблиці 1.8.

Таблиця 1.8

Порівняльна характеристика методів оцінки ризиків

Метод	**Тип оцінки**	**Переваги**	**Недоліки**
SWOT-аналіз	Якісний	Простота застосування, стратегічне бачення	Суб'єктивність, немає точного кількісного результату
Сценарний аналіз	Якісно-кількісний	Аналіз декількох варіантів розвитку подій	Складність формування сценаріїв, трудомісткість
Аналіз на основі подій (ETA)	Кількісний	Дозволяє побудувати можливі ланцюжки подій	Потребує великої кількості вхідних даних
Аналіз на основі відмов (FTA)	Кількісний	Виявлення критичних точок у системі	Складність побудови та підтримки дерева відмов
BIA (Business Impact Analysis)	Якісно-кількісний	Визначає критичні процеси та їх залежності	Не оцінює ймовірність подій
Монте-Карло моделювання	Кількісний	Висока точність при великій кількості даних	Високі вимоги до обчислювальних ресурсів
Математичне моделювання	Кількісний	Можливість прогнозування та оптимізації	Складність моделей, потреба в точних даних
Експертні оцінки (Delphi)	Якісний	Дозволяє отримати консенсус експертів	Суб'єктивність, залежність від компетентності експертів
Матриці ризиків (Risk Matrix)	Якісно-кількісний	Наглядність, легкість візуалізації	При спрощенні можливі похибки в оцінці
Ранжування ризиків	Якісно-кількісний	Простота застосування, швидкий результат	Обмеженість деталізації, залежить від критеріїв

На етапі ідентифікації ризиків визначаються потенційні загрози, слабкі місця та можливі наслідки їхньої реалізації. Процес ідентифікації ризиків включає аналіз як технічних, так і організаційних аспектів безпеки та передбачає використання різних методів для отримання найбільш повної картини загроз.

До основних методів ідентифікації ризиків належать експертні опитування, які базуються на колективній оцінці ризиків фахівцями в галузі кібербезпеки, та аналіз вразливостей, що використовує автоматизовані засоби

для виявлення технічних слабких місць інформаційних систем. Окрім цього, застосовуються методи аналізу сценаріїв загроз, які дозволяють моделювати можливі атаки, аналіз попередніх інцидентів, що допомагає оцінити ймовірність повторення загроз, а також аналіз бізнес-процесів, який розглядає ІБ через призму критично важливих операцій організації. Додатково використовуються функціональний аналіз активів та їхньої критичності, що дозволяє оцінити рівень ризику для конкретних інформаційних ресурсів.

Метод 1 – це метод якісної оцінки ризиків, який передбачає стратегічне бачення ситуації та експертну оцінку. Етапи застосування методу відображено на рисунку 1.2 [16].

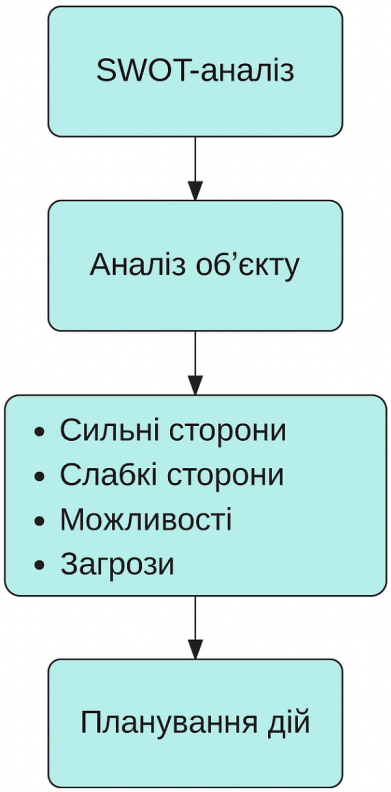

Рис. 1.2. Метод якісної оцінки

Метод 2 – це метод кількісної оцінки, що базується на аналізі подій (ETA – Event Tree Analysis). Він дозволяє моделювати можливі сценарії розвитку подій на основі початкової події, враховуючи вірогідність спрацьовування запобіжних заходів або їх відмов. Основна мета – визначити ймовірні наслідки і оцінити

рівень ризику для кожного з можливих сценаріїв. Застосування методу передбачає реалізацію заходів, як показано на рисунку 1.3 [17].

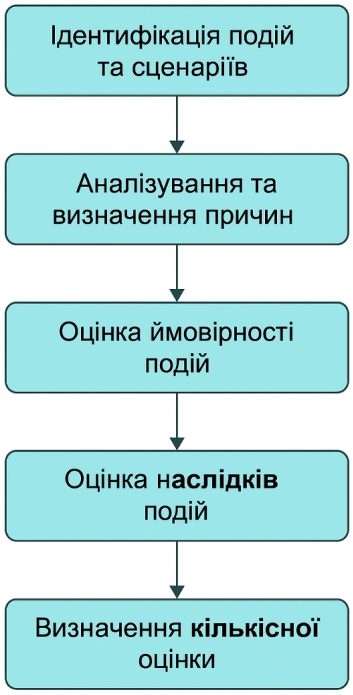

Рис. 1.3. Алгоритм кількісного аналізу ризиків методом аналізу подій (ETA)

Метод 3 – це метод якісної оцінки, який базується на ранжуванні ризиків. На рисунку 1.4 представлено алгоритм дій, що включають ідентифікацію, оцінку та порівняння ризиків для визначення пріоритетів.

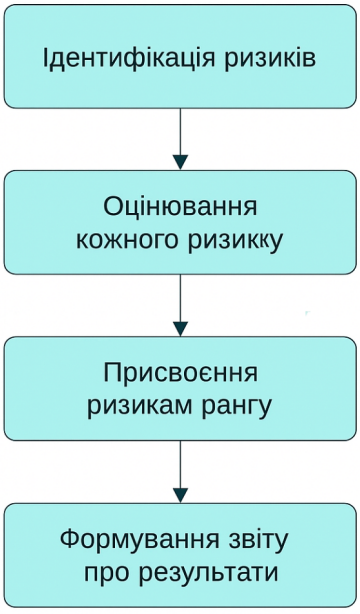

Рис. 1.4. Алгоритм якісного аналізу ризиків методом ранжування

Метод 4 – це метод якісно-кількісної оцінки ризиків, що передбачає моделювання декількох можливих сценаріїв розвитку подій з урахуванням ймовірностей та наслідків. Такий підхід дозволяє проаналізувати альтернативні шляхи виникнення інцидентів безпеки, варіанти реагування на них та вплив кожного варіанту на інформаційні активи. Застосування методу представлено на рисунку 1.5.

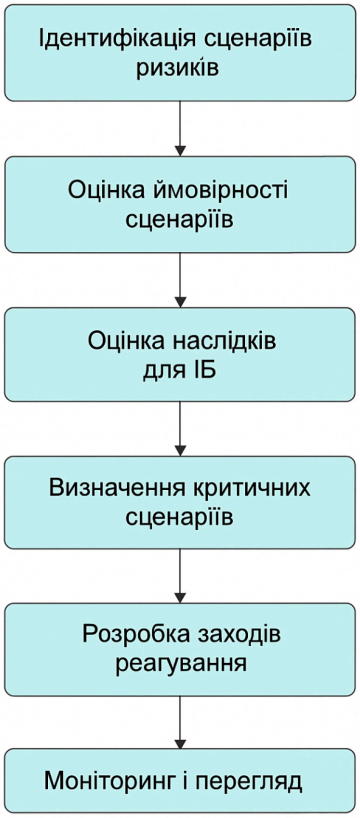

Рис. 1.5. Алгоритм аналізу сценаріїв ризику

Метод 5 – це метод Business Impact Analysis (BIA), який належить до якісно-кількісних методів оцінки ризиків. Його метою є визначення критичних бізнес-процесів, їх пріоритетності та часу відновлення у разі порушень. Метод дозволяє оцінити вплив потенційних інцидентів на функціонування організації та визначити допустимі рівні простоїв для забезпечення безперервності бізнесу. Застосування методу BIA представлено на рисунку 1.6 [16-19].

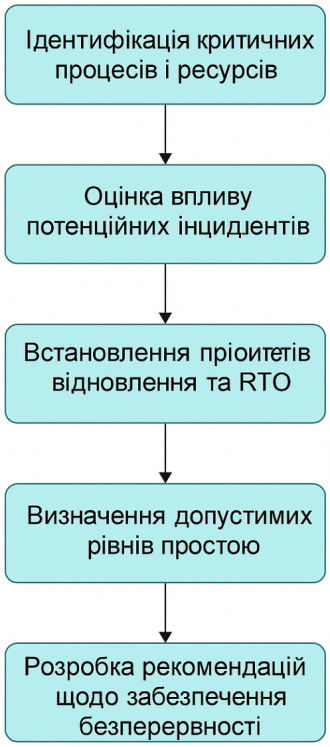

Рис. 1.6. Метод BIA

Метод 6 – це кількісний метод оцінки ризиків – метод Монте-Карло моделювання. Цей підхід передбачає використання статистичних методів для моделювання можливих результатів на основі великої кількості випадкових входів. Монте-Карло моделювання дозволяє враховувати невизначеність вхідних параметрів і дає змогу оцінити ймовірні розподіли ризиків. Метод забезпечує високу точність при достатній кількості даних, однак вимагає значних обчислювальних ресурсів та спеціалізованого програмного забезпечення. Етапи застосування методу наведено на рисунку 1.7 [19].

Метод 7 – це кількісний метод оцінки ризиків – математичне моделювання. Даний метод базується на побудові математичних моделей, які описують функціонування об'єкта з урахуванням ризик-факторів. Він дозволяє здійснювати точне прогнозування та оптимізацію процесів, що впливають на ІБ. Застосування цього методу доцільне у випадках, коли існує достатньо точних даних про систему, однак складність моделей і потреба в аналітичних ресурсах можуть ускладнювати реалізацію. Основні етапи застосування математичного моделювання відображено на рисунку 1.8 [20].

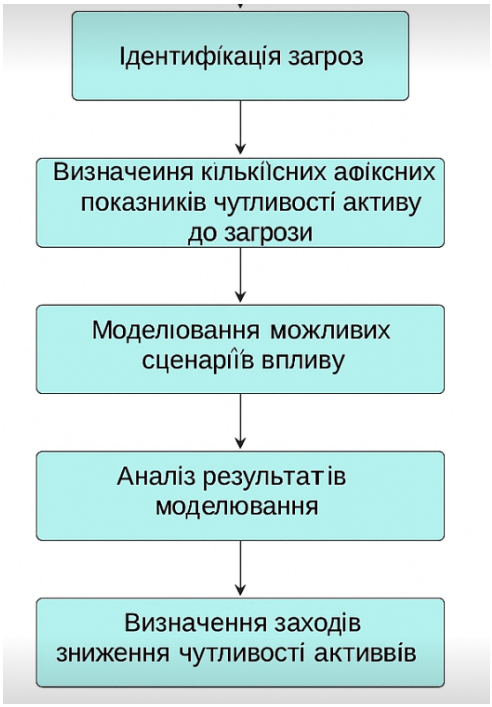

Рис. 1.7. Алгоритм Монте-Карло моделювання для оцінки ризиків

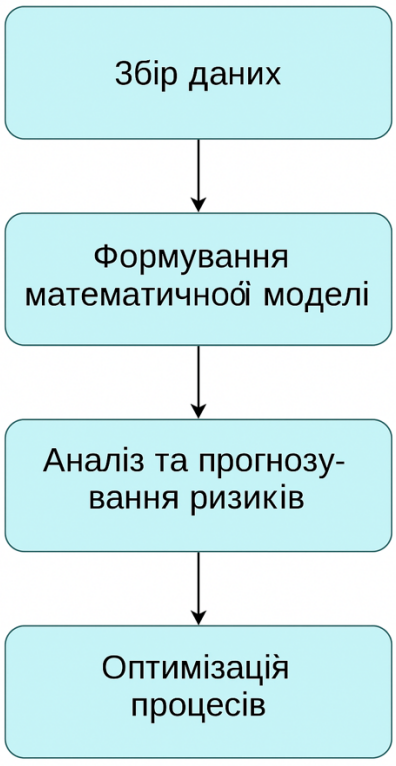

Рис. 1.8. Алгоритм застосування математичного моделювання для оцінки ризиків

Метод 8 – це метод експертних оцінок (Delphi), який належить до якісних методів оцінювання ризиків. Він базується на зборі думок експертів із подальшою обробкою та узагальненням їхніх оцінок з метою досягнення консенсусу. Особливістю методу є анонімність експертів і можливість проведення кількох раундів опитувань із зворотним зв'язком. Це дозволяє знизити вплив авторитетів і суб'єктивізму. Етапи реалізації методу подано на рисунку 1.9.

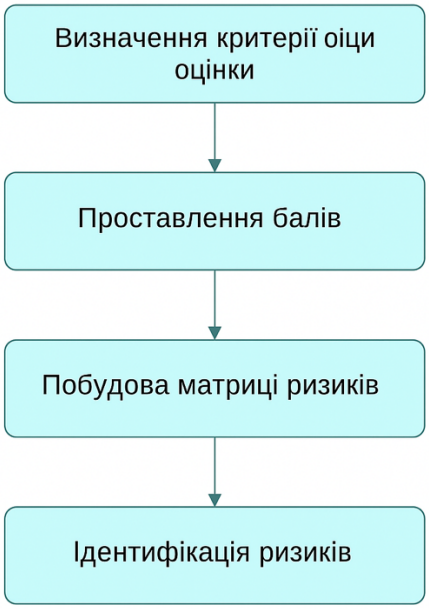

Рис. 1.9. Алгоритм методу експертних оцінок (Delphi)

Метод 9 – це метод комбінованої оцінки ризиків, що базується на побудові матриці ризиків (Risk Matrix). Цей метод поєднує якісну та кількісну інформацію для оцінювання ймовірності виникнення загроз і потенційного впливу на активи. Він дозволяє візуально представити ризики та ефективно визначати пріоритети для управління ними, що робить його корисним інструментом у прийнятті рішень щодо безпеки інформаційних систем. Етапи застосування цього методу наведено на рисунку 1.10 [20].

Метод 10 – це метод якісно-кількісної оцінки ризиків, відомий як ранжування ризиків. Його суть полягає в оцінюванні ризиків за ймовірністю їх виникнення та масштабом потенційного впливу з подальшим присвоєнням кожному ризику рейтингового значення. Це дозволяє встановити пріоритети у

впровадженні заходів безпеки та оптимально розподілити ресурси організації. Алгоритм застосування методу наведено на рисунку 1.11.

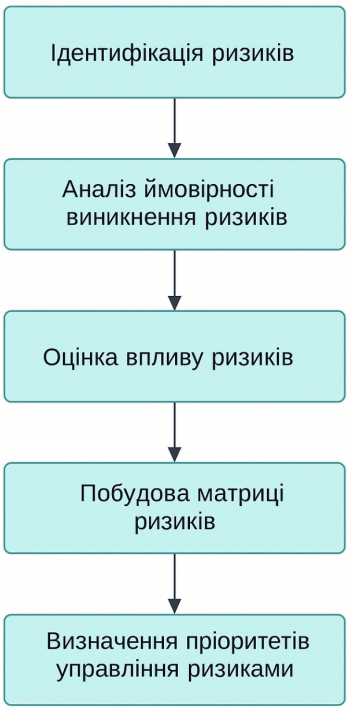

Рис. 1.10. Алгоритм методу матриці ризиків

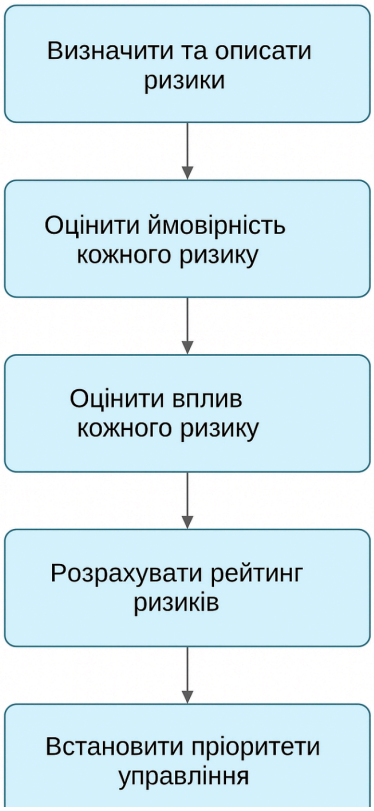

Рис. 1.11. Алгоритм методу ранжування ризиків

Таблиця 1.9 демонструє результати порівняльного аналізу зазначених методів.

Таблиця 1.9

Класифікація методів оцінки ризиків за типами

Методи оцінки ризиків			
	Якісні	**Кількісні**	**Комбіновані**
SWOT-аналіз	+		
Сценарний аналіз			+
Аналіз на основі подій (ETA)		+	
Аналіз на основі відмов (FTA)		+	
BIA (Business Impact Analysis)			+
Монте-Карло моделювання		+	
Математичне моделювання		+	
Експертні оцінки (Delphi)	+		
Матриці ризиків (Risk Matrix)			+
Ранжування ризиків			+

Таким чином, якісний підхід дозволяє швидко оцінити ризики за рівнем серйозності, тоді як кількісний метод забезпечує точні фінансові розрахунки для оцінки збитків. Комбіновані методи поєднують обидва підходи, забезпечуючи баланс між точністю та доступністю оцінки ризиків. Вибір методології залежить від специфіки організації, наявності історичних даних і рівня необхідної деталізації аналізу [20].

Висновки до розділу 1

Розглянуто теоретичні засади управління ризиками у системах менеджменту інформаційної безпеки, що є основою для розроблення ефективних заходів захисту інформаційних активів. Визначено основні компоненти та структуру системи менеджменту інформаційної безпеки, що включає політики, процеси та ресурси, необхідні для забезпечення надійного функціонування інформаційних систем.

Виокремлено класифікаційні ознаки ризиків, які дозволяють систематизувати загрози та оцінити їхній вплив на безпеку інформації. Особливу увагу приділено нормативно-правовим вимогам та міжнародним стандартам,

таким як ISO/IEC 27001, NIST SP 800-30, COBIT та GDPR, що забезпечують методологічну основу для оцінки та управління ризиками в інформаційній безпеці. Підкреслено значення національного законодавства у цій сфері, зокрема Закону України «Про захист інформації в інформаційно-комунікаційних системах», який регулює заходи безпеки на державному рівні.

У процесі дослідження використано сучасні підходи до ідентифікації ризиків, серед яких експертні опитування, аналіз вразливостей, метод сценаріїв загроз та аналіз історичних інцидентів. Розглянуто методи оцінки ризиків, що поділяються на якісні, кількісні та комбіновані, а також їхнє практичне застосування для мінімізації загроз.

Розділ 2 АНАЛІЗ І ОБҐРУНТУВАННЯ МЕТОДІВ ОЦІНКИ ТА МІНІМІЗАЦІЇ РИЗИКІВ У СИСТЕМАХ МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

2.1 Аналіз кількісних методів оцінки ризиків та їх застосування у системах менеджменту інформаційної безпеки

Матриця ризиків є одним із найбільш розповсюджених інструментів для оцінки ризиків в ІБ, оскільки дозволяє структуровано аналізувати рівень загроз на основі їхньої ймовірності та потенційного впливу. Цей метод належить до кількісних та якісних підходів, оскільки може використовувати як експертні оцінки, так і фактичні статистичні дані для визначення рівня ризику.

Матриця ризиків будується у вигляді таблиці (найчастіше формату 3×3, 4×4 або 5×5), де по горизонталі відображається ймовірність виникнення ризику, що може бути класифікована як низька, середня, висока (або поділена на більше градацій), а по вертикалі зазначається ступінь впливу ризику на ІБ організації, який також може бути незначним, середнім або критичним [21,22].

Перетин відповідних значень ймовірності та впливу визначає загальний рівень ризику, який може бути позначений кольорами (наприклад, зелений – низький ризик, жовтий – середній, червоний – критичний) (рис. 2.1).

Рис. 2.1. Матриця ризиків 3x3

Матриця ризиків дозволяє класифікувати ризики за рівнем критичності та приймати обґрунтовані рішення щодо необхідності реагування.

Оцінка ризиків у матриці ґрунтується на трьох основних параметрах. Першим є ймовірність виникнення ризику (P – Probability), яка визначається на основі історичних даних, аналізу загроз або статистичних моделей. Зазвичай вона класифікується за рівнями, такими як рідкісний, можливий, частий або дуже ймовірний. Другим параметром виступає вплив на систему (I – Impact), що оцінюється за наслідками для конфіденційності, цілісності та доступності інформації, а також враховує можливі фінансові, репутаційні та операційні збитки. Нарешті, загальний рівень ризику обчислюється як добуток ймовірності на вплив за формулою [23]:

$$Risk = \text{Probability} * \text{Impact} \tag{2.1}$$

У таблиці 2.1 наведено основні переваги та недоліки використання матриці ризиків у сфері ІБ, що дозволяє оцінити її ефективність та визначити можливі напрямки удосконалення.

Таблиця 2.1

Переваги та недоліки матриці ризиків

Переваги	**Недоліки**
Простота у використанні – дозволяє швидко ідентифікувати критичні ризики без складних розрахунків.	Суб’єктивність оцінки – експертні оцінки можуть бути неточними або упередженими.
Візуалізація загроз – полегшує розуміння ризиків для керівництва та співробітників.	Обмеженість градацій – поділ ризиків на кілька рівнів не завжди відображає повну картину загроз.
Гнучкість – може адаптуватися до різних типів інформаційних систем та організацій.	Відсутність детального фінансового аналізу – не дозволяє точно визначити економічні втрати від реалізації ризику.
Підтримка прийняття рішень – допомагає визначити пріоритетність заходів безпеки.	Не враховує комбінацію загроз – складні атаки можуть мати взаємопов’язаний вплив, що не завжди відображається у стандартній матриці.

Метод FMEA (Failure Mode and Effects Analysis) є кількісним підходом до оцінки ризиків, який використовується для виявлення можливих відмов у

системах та оцінки їхнього впливу на безпеку. Спочатку цей метод був розроблений у військовій та аерокосмічній промисловості, проте сьогодні він широко застосовується у сфері ІБ для оцінки ризиків, пов'язаних із відмовами систем, вразливостями програмного забезпечення та загрозами для IT-інфраструктури.

Концепція FMEA:

- F (Failure) – Виявлення потенційної відмови;
- M (Mode) – Визначення типів, способів та можливих варіантів відмови;
- E (Effect) – Аналіз негативного впливу відмови на процес;
- A (Analysis) – Дослідження ризику та розробка заходів для його мінімізації.

Основна ідея FMEA полягає у систематичному аналізі можливих відмов у системах, визначенні їхніх причин та наслідків, а також пріоритезації заходів для їхнього запобігання або зниження впливу.

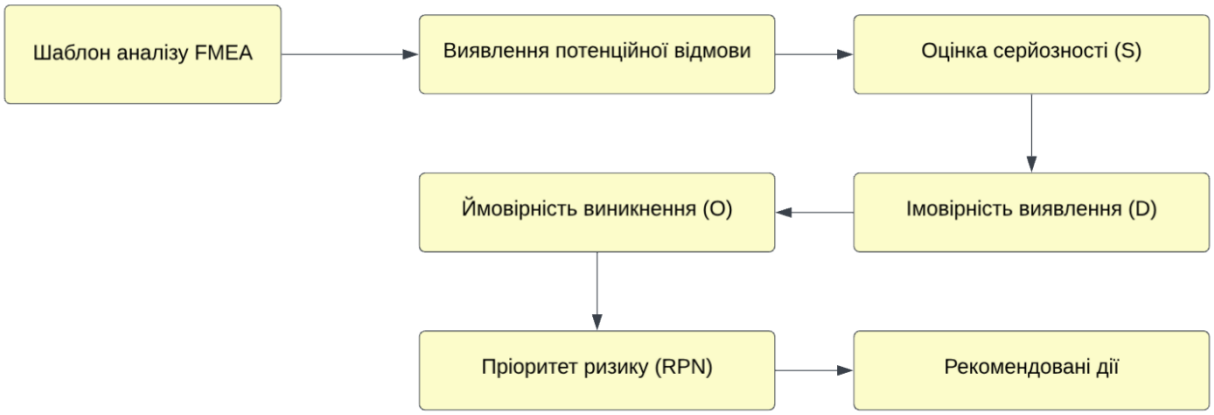

Рис. 2.2. Концепція FMEA

Короткий опис етапів алгоритму наведено нижче:

1. Ідентифікація елементів/процесів (наприклад: сервери, мережеві компоненти, БД);
2. Виявлення можливих відмов (наприклад: збої, витік даних, зломи);
3. Аналіз наслідків відмов (оцінка шкоди ІБ та бізнесу);
4. Аналіз причин відмов (наприклад, людський фактор, технічні помилки, атаки);

5. Оцінка ризику за трьома критеріями: S (Severity) – серйозність, O (Occurrence) – ймовірність, D (Detection) – імовірність виявлення;

6. Розрахунок пріоритету ризику (RPN);

7. Розробка та впровадження коригувальних дій.

Для кожної можливої відмови розраховується число пріоритету ризику (Risk Priority Number, RPN) за формулою:

$$RPN = S * O * D, \tag{2.2}$$

де: S (Severity, серйозність наслідків) – показує рівень впливу відмови на систему, оцінка проводиться за шкалою від 1 (незначний вплив) до 10 (катастрофічні наслідки); O (Occurrence, ймовірність виникнення) – відображає частоту виникнення потенційної загрози, оцінюється від 1 (дуже рідко) до 10 (дуже часто); D (Detection, ймовірність виявлення) – оцінює здатність виявити проблему до того, як вона реалізується, визначається в межах від 1 (легко виявляється) до 10 (важко виявити).

На основі цих трьох коефіцієнтів розраховується число пріоритету ризику.

Наступним етапом є пріоритизація та усунення ризиків, що передбачає визначення найбільш критичних загроз за величиною RPN та розробку відповідних заходів для зменшення ризиків. До таких заходів належать впровадження додаткових механізмів безпеки, удосконалення процедур контролю, а також регулярне тестування вразливих елементів системи.

В таблиці 2.2 розглянуто приклад оцінки ризику за методом FMEA для бази даних, що містить конфіденційну інформацію [24]. В даному випадку найвищий RPN (189) має ризик несанкціонованого доступу, що вимагає першочергового впровадження заходів безпеки, таких як двофакторна автентифікація, посилена політика паролів та аудит доступу.

Таблиця 2.2

Приклад оцінки ризику за методом FMEA

Можлива відмова	**Наслідки**	**Причини**	**S**	**O**	**D**	**RPN**
Несанкціонований доступ до бази даних	Витік конфіденційної інформації	Використання слабких паролів, недостатня автентифікація	9	7	3	189
Втрата даних через збій	Порушення роботи системи	Відсутність резервного копіювання	8	5	2	80
Вразливість у програмному забезпеченні	Можливість експлуатації хакерами	Використання застарілих компонентів	7	6	4	168

Метод FMEA знайшов широке застосування в СМІБ завдяки здатності ідентифікувати потенційні відмови, оцінювати їх вплив, ймовірність виникнення та можливість виявлення, а також визначати пріоритетність обробки ризиків. Алгоритм його реалізації наведено на рисунку 2.3 [25].

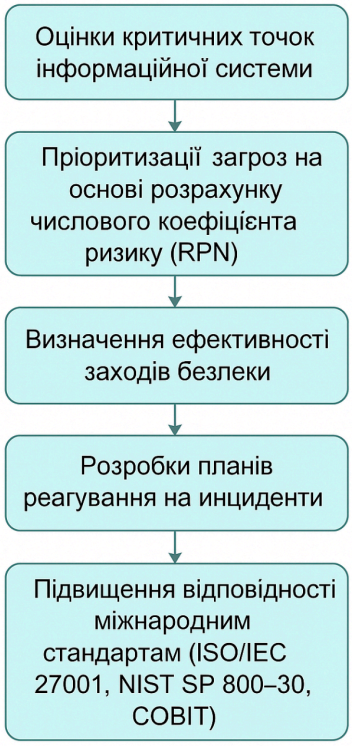

Рис. 2.3. Алгоритм застосування методу FMEA в СМІБ

У таблиці 2.3 наведено основні переваги та недоліки використання методу FMEA, що дозволяє оцінити його ефективність та визначити оптимальні умови для його застосування в системах управління ризиками ІБ.

Таблиця 2.3

Переваги та недоліки методу FMEA

Переваги	**Недоліки**
Дає чітке уявлення про ризики та їхні наслідки.	Процес може бути трудомістким для великих організацій.
Дозволяє пріоритизувати загрози та зосередитися на найбільш критичних.	Вимагає глибокої експертизи та детальної документації.
Використовує числові значення, що полегшує прийняття рішень.	Не враховує взаємозв'язок між ризиками та їхній комбінований вплив.
Може бути адаптований до різних типів організацій.	Висока залежність від точності вихідних оцінок.

Метод FMEA є потужним інструментом оцінки ризиків у сфері ІБ, який дозволяє систематично аналізувати потенційні відмови, їхні причини та наслідки. Завдяки розрахунку числа пріоритету ризику (RPN) організації можуть ефективно пріоритизувати загрози та розробляти стратегії їхнього мінімізації. Незважаючи на певні обмеження, метод FMEA є універсальним підходом, який можна адаптувати до різних інформаційних систем і бізнес-процесів. Його застосування допомагає підвищити рівень ІБ та відповідність нормативним вимогам, знижуючи ймовірність серйозних загроз та інцидентів у кіберпросторі.

Кількісні методи оцінки ризиків у СМІБ відіграють важливу роль у визначенні рівня загроз, уразливостей та можливих наслідків для організації. Вони дозволяють використовувати математичні моделі та статистичні підходи для розрахунку ймовірності виникнення ризиків та оцінки їхнього впливу.

Метод аналізу дерева відмов (Fault Tree Analysis, FTA) є одним із найпоширеніших методів кількісного аналізу ризиків. Він використовується для виявлення та оцінки комбінацій подій, які можуть призвести до відмови системи або критичних інцидентів [26-28].

На рисунку 2.4 представлено основні етапи реалізації методу аналізу на основі відмов (FTA), що використовується для ідентифікації причин небажаних подій та оцінки ймовірності їх виникнення.

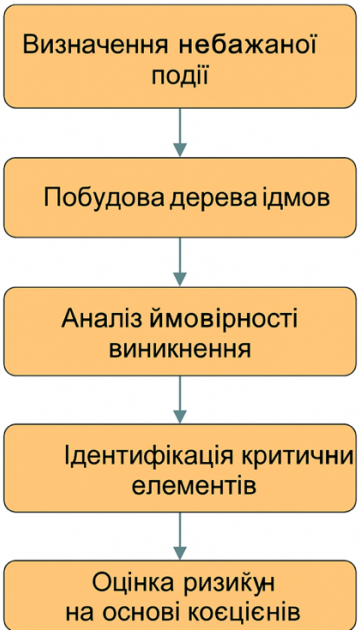

Рис. 2.4. Етапи реалізації методу FTA (Fault Tree Analysis)

У таблиці 2.4 наведено основні переваги та недоліки кількісних методів оцінки ризиків, які використовуються в СМІБ.

Таблиця 2.4

Переваги та недоліки кількісних методів оцінки ризиків

Переваги	**Недоліки**
Об'єктивність – оцінка базується на числових значеннях, що зменшує суб'єктивність аналізу.	Необхідність точних вхідних даних – без достовірних статистичних даних результати можуть бути неточними.
Прогнозування – можливість передбачити потенційні загрози та оцінити їх вплив.	Складність розрахунків – деякі методи вимагають значних обчислювальних ресурсів і спеціалізованого програмного забезпечення.
Підтримка прийняття рішень – результати аналізу допомагають у виборі оптимальних заходів для мінімізації ризиків.	Ігнорування якісних аспектів – кількісні методи не завжди враховують нематеріальні фактори, такі як людська поведінка чи організаційна культура.
Автоматизація – використання математичних моделей та алгоритмів дозволяє автоматизувати процес аналізу ризиків.	Обмеженість при роботі з унікальними або новими ризиками, для яких немає історичних даних.
Можливість кількісного порівняння ризиків між різними системами чи сценаріями.	Можливість хибної точності – математичні моделі можуть створювати ілюзію високої точності, тоді як вхідні дані можуть бути неточними.
Деталізованість – дозволяє глибоко аналізувати ризики за допомогою моделей ймовірностей.	Необхідність експертної оцінки для інтерпретації отриманих результатів.
Можливість використання історичних даних для підвищення точності прогнозів.	Часозатратність – потребує значних ресурсів на збирання, обробку та аналіз даних.

2.2 Визначення особливостей якісних методів оцінки ризиків і їх ролі в ухваленні управлінських рішень

Управління ризиками в ІБ базується не лише на кількісному аналізі, а й на якісних методах, які дозволяють оцінити рівень небезпеки в умовах відсутності точних числових даних або їх недостатності. Якісні методи є важливою складовою процесу прийняття рішень у сфері ІБ, оскільки дають можливість систематизувати знання експертів, ідентифікувати потенційні загрози та оцінити їхній вплив на організацію.

Метод експертних оцінок та Delphi. Метод експертних оцінок полягає у зборі думок фахівців у певній галузі для визначення потенційних ризиків, їхньої ймовірності та можливого впливу. Такий підхід дає змогу враховувати практичний досвід експертів, особливо в ситуаціях, коли об'єктивні дані відсутні або неповні [28].

Одним з удосконалених варіантів цього методу є метод Delphi – багатоетапний процес опитування експертів, який передбачає кілька раундів анкетування з подальшим наданням учасникам зведених результатів попереднього етапу. Це стимулює перегляд та уточнення оцінок, наближаючи учасників до консенсусу. Метод Delphi допомагає зменшити суб'єктивність оцінювання та враховувати різноманітні точки зору.

Роль якісних оцінок в управлінні ІБ та прийнятті рішень. Якісні методи оцінки ризиків у сфері ІБ відіграють критичну роль у процесі ухвалення управлінських рішень. Вони дають змогу визначити пріоритети захисту в умовах обмежених ресурсів, а також оцінити сценарії розвитку загроз без потреби в точних числових даних. Завдяки залученню досвіду фахівців такі методи забезпечують обґрунтованість управлінських рішень та покращують комунікацію між підрозділами організації через просту візуалізацію результатів, зокрема за допомогою матриць ризиків. Окрім того, якісні методи підвищують гнучкість управління ІБ, оскільки дозволяють адаптуватися до змін у зовнішньому середовищі.

Таким чином, якісні методи оцінки ризиків виступають важливим інструментом для аналізу складних систем без чітко визначених параметрів, сприяючи ефективному управлінню ІБ та оптимізації рішень щодо мінімізації ризиків [29].

Метод DELPHI – це структурований підхід до прогнозування та оцінки ризиків, який базується на колективній думці експертів. Він широко використовується в процесі прийняття управлінських рішень, особливо у сфері ІБ, стратегічного планування та оцінки ризиків.

Метод Delphi є одним із ключових якісних інструментів у сфері оцінки ризиків ІБ. Його основною особливістю є анонімність експертів, що дозволяє уникнути впливу авторитетів та групового тиску. Метод реалізується через ітеративний процес опитувань, під час яких експерти надають свої оцінки незалежно один від одного. Після кожного раунду результати агрегуються та аналізуються статистично, а експерти отримують зворотний зв’язок і можуть переглянути власні відповіді. Такий підхід сприяє досягненню консенсусу та дозволяє зробити більш зважені управлінські висновки.

Застосування методу Delphi передбачає формування групи фахівців, підготовку анкет, проведення кількох раундів оцінювання та фінальну обробку результатів. Його використовують для стратегічного прогнозування, формування політик у сфері ІБ та аналізу ймовірних сценаріїв розвитку загроз. Метод дозволяє зменшити суб’єктивність у прийнятті рішень, визначити критичні ризики, а також спрогнозувати тенденції, які можуть мати довгостроковий вплив на організацію.

Методика анкетування – це один із якісних методів оцінки ризиків, що базується на зборі думок експертів, працівників або зацікавлених осіб через спеціально розроблені анкети. Вона є важливим інструментом в управлінні ризиками, оскільки дозволяє виявити потенційні загрози, оцінити їх вплив та розробити відповідні заходи для мінімізації ризиків. Етапи проведення анкетування наведено в таблиці 2.5 [30].

Таблиця 2.5

Етапи проведення анкетування

Етап	Опис
1. Формулювання цілей	Визначення мети дослідження: оцінка ризиків, визначення проблемних зон, прогнозування загроз.
2. Розробка анкети	Підготовка змісту: формулювання запитань (відкритих, закритих, змішаних), вибір масштабу оцінки ризиків (наприклад, шкала від 1 до 5).
3. Визначення цільової аудиторії	Вибір експертів, співробітників або зацікавлених осіб, які будуть відповідати на запитання.
4. Проведення анкетування	Розсилка анкет та збір відповідей (електронні чи паперові форми, інтерв'ю).
5. Аналіз та обробка даних	Узагальнення відповідей, статистичний аналіз, виявлення основних ризиків та їх рівня впливу.
6. Формування висновків	Визначення основних загроз, підготовка рекомендацій для управлінських рішень.

Методика анкетування є ефективним інструментом для збору інформації про ризики та їхню оцінку, що допомагає у прийнятті управлінських рішень. Вона має як значні переваги, так і певні обмеження, які слід враховувати при її застосуванні. У таблиці 2.6 наведено основні переваги та недоліки анкетування в контексті оцінки ризиків.

Таблиця 2.6

Переваги та недоліки методики анкетування

Переваги	Недоліки
Доступність та простота впровадження	Можливість упередженості або суб'єктивності відповідей
Охоплення великої аудиторії	Потреба у ретельному формулюванні питань
Можливість автоматизованої обробки даних	Відсутність глибокого аналізу проблеми (лише поверхневий зріз інформації)
Гнучкість (можливість зміни питань, адаптації під конкретні задачі)	Ймовірність низького рівня залученості респондентів (відповіді можуть бути поверхневими)

2.3 Проведення порівняльного аналізу методів оцінки ризиків та обґрунтування вибору оптимального підходу

Вибір методу оцінки ризиків в СМІБ залежить від багатьох факторів, включаючи обсяг доступної інформації, цілі оцінювання, ресурси організації та специфіку діяльності. У цьому контексті доцільно провести порівняльний аналіз кількісних та якісних методів оцінки ризиків. Порівняння якісних та кількісних методів оцінки ризиків дозволяє визначити їх сильні та слабкі сторони залежно від контексту використання. У таблиці 2.7 представлено основні відмінності між цими підходами за ключовими ознаками [31].

Таблиця 2.7

Порівняння якісних та кількісних методів оцінки ризиків

Ознака	Якісні методи	Кількісні методи
Точність	Суб'єктивна оцінка, базується на експертному досвіді	Висока точність за наявності достатніх даних
Складність застосування	Просте застосування, не потребує спеціалізованих інструментів	Вимагає використання спеціальних моделей, програмного забезпечення
Час та витрати	Менші витрати та короткий час проведення	Більші витрати на збирання даних і моделювання
Гнучкість	Висока адаптивність до змін	Менш гнучкі через залежність від даних
Прийнятність в умовах невизначеності	Добре підходять за відсутності повних даних	Ефективні при наявності великого обсягу точної інформації
Результат	Якісна категоризація ризиків (високий, середній, низький)	Конкретні числові значення ризиків, очікувані збитки

Кількісні та якісні методи оцінки ризиків є двома основними підходами, які використовуються для аналізу потенційних загроз та ухвалення управлінських рішень. Кількісні методи базуються на числових даних і математичних розрахунках, тоді як якісні методи використовують експертні оцінки, опитування та описові характеристики ризиків. У таблиці 2.8 наведено основні відмінності між цими двома підходами [31].

Таблиця 2.8

Порівняння кількісних і якісних методів оцінки ризиків

Критерій	**Кількісні методи**	**Якісні методи**
Суть підходу	Використання числових даних, математичних моделей, ймовірнісного аналізу	Оцінка ризиків на основі експертних думок, анкетування, аналізу сценаріїв
Тип даних	Кількісні показники (ймовірності, фінансові втрати, статистичні дані)	Вербальні оцінки (низький, середній, високий ризик)
Інструменти	Формули, статистичні моделі, метод Монте-Карло, аналіз дерева рішень	Анкетування, експертні оцінки, SWOT-аналіз, метод DELPHI
Об’єктивність	Висока (базується на точних числових розрахунках)	Помірна (залежить від суб’єктивних оцінок експертів)
Глибина аналізу	Висока деталізація, що дозволяє робити точні прогнози	Загальний аналіз ризиків без точних значень
Гнучкість	Менш гнучкий, потребує наявності історичних даних	Висока гнучкість, можливість застосування в умовах невизначеності
Часовитрати	Високі (потребує збору та обробки великого масиву даних)	Нижчі, ніж у кількісних методах (можна швидко отримати результати)
Доступність	Вимагає спеціалізованих знань та програмного забезпечення	Доступний навіть за відсутності великої кількості даних
Області застосування	Фінансовий аналіз, кібербезпека, технічні ризики	Управління безпекою, стратегічне планування, організаційні ризики

Обидва підходи мають свої переваги та недоліки, тому їх варто використовувати у комплексі для отримання більш повної картини ризиків.

- кількісні методи дають точні результати, проте потребують наявності достовірних даних;
- якісні методи дозволяють швидко оцінити ризики та визначити їхню пріоритетність навіть за умов обмеженої інформації.

Оптимальний підхід полягає у комбінуванні обох методів: якісна оцінка використовується для первинного аналізу ризиків, а кількісна – для їх детального вимірювання та прогнозування наслідків.

Різні організації мають унікальні вимоги до оцінки ризиків залежно від своєї діяльності, масштабу та рівня критичності можливих загроз. Вибір між якісними, кількісними або комбінованими методами оцінки ризиків залежить від типу організації, доступності даних, а також специфіки прийняття рішень. У

таблиці 2.9 представлено оптимальні методи оцінки ризиків для різних типів організацій [32].

Таблиця 2.9

Оптимальні методи оцінки ризиків залежно від типу організації

Тип організації	**Оптимальні методи оцінки ризиків**
Великі корпорації (банки, страхові компанії, міжнародні підприємства)	Кількісні методи: статистичний аналіз, метод Монте-Карло, аналіз дерева рішень, аналіз втрат (Loss Event Analysis). Додатково: якісні методи для стратегічного аналізу (SWOT, експертні оцінки).
Малі та середні підприємства (МСБ)	Комбіновані методи: SWOT-аналіз, анкетування, експертні оцінки, PHA (Preliminary Hazard Analysis), аналіз сценаріїв.
Державні установи та органи влади	Якісні методи: анкетування, експертні оцінки (метод DELPHI), аналіз сценаріїв. Додатково: кількісні методи при аналізі фінансових ризиків або оцінці ефективності політик.
IT-компанії та організації, що працюють із даними	Кількісні методи: аналіз ризиків кібератак (Quantitative Risk Assessment), FMEA (Failure Modes and Effects Analysis), методи оцінки ймовірностей атак (Bayesian Networks). Додатково: якісні методи (аналіз загроз, експертні опитування).
Медичні установи (лікарні, фармацевтичні компанії)	Комбіновані методи: аналіз наслідків відмов (FMEA), SWOT-аналіз, експертні оцінки, статистичний аналіз ризиків пацієнтів.
Будівельні компанії та промислові підприємства	Кількісні методи: HAZOP (Hazard and Operability Study), аналіз дерева відмов, статистичний аналіз аварій. Додатково: якісні методи для попереднього аналізу загроз (анкетування, метод сценаріїв).
Навчальні заклади та науково-дослідні установи	Якісні методи: SWOT-аналіз, метод DELPHI, анкетування для оцінки безпеки освітнього середовища. Додатково: кількісні методи при дослідженнях ризиків у фінансуванні та ефективності навчальних програм.

Вибір оптимального методу оцінки ризиків залежить від:

1. Розміру організації та доступності даних (великі корпорації мають можливість застосовувати складні кількісні методи, тоді як малий бізнес покладається на якісні оцінки);

2. Сфери діяльності (наприклад, у кібербезпеці більш ефективні кількісні методи, а в державному управлінні – якісні);

3. Критичності ризиків (у високоризикових галузях, як-от медицина та будівництво, використовуються комбіновані підходи).

Найбільш ефективною є комбінована стратегія, коли якісні методи допомагають ідентифікувати ризики, а кількісні – їх деталізовано оцінити та прогнозувати можливі наслідки [33].

2.4 Розроблення адаптивних стратегій мінімізації ризиків з урахуванням новітніх викликів кіберзагроз

У контексті сучасних загроз ІБ, актуальним завданням є впровадження адаптивних стратегій мінімізації ризиків, що дозволяють оперативно реагувати на зміну кіберзагроз і зменшувати їх потенційний вплив на інформаційні активи організації. Основою для побудови таких стратегій є класифікація методів реагування на ризики, яка включає чотири базові підходи: уникнення ризику, зменшення ризику, передача ризику та прийняття ризику. У процесі управління ризиками після їх ідентифікації та оцінки необхідно обрати відповідну стратегію реагування. У таблиці 2.10 наведено основні стратегії обробки ризиків у сфері ІБ разом з їх короткою характеристикою [34, 35].

Таблиця 2.10

Основні стратегії обробки ризиків у сфері ІБ

Стратегія	Сутність
Уникнення	Повна відмова від діяльності, що генерує надмірний ризик.
Зменшення	Застосування технічних та організаційних заходів для зниження ймовірності виникнення або наслідків ризику.
Передача	Передача ризику сторонній стороні (страхування, аутсорсинг).
Прийняття	Усвідомлене прийняття залишкового ризику за умови, що витрати на його зменшення перевищують можливі збитки.

Актуальними сучасними підходами до мінімізації ризиків в ІБ є використання концепції Zero Trust (архітектура нульової довіри), яка базується на припущенні, що жоден користувач чи пристрій не є автоматично довіреним, навіть всередині корпоративної мережі. Обов'язковим компонентом таких стратегій виступає багатофакторна автентифікація (MFA), що значно ускладнює несанкціонований доступ навіть у випадку компрометації паролів. Іншим важливим інструментом є аналіз поведінки користувачів (UEBA – User and Entity

Behavior Analytics), який дозволяє виявляти аномальні дії та потенційні інциденти безпеки ще на ранніх етапах.

Для технічної реалізації стратегій зменшення ризиків доцільно використовувати сучасні технологічні рішення:

- SIEM (Security Information and Event Management) – збір, аналіз і кореляція подій безпеки для оперативного реагування;
- XDR (Extended Detection and Response) – розширене виявлення та реагування на інциденти в усіх компонентах IT-інфраструктури;
- EDR (Endpoint Detection and Response) – моніторинг та реагування на загрози на рівні кінцевих пристроїв;
- IAM (Identity and Access Management) – управління доступом та ідентифікацією користувачів, що дозволяє забезпечити принцип найменших привілеїв.

Сучасні виклики кібербезпеки потребують адаптивних стратегій управління ризиками, що можуть динамічно реагувати на загрози в реальному часі. Інтеграція штучного інтелекту (AI) та машинного навчання (ML) у ризик-менеджмент дозволяє значно підвищити ефективність виявлення, аналізу та мінімізації ризиків у цифровому середовищі.

AI та ML використовуються для:

- аналізу великих обсягів даних – розпізнавання аномалій у поведінці користувачів та мережевого трафіку;
- автоматичного виявлення загроз – прогнозування атак на основі історичних даних;
- оцінки ризиків у реальному часі – адаптивна реакція на нові загрози та мінімізація їх наслідків;
- прогнозування можливих атак – виявлення потенційних вразливостей та розробка проактивних заходів захисту;
- оптимізації прийняття рішень – використання алгоритмів машинного навчання для автоматичного ранжування загроз за рівнем критичності.

Використання штучного інтелекту та машинного навчання в кібербезпеці

дозволяє ефективно аналізувати загрози, прогнозувати атаки та автоматизувати процеси захисту інформаційних систем. Різні AI/ML-підходи застосовуються для виявлення аномалій, аналізу поведінки користувачів, обробки природної мови та автономного ухвалення рішень. У таблиці 2.11 наведено основні методи та їх застосування в галузі кібербезпеки [36].

Таблиця 2.11

Ключові AI/ML-підходи у кібербезпеці

Метод AI/ML	**Опис**	**Приклад застосування**
Аналіз аномалій (Anomaly Detection)	Використання ML-алгоритмів для виявлення нетипової активності в мережі	Виявлення спроб несанкціонованого доступу до корпоративних систем
Глибоке навчання (Deep Learning)	Використання нейронних мереж для аналізу складних патернів кіберзагроз	Аналіз фішингових атак та розпізнавання шкідливих вкладень
Обробка природної мови (NLP)	Розпізнавання шкідливого контенту в електронній пошті та веб-трафіку	Виявлення соціальної інженерії в повідомленнях
Автоматизоване ухвалення рішень (AI-driven Decision Making)	AI-системи аналізують рівень ризику та рекомендують дії	Автоматичне блокування підозрілих транзакцій у банківських системах
Прогнозна аналітика (Predictive Analytics)	Використання історичних даних для прогнозування майбутніх атак	Визначення ймовірності DDoS-атаки на основі попередніх спроб вторгнення
Автономні системи реагування (Autonomous Response Systems)	AI-системи автоматично реагують на загрози без втручання людини	Самостійне ізолювання заражених пристроїв у корпоративній мережі

Інтеграція штучного інтелекту (AI) та машинного навчання (ML) у ризик-менеджмент має низку переваг. Однією з головних є висока швидкість аналізу, адже AI здатний обробляти великі обсяги даних набагато швидше, ніж традиційні методи. Це також сприяє зниженню людського фактора, оскільки автоматизація процесів мінімізує ймовірність помилок, спричинених людським втручанням. Крім того, AI забезпечує проактивний підхід до управління ризиками, що дозволяє не лише виявляти загрози, а й прогнозувати їх та запобігати можливим атакам. Завдяки високій гнучкості та адаптивності AI-системи здатні швидко реагувати на нові кіберзагрози в режимі реального часу. Також машинне навчання допомагає ефективно ранжувати ризики, визначаючи

їх критичність, що дозволяє оптимально розподіляти ресурси для захисту найбільш вразливих напрямів.

Проте існують і певні виклики та обмеження впровадження AI та ML у ризик-менеджмент. Одним із них є потреба у великих обсягах навчальних даних, оскільки ефективність системи безпосередньо залежить від якості та кількості вхідної інформації. Крім того, штучний інтелект сам може стати об’єктом атак, оскільки хакери можуть використовувати техніки "adversarial AI" для введення системи в оману. Висока вартість впровадження також є суттєвим фактором, оскільки інтеграція AI-рішень потребує значних фінансових і технічних ресурсів. Незважаючи на високу автономність, навіть найсучасніші AI-системи все ще потребують людського контролю, постійного моніторингу та коригування їхньої роботи.

З розвитком кіберзагроз організації потребують комплексних рішень для виявлення, аналізу та реагування на інциденти безпеки. Два ключові елементи сучасного ризик-менеджменту в кібербезпеці – це SIEM-системи (Security Information and Event Management) та SOC-центри (Security Operations Center).

SIEM (Security Information and Event Management) – це технологічне рішення, яке збирає, аналізує та корелює журнали подій із різних джерел у реальному часі. Воно дозволяє виявляти потенційні загрози та порушення безпеки на основі аналітики поведінки та правил кореляції.

Ключові функції SIEM [37,38]:

- централізований збір логів – об'єднання подій із серверів, мережевого обладнання, баз даних та кінцевих пристроїв;
- аналіз кореляцій подій – виявлення аномалій та шкідливих патернів у поведінці систем і користувачів;
- моніторинг у реальному часі – швидке реагування на підозрілі події та активність;
- автоматичне сповіщення – повідомлення аналітиків про потенційні атаки;

- формування звітності – аудит подій безпеки для відповідності стандартам (ISO 27001, GDPR, PCI DSS).

Завдяки цим можливостям SIEM допомагає організаціям не лише оперативно виявляти кіберзагрози, а й виконувати довгостроковий аналіз інцидентів для вдосконалення захисту.

Висновки до розділу 2

Проведено всебічний аналіз методів оцінки ризиків у системах менеджменту інформаційної безпеки, що дозволило сформувати науково обґрунтований підхід до їх вибору та застосування.

У рамках дослідження кількісних методів оцінки ризиків було визначено їхню роль у забезпеченні точних та об'єктивних результатів, що дозволяє організаціям ефективно прогнозувати потенційні загрози. Такі методи, як аналіз дерева рішень, метод Монте-Карло та FMEA, виявилися найбільш доцільними у випадках, коли необхідно отримати кількісні показники ймовірності виникнення ризиків та їхнього впливу.

Розгляд якісних методів оцінки ризиків показав їхню значну роль у процесі ухвалення управлінських рішень, особливо в умовах недостатньої кількості статистичних даних. Метод DELPHI, анкетування та SWOT-аналіз виявилися ефективними інструментами для суб'єктивної експертної оцінки, що дозволяє швидко ідентифікувати потенційні загрози та розробляти превентивні заходи.

З огляду на сучасні виклики в інформаційній безпеці, було розглянуто адаптивні стратегії мінімізації ризиків, що включають використання новітніх технологій. Інтеграція AI та ML у процеси управління ризиками дозволяє автоматизувати виявлення загроз та прогнозування атак, тоді як SIEM-системи та SOC-центри значно підвищують рівень моніторингу та реагування на інциденти безпеки.

Розділ 3 ПРАКТИЧНЕ ВПРОВАДЖЕННЯ МЕТОДІВ ОЦІНКИ ТА МІНІМІЗАЦІЇ РИЗИКІВ У СИСТЕМАХ МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

3.1 Оцінка поточного стану системи менеджменту інформаційної безпеки досліджуваної організації

У рамках даного дослідження було проаналізовано реальний стан СМІБ у досліджуваній організації SeriesWedgiX. Організація вже має затверджену політику ІБ, проте виявлено, що не всі її положення відповідають актуальним вимогам міжнародних стандартів. Зокрема, виявлено часткову відповідність ISO/IEC 27001, яка проявляється у наявності процедур контролю доступу та базових заходів аудиту, однак процес управління ризиками ще недостатньо формалізований [39].

Організаційна структура управління ІБ включає призначеного відповідального за ІБ, але відсутній повноцінний підрозділ або служба ІБ. Обов’язки щодо моніторингу та реагування на інциденти частково розподілено між ІТ-відділом та керівником з безпеки. Це створює ризики нечіткого розмежування відповідальності у випадку інцидентів.

Вивчення внутрішніх процедур показало, що організація використовує нерегулярний підхід до аналізу ризиків. Формалізовані політики управління ризиками наявні частково, однак не всі з них відображають практичні механізми виявлення та оцінки потенційних загроз. Наприклад, регулярний моніторинг активів проводиться, проте не супроводжується системним аналізом їхньої критичності.

Рівень обізнаності персоналу щодо загроз у сфері ІБ виявився нерівномірним. Попри епізодичні тренінги, результати анкетування свідчать про відсутність розуміння ключових політик ІБ у частини працівників, особливо серед не-ІТ персоналу. Це потребує впровадження постійної програми підвищення обізнаності.

Серед ключових активів було визначено сервери з клієнтськими БД, CRM-систему, а також хмарну інфраструктуру, яка обробляє фінансові дані. Вразливими векторами визнано використання застарілого ПЗ, недостатній контроль над правами доступу та обмежену видимість подій у хмарному середовищі.

Аналіз інцидентів за останній рік показав кілька випадків фішингу, втрати конфіденційної інформації через людський фактор і дві події, що класифікуються як витік даних. Усі інциденти мали низький або середній рівень впливу, проте ефективність реагування виявилася недостатньою – не всі інциденти було зафіксовано своєчасно.

Узагальнюючи результати, можна стверджувати, що система ІБ перебуває на середньому рівні зрілості. Організація має базові документи та процедури, однак відсутня інтегрована система управління ризиками, належний моніторинг і системне підвищення обізнаності персоналу. Впровадження системного підходу до ІБ відповідно до ISO/IEC 27001 із адаптацією під реальні потреби бізнесу дозволить значно підвищити стійкість організації до сучасних кіберзагроз [39,40].

Аналіз існуючих політик інформаційної безпеки, їх відповідність міжнародним стандартам (ISO/IEC 27001, NIST, COBIT). У межах аналізу поточного стану системи ІБ підприємства SeriesWedgiX було проведено огляд локальних політик, що регламентують основні аспекти ІБ. На момент оцінювання організація мала затверджені документи, які охоплюють контроль доступу до інформаційних систем, політику паролів, регламент резервного копіювання та порядок реагування на інциденти. Проте виявлено, що структура більшості з цих документів не відповідає формальним вимогам міжнародних стандартів і не включає належної деталізації обов’язків, критеріїв ризику або періодичності перегляду.

У порівнянні з вимогами стандарту ISO/IEC 27001:2022, документи SeriesWedgiX лише частково реалізують вимоги щодо забезпечення конфіденційності, цілісності та доступності інформаційних активів. Наприклад,

визначення відповідальностей за реалізацію заходів безпеки здійснено фрагментарно, а ризик-орієнтований підхід не є системним. Також у політиках відсутній опис методів оцінки ризиків, що є необхідною складовою для відповідності ISO-критеріям.

Порівняльний аналіз з рекомендаціями фреймворку COBIT 2019 свідчить про нестачу орієнтації на управління продуктивністю ІБ-процесів, відсутність KPI для контролю ефективності заходів безпеки, а також про низький рівень інтеграції політик у загальну систему управління підприємством. Проблемною є й відсутність чітких процедур ескалації інцидентів ІБ, що унеможливлює побудову повного циклу PDCA (Plan-Do-Check-Act) у рамках СМІБ [41].

Стандарти NIST SP 800-53 частково враховуються в аспектах технічного контролю доступу, шифрування даних і автентифікації, однак недотримано вимог щодо безпеки персоналу, реагування на інциденти, а також аудиту й логування подій. Брак централізованої системи моніторингу подій безпеки призводить до низької виявлюваності потенційних загроз, що суперечить принципам zero trust, визначеним у сучасних рекомендаціях NIST.

Дослідження організаційної структури управління інформаційною безпекою: розподіл відповідальності, наявність спеціалізованих підрозділів або посад. В організаційній структурі SeriesWedgiX відсутній окремий підрозділ ІБ. Всі функції контролю й забезпечення ІБ розподілені між ІТ-відділом та одним відповідальним за ІБ фахівцем, який виконує обмежений перелік завдань. Це створює ситуацію, коли реалізація заходів безпеки має фрагментарний характер і залежить від компетентності окремих працівників, а не від функціональної моделі управління.

На рисунку 3.1 представлено спрощену схему поточної структури управління ІБ в SeriesWedgiX. Вона відображає існуючі зв’язки між адміністративним керівництвом, технічними службами та відповідальною особою за ІБ.

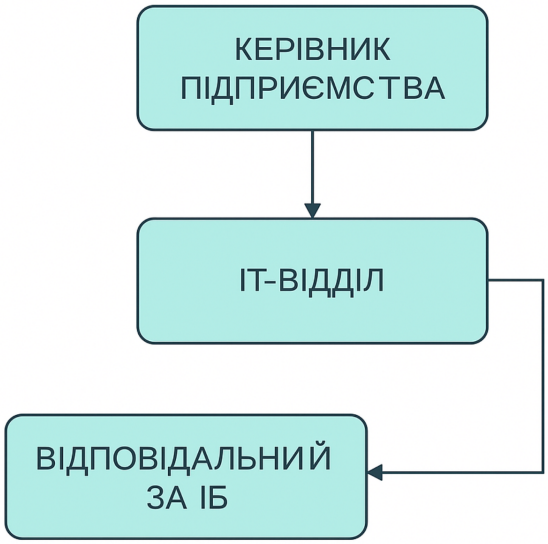

Рис. 3.1. Схема поточної структури управління інформаційною безпекою в SeriesWedgiX

Відсутність спеціалізованого підрозділу або чітко регламентованих ролей призводить до того, що процеси управління ризиками, реагування на інциденти, аудит, навчання персоналу та інші ключові елементи СМІБ не мають визначених виконавців. Це знижує здатність компанії швидко реагувати на загрози та перешкоджає реалізації принципу розмежування обов'язків (separation of duties), який визначено як базовий у NIST та ISO/IEC 27001 [42].

Оцінка наявності та ефективності регламентованих процедур управління ризиками інформаційної безпеки. Оцінка наявності та ефективності регламентованих процедур управління ризиками ІБ є критично важливою для підтримання сталого функціонування СМІБ. У досліджуваній організації такі процедури мають бути задокументовані в локальних нормативних актах (ЛНА), що регламентують порядок ідентифікації, аналізу, оцінювання, реагування та моніторингу ризиків.

Наявність формалізованих процедур свідчить про системний підхід до управління ризиками, зокрема – про запровадження механізмів оцінки впливу на конфіденційність, цілісність і доступність (CIA) інформаційних активів. Водночас, для ефективності цих процедур важливо забезпечити не лише наявність методологічної бази, але й регулярне проведення аналізу ризиків

(згідно з вимогами ISO/IEC 27005) з фіксацією результатів у вигляді звітів та матриць ризиків [43-45].

До ключових індикаторів ефективності регламентованих процедур управління ризиками належать:

- наявність реєстру активів та відповідних загроз;
- застосування методів кількісної чи якісної оцінки (наприклад, матриця ймовірності та впливу);
- регулярність оновлення оцінки ризиків (не рідше одного разу на рік або при суттєвих змінах ІТ-інфраструктури);
- інтеграція результатів оцінки ризиків у процес прийняття рішень щодо впровадження заходів ІБ.

Аналіз рівня усвідомленості персоналу щодо ризиків інформаційної безпеки на основі опитувань, тестувань або аналізу інцидентів. Аналіз рівня усвідомленості персоналу щодо ризиків ІБ дозволяє оцінити, наскільки працівники розуміють власну роль у забезпеченні безпеки інформаційних активів організації. Цей аспект є невіддільною складовою ефективної СМІБ, оскільки навіть найсучасніші технічні засоби не забезпечують належного рівня захисту без належної поведінки користувачів.

У досліджуваній організації рівень обізнаності персоналу може оцінюватися за допомогою таких підходів:

- анонімні опитування, які виявляють загальний рівень знань про політики ІБ, типові загрози, правила роботи з конфіденційною інформацією;
- тестування після проходження навчальних модулів або тренінгів з ІБ (в тому числі за напрямами: фішинг, створення паролів, робота з хмарними сервісами тощо);
- аналіз зареєстрованих інцидентів, спричинених помилками користувачів або порушеннями процедур (наприклад, відкриття фішингових листів, підключення незахищених пристроїв тощо).

Для представлення результатів опитування та тестування доцільно використовувати індекс обізнаності з ІБ (Security Awareness Index), що обчислюється за формулою [44]:

$$SAI = \frac{\sum P_i * W_i}{\sum W_i}, \quad (3.1)$$

де P_i – індивідуальний бал працівника за окремими категоріями (політики, загрози, поведінка), W_i – ваговий коефіцієнт значущості кожної категорії.

Отримані результати дозволяють виявити слабкі місця в підготовці персоналу та сформувати рекомендації щодо посилення освітніх заходів. У разі низького рівня усвідомленості – рекомендується запровадити регулярні тренінги, симуляції атак (наприклад, фішингових кампаній) і щоквартальні перевірки знань. Це підвищує не лише загальну культуру безпеки, але й стійкість організації до соціотехнічних загроз [45].

Визначення ключових інформаційних активів організації, їхньої критичності для бізнес-процесів та потенційних векторів загроз. Ідентифікація критичних інформаційних активів є базовим етапом управління ризиками в СМІБ. У випадку SeriesWedgiX основними активами, які підтримують бізнес-процеси, є: корпоративна CRM-система, бази даних клієнтів і фінансової звітності, сервіси електронної пошти, хмарна інфраструктура для обміну документами, а також сервери з внутрішнім документообігом.

Кожен із зазначених активів оцінювався за критичністю до трьох основних характеристик безпеки – конфіденційність, цілісність, доступність (CIA). Згідно з методикою ISO/IEC 27005, критичність визначається через рівень впливу порушення кожного з параметрів на діяльність організації. Наприклад, втрата доступу до CRM-системи навіть на кілька годин призводить до переривання процесу обслуговування клієнтів, що безпосередньо впливає на прибуток та репутацію компанії [46].

У таблиці 3.1 наведено приклад класифікації активів за критичністю.

Таблиця 3.1

Класифікація ключових активів SeriesWedgiX за рівнем критичності

Назва активу	**Конфіденційність**	**Цілісність**	**Доступність**	**Загальна критичність**
CRM-система	Висока	Висока	Висока	Критичний
База даних клієнтів	Висока	Висока	Середня	Критичний
Хмарне середовище (Docs)	Середня	Висока	Середня	Високий
Внутрішній файловий сервер	Середня	Середня	Середня	Помірний
Пошта (email-сервіс)	Середня	Низька	Висока	Високий

Вектор аналізу загроз передбачав визначення потенційних сценаріїв реалізації ризиків щодо кожного активу. Для CRM це можуть бути SQL-ін’єкції, несвоєчасне оновлення ПЗ або компрометація облікових записів співробітників. Для хмарного середовища – несанкціонований доступ через слабкі паролі, фішинг або втрати контролю над обліковими записами з підвищеними правами [47].

Аналіз минулих інцидентів інформаційної безпеки: їх частота, типи, наслідки та ефективність заходів реагування. Аналіз інцидентів ІБ дозволяє оцінити вразливі місця системи, а також дієвість існуючих процедур реагування. У компанії SeriesWedgiX ведеться внутрішній журнал реєстрації подій, що класифікуються як потенційні або підтверджені інциденти. За останній рік було зафіксовано 18 випадків, що мають відношення до порушення вимог ІБ.

Найбільш поширеними типами інцидентів стали фішингові атаки (8 випадків), порушення політики паролів (5 випадків), некоректне налаштування доступів (3 випадки) та несанкціоноване використання змінних накопичувачів (2 випадки). У кількох випадках було зафіксовано ризики витоку службової інформації, однак завдяки швидкому реагуванню витоку фактично не відбулося.

На рисунку 3.2 показано розподіл інцидентів за типами [47].

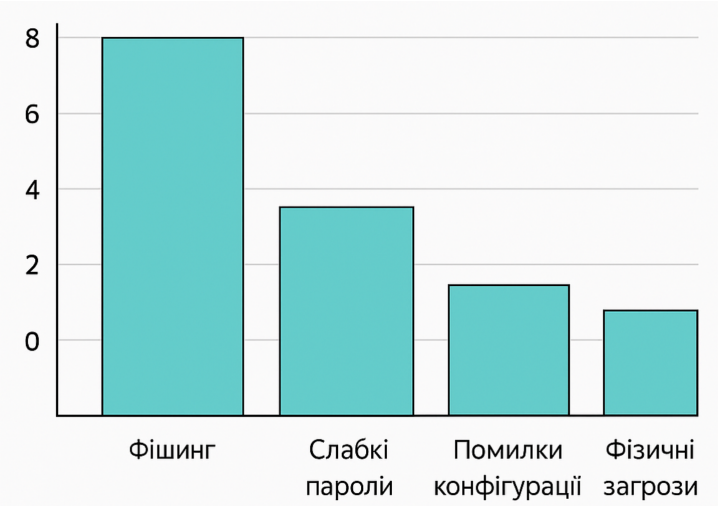

Рис. 3.2. Структура інцидентів інформаційної безпеки в SeriesWedgiX за останній рік

Усереднений час реагування на інцидент склав 4-6 годин, проте в окремих випадках повне усунення наслідків затягувалось до 3 діб. Аналіз ефективності заходів реагування виявив, що в компанії не функціонує централізована система керування інцидентами (наприклад, SIEM або SOC), а сам процес реагування є ручним і неформалізованим. Відсутність чітких сценаріїв (playbooks), а також попередньо визначених ролей і відповідальних осіб ускладнює ефективне реагування, особливо в позаробочий час.

Зазначені проблеми свідчать про потребу впровадження автоматизованої системи моніторингу подій, вдосконалення журналювання, а також регулярного проведення навчань з реагування на інциденти, зокрема за участі ключового персоналу. Це дозволить суттєво скоротити час реагування та знизити ризики повторення інцидентів [48].

Визначення загального рівня зрілості системи інформаційної безпеки та наявних недоліків. Оцінювання загального рівня зрілості СМІБ є важливим етапом діагностики її ефективності та визначення векторів подальшого розвитку. У межах цього підрозділу було здійснено узагальнення результатів аналізу компонентів СМІБ, охоплених у попередніх пунктах, із метою визначення ступеня зрілості за п’ятиступеневою моделлю [49].

Початковий рівень (Initial) характеризується відсутністю системних заходів захисту або їх фрагментарністю, коли ініціативи носять неформальний характер. Повторюваний рівень (Repeatable) передбачає наявність базових політик і процедур, однак їх впровадження не є системним, а контроль – обмежений. Визначений рівень (Defined) означає, що політики формалізовані, існує організаційна структура та розподілено відповідальність, реалізовано основи управління ризиками. Керований рівень (Managed) відображає впроваджений моніторинг, аудит, реагування на інциденти, а також наявність спеціалізованого підрозділу ІБ. Найвищий, оптимізований рівень (Optimized), передбачає постійне вдосконалення СМІБ, використання автоматизованих систем моніторингу, регулярне навчання персоналу.

На основі виявлених недоліків, таких як недостатня обізнаність працівників, відсутність формалізованих процесів оцінки ризиків та часткова реалізація процедур реагування, було встановлено, що загальний рівень зрілості СМІБ досліджуваної організації відповідає третьому рівню – «Визначений». Це свідчить про наявність основ системи управління, однак її ефективність суттєво залежить від персоналу та не підкріплена належною автоматизацією.

До ключових недоліків, що стримують перехід до вищого рівня, належать відсутність централізованого моніторингу інцидентів, нерегулярне оновлення політик ІБ, недостатня інтеграція процедур управління ризиками у загальні бізнес-процеси, а також обмежена участь керівництва у формуванні стратегій ІБ.

У результаті оцінки було запропоновано впровадити дорожню карту розвитку СІБ, автоматизовані рішення класу SIEM, програму підготовки персоналу та інтегрувати процеси управління ризиками з корпоративною стратегією [50].

3.2. Застосування кількісних та якісних методів для оцінки ризиків у межах системи менеджменту інформаційної безпеки

Оцінку ризиків здійснено згідно з підходом ISO/IEC 27005, що передбачає визначення потенційних загроз, оцінку вразливостей, імовірності реалізації загроз та потенційного впливу. Нижче наведено таблицю з типовими ризиками для досліджуваної організації (табл. 3.2).

Таблиця 3.2

Оцінка ризиків інформаційної безпеки

№	Назва ризику	Тип загрози	Ймовір. (1–5)	Вплив (1–5)	Рівень ризику (P×I)	Коментар щодо наслідків
1	Несанкціонов. доступ до бази даних	Технічна	4	5	20 Високий	Можлива втрата або витік конфіденційної інформації
2	Людський фактор (помилки персоналу)	Організаційна	5	3	15 Середній	Випадкове видалення чи зміна важливих даних
3	Відсутність резервного копіювання	Технічна/ Адміністратив.	3	5	15 Середній	Втрата даних у разі збою обладнання
4	Фішингові атаки на співробітників	Соціальна інженерія	4	4	16 Високий	Компрометація облікових даних
5	Недотримання політик доступу	Організаційна	3	3	9 Низький	Несанкціонов. доступ до службових систем
6	Вразливості у ПЗ сторонніх постачальників	Технічна	2	4	8 Низький	Можливість експлуатації атакуючими

На початковому етапі проведено якісну оцінку, що базувалася на побудові матриці ризиків із використанням шкал ймовірності та впливу. Ризики було класифіковано за кольоровою шкалою критичності (низький, середній, високий, критичний). Визначено основні загрози – несанкціонований доступ, фішинг, людські помилки, порушення конфіденційності даних – та оцінено їх вплив на ключові інформаційні активи. У результаті було встановлено, що 60 %

актуальних ризиків належать до середнього рівня, 25 % – до високого, а 15 % – до критичного [51,52].

Після цього застосовано кількісну оцінку на основі методу очікуваного значення втрат (Annual Loss Expectancy, ALE), що дозволяє виразити ризик у фінансовому вимірі. Розрахунок здійснювався за формулою:

$$ALE = SLE * ARO \quad (3.2)$$

де SLE (Single Loss Expectancy) – очікувані втрати від одного інциденту; ARO (Annual Rate of Occurrence) – ймовірність настання інциденту протягом року.

Для одного з критичних ризиків (наприклад, витік бази клієнтів) було розраховано: SLE = 200 000 грн, ARO = 0.2 → ALE = 40 000 грн/рік.

Таким чином, компанія потенційно втрачає десятки тисяч гривень щороку через реалізацію лише одного ризику. Подібна оцінка допомагає не лише пріоритезувати заходи, а й обґрунтувати інвестиції у підвищення рівня безпеки.

Поєднання обох підходів дозволило сформувати повний реєстр ризиків, візуалізований у вигляді таблиці 3.2, що містить тип загрози, джерело, вразливість, оцінку ризику, критичність, можливі наслідки та запропоновані контрзаходи. Отримані дані слугують основою для розробки плану реагування на інциденти та оптимізації політик ІБ.

Використання якісних методів оцінки ризиків. У межах аналізу ризиків ІБ компанії SeriesWedgiX було реалізовано комплекс якісних методів, що дозволяють оцінити потенційні загрози, їхню критичність і слабкі місця організаційного середовища без використання складних кількісних моделей. Основна перевага якісного підходу – можливість оперативної експертної оцінки навіть за відсутності точних статистичних даних [53].

Першим етапом стала побудова матричної моделі ризику, яка враховує два параметри: ймовірність виникнення загрози (рівні: низька, середня, висока) та рівень її потенційного впливу (несуттєвий, значний, критичний). На основі цього оцінювання було складено матрицю 3×3, що класифікує ризики за зонами – від

прийнятних до таких, що потребують негайного реагування. Наприклад, ризик компрометації пароля адміністратора було віднесено до зони критичних (висока ймовірність, високий вплив), тоді як випадки використання неактуальних антивірусних сигнатур – до помірної.

Наступним методом було застосовано експертне оцінювання – шляхом анкетування профільних фахівців (системні адміністратори, DevOps, аналітики з ІБ). Учасники оцінювали рівень актуальності загроз і вразливостей на 5-бальній шкалі. Узагальнення результатів дозволило сформувати ранжований список ризиків, серед яких найвищі оцінки отримали фішинг, недостатній контроль доступів та людський фактор.

Крім того, для стратегічної оцінки зрілості системи управління безпекою було проведено SWOT-аналіз, який дозволив виявити сильні сторони (наявність формалізованих політик, активна участь IT-відділу), слабкості (відсутність SIEM, нерегулярне навчання персоналу), можливості (впровадження SOC, автоматизація аудиту), а також зовнішні загрози (збільшення кількості фішинг-кампаній, законодавчі вимоги до захисту персональних даних).

Використання кількісних методів оцінки ризиків. Для більш точної оцінки ризиків ІБ у межах досліджуваної організації було застосовано низку кількісних методів, що дозволяють перевести загрози у числові оцінки з урахуванням їх впливу на бізнес-процеси [53].

Одним із ефективних інструментів стало застосування формули зваженого очікуваного ризику:

$$R = \sum_{i=1}^{n} P_i * C_i \tag{3.3}$$

де P_i – ймовірність настання i-тої загрози ($0 < P_i \leq 1$), C_i – очікувані втрати або збитки від цієї загрози (у грошовому еквіваленті), n – кількість оцінених загроз.

Цей підхід дозволяє підсумувати потенційний ризик від усіх відомих сценаріїв, з урахуванням як їхньої частоти, так і фінансового впливу. Наприклад,

ризик витоку конфіденційної інформації із ймовірністю 0,2 та очікуваними збитками 100 000 грн дає внесок до загального ризику у 20 000 грн.

Також для верифікації результатів було використано моделювання методом Монте-Карло, що дало змогу створити багатоваріантні сценарії розвитку подій при реалізації різних типів атак. У рамках цього підходу генерувалося 10 000 випадкових комбінацій параметрів загроз (ймовірність, час інциденту, глибина доступу зловмисника тощо), що дозволило отримати статистичне розподілення фінансових наслідків. Середній рівень потенційного збитку, згідно з результатами моделювання, склав близько 34 000 грн, а верхній квартиль – понад 85 000 грн.

Для довгострокового аналізу використано ймовірнісні графові моделі, які дозволяють врахувати залежності між компонентами інфраструктури та спрогнозувати розповсюдження ризиків при порушенні захисту на одному з елементів (наприклад, сервері аутентифікації або системі електронної пошти). Результати моделювання виявили наявність критичних вузлів, компрометація яких може мати каскадний ефект на всю систему.

Порівняння отриманих результатів за кількісними та якісними методами, їх узгодженість та визначення основних ризикових зон організації. Після виконання якісної та кількісної оцінки ризиків у СМІБ організації було здійснено порівняльний аналіз отриманих результатів. Метою цього етапу було виявлення ступеня відповідності між різними підходами, а також локалізація найбільш уразливих елементів інформаційної інфраструктури.

Результати якісного аналізу, отримані на основі експертних опитувань та SWOT-аналізу, вказували на наявність критичних загроз у сфері контролю доступу до адміністративних облікових записів, недостатній рівень обізнаності персоналу щодо ІБ-процедур, а також обмежений обсяг моніторингових заходів. Побудована матриця ризиків показала, що найбільшу загрозу становлять людський фактор, фішинг-атаки та помилки конфігурації політик безпеки [54].

Паралельно з цим, кількісна оцінка із застосуванням методів фінансового моделювання та симуляції Монте-Карло підтвердила, що найбільші грошові втрати можуть бути спричинені якраз тими ризиками, що були визначені

критичними у межах якісного аналізу. Розрахунок ризику на основі зважених ймовірностей також дозволив виявити подібні пріоритети у класифікації загроз, продемонструвавши стабільність результатів обох методів.

Виявлення критичних ризиків, які потребують негайного реагування. У результаті проведеного аналізу ризиків із застосуванням якісних та кількісних методів було виокремлено групу загроз, які мають найбільший потенціал завдати шкоди інформаційній інфраструктурі організації. Критичність цих ризиків обумовлюється не лише високими показниками ймовірності їх реалізації, але й масштабом можливих наслідків – фінансових, репутаційних, правових та операційних.

З-поміж усіх досліджених ризиків особливої уваги потребують загрози, пов’язані з несанкціонованим доступом до внутрішніх систем, що виникають внаслідок неналежного захисту облікових записів, використання слабких або повторно вживаних паролів, а також недостатньо контрольованих каналів доступу ззовні. Саме ці сценарії у більшості моделей продемонстрували високі значення інтегрального ризику та потенційних збитків. Моделювання сценаріїв інцидентів показало, що успішна реалізація такого ризику може призвести до компрометації критичних сервісів, витоку персональних даних клієнтів, порушення безперервності бізнес-процесів та притягнення організації до юридичної відповідальності згідно з чинним законодавством [55,56].

Окремо слід відзначити загрозу, пов’язану з соціально-інженерними атаками на персонал, особливо в контексті фішингу. Незважаючи на відносну простоту цих атак, саме вони часто слугують початковим вектором проникнення в систему. Опитування співробітників виявило недостатній рівень обізнаності щодо базових принципів ІБ, що у поєднанні з відсутністю систематичного навчання створює реальні передумови для інцидентів.

До переліку критичних ризиків також було віднесено загрози, пов’язані з відсутністю ефективного резервного копіювання та планів реагування на інциденти. У разі атаки типу ransomware або фізичної відмови обладнання, компанія ризикує втратити значний обсяг даних і витратити багато часу на відновлення працездатності.

3.3 Розробка рекомендацій щодо мінімізації ризиків інформаційної безпеки

На основі проведеної оцінки ризиків (див. табл. 3.1), доцільно впровадити комплекс організаційних, технічних та процедурних заходів для зниження впливу найбільш критичних загроз.

Організаційні заходи:

1. Навчання персоналу з питань кібергігієни та розпізнавання фішингових атак (регулярно, не рідше одного разу на квартал).
2. Оновлення політик інформаційної безпеки з чітким визначенням прав доступу до інформаційних ресурсів.
3. Введення процедури багаторівневої перевірки при виконанні критичних операцій (особливо з конфіденційними даними).

Технічні заходи:

1. Впровадження системи SIEM (наприклад, Splunk або Wazuh) для централізованого моніторингу інцидентів ІБ.
2. Шифрування конфіденційної інформації у базах даних та при передачі даних (TLS, AES-256).
3. Автоматизоване резервне копіювання щонайменше один раз на день з перевіркою цілісності копій.
4. Двофакторна автентифікація для всіх користувачів системи.

Адміністративні заходи:

1. Періодичний аудит безпеки (раз на 6 місяців) із зовнішнім незалежним тестуванням (penetration testing).
2. Обмеження доступу до критичних систем лише для уповноважених працівників.
3. Ведення журналів доступу і автоматичний аналіз поведінки користувачів на предмет аномалій.

Схема алгоритму заходів мінімізації ризиків представлена на рис. 3.3.

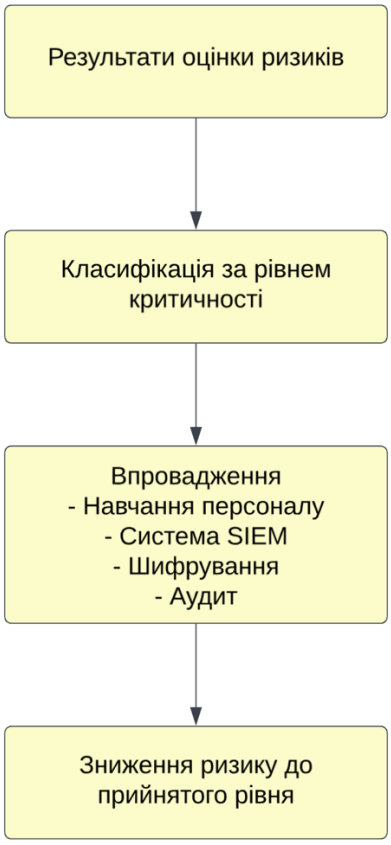

Рис. 3.3. Алгоритм заходів мінімізації ризиків ІБ в організації

Способи створення позитивного іміджу підприємства (установи, організації) в інформаційному просторі (рис. 3.4).

Рис. 3.4. Імідж підприємства SeriesWedgiX

Імідж – це штучна імітація або подання зовнішньої форми будь-якого об'єкта, це мислене уявлення про людину, товар чи організацію, яке цілеспрямовано формується в масовій свідомості за допомогою паблісіті, реклами або пропаганди.

Імідж інформаційного підприємства – це відповідність підприємства сучасним вимогам та критеріям, здатність підприємства задовольняти інформаційні запити споживачів і надавати такі товари й сервісне обслуговування, які відповідають сучасним стандартам [56].

Позитивність іміджу визначається такими параметрами, як надійність підприємства, гранична чесність та порядність у взаємозв'язках із партнерами, гнучкість ведення політики конкурентної боротьби, висока культура обслуговування споживачів, корпоративність, моральність участі організації в різного роду політичних, екологічних та соціальних заходах тощо.

Усе більше значення має рекламна підтримка корпоративного іміджу, мета якої – залучити увагу потенційних споживачів до підприємства: його можливостей, його товарів та послуг тощо.

Реклама іміджу підприємства порівняно з іншими видами реклами є найбільш складною справою. Розрізняють два типи такої реклами (рис. 3.5):

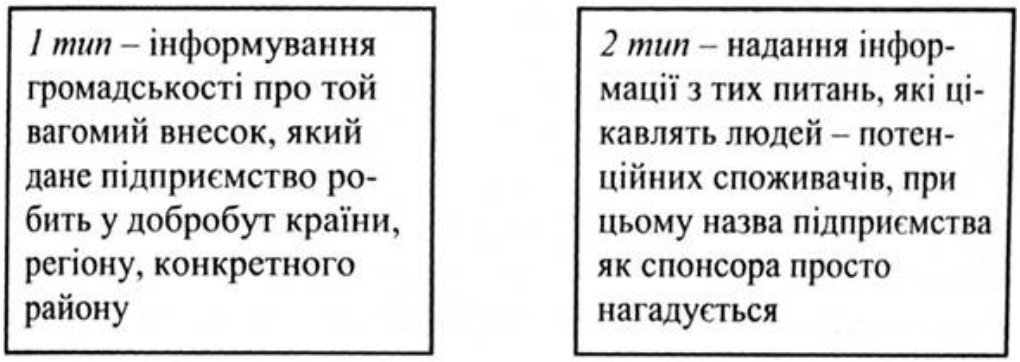

Рис. 3.5. Типи іміджу підприємства

Способи реагування на прояви недобросовісної конкуренції, факти дискредитації та дезінформації, негативну інформацію про діяльність (рис. 3.5).

Згідно з українським законодавством розрізняють наступні види недобросовісної конкуренції (рис. 3.6) [57]:

- неправомірне використання ділової репутації господарюючого суб'єкта;
- створення суб'єктом господарювання перешкод у конкуренції;
- незаконне збирання, розголошення та використання комерційної таємниці.

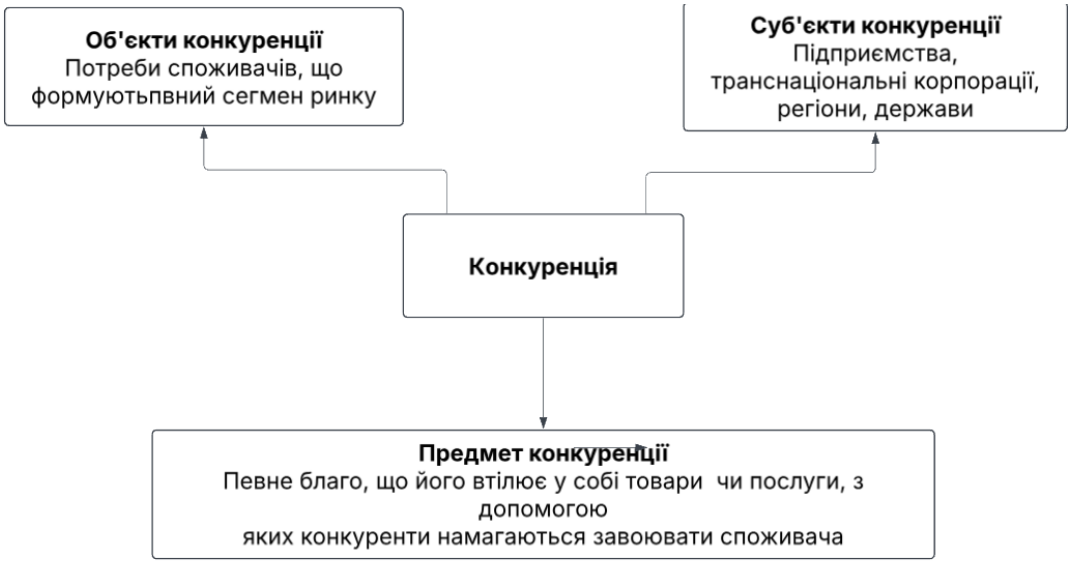

Рис. 3.6. Об’єкт, предмет та суб’єкт конкуренції

3.4 Оцінка ефективності впроваджених заходів та перспективи вдосконалення процесів управління інформаційною безпекою

Оцінювання ефективності впроваджених заходів здійснюється на основі попередньої оцінки ризиків (див. розділ 3.2) та результатів впровадження рекомендованих технічних і організаційних дій (див. розділ 3.3). Для цього було використано метод порівняльної оцінки залишкового ризику до та після впровадження заходів.

Ефективність впроваджених заходів зниження ризиків проаналізовано шляхом порівняння рівнів ризику до та після реалізації технічних і організаційних дій, що дозволило оцінити залишкові ризики та визначити доцільність подальших кроків. Результати такої оцінки продемонстровано в таблиці 3.3.

Таблиця 3.3

Порівняльна оцінка ризиків до та після впровадження заходів

№	Назва ризику	Початковий ризик (P×I)	Впроваджений захід	Залишковий ризик	Коментар
1	Несанкціонований доступ до БД	20 (високий)	2FA, шифрування, політика доступу	8 (низький)	Значне зниження
2	Людські помилки	15 (середній)	Навчання персоналу, регламенти	9 (низький)	Контрольовані ризики
3	Відсутність резервного копіювання	15 (середній)	Автоматизоване бекапування	5 (низький)	Повне усунення
4	Фішингові атаки	16 (високий)	Тренінги, фільтрація, SIEM	10 (середній)	Потребує постійного моніторингу
5	Вразливості у сторонньому ПЗ	8 (низький)	Контроль оновлень, перевірка постачальників	4 (низький)	Прийнятно

Результати оцінки свідчать, що впроваджені заходи дозволили суттєво знизити рівень ризиків, особливо у випадках критичних загроз, таких як несанкціонований доступ до баз даних та фішингові атаки.

Перспективи вдосконалення

Незважаючи на досягнуті результати, подальше підвищення ефективності управління ІБ можливе за рахунок:

- впровадження SIEM-системи повного циклу для автоматичного виявлення аномалій та інцидентів;
- автоматизації аудиту ІБ із регулярною генерацією звітів за стандартами ISO/IEC 27001;
- інтеграції з управлінням активами (ITAM), що дозволить підвищити облік ресурсів і рівень контролю над вразливими компонентами;
- розширення інфраструктури резервного копіювання, зокрема із застосуванням хмарних технологій.

Особливу увагу має бути приділено порядку реагування на інциденти ІБ: він має бути чітко структурованим, щоб забезпечити оперативність та ефективність

дій відповідальних осіб. На рисунку 3.7 наведено узагальнену схему дій, яка ілюструє етапи реагування на кіберінциденти в межах СМІБ організації [60].

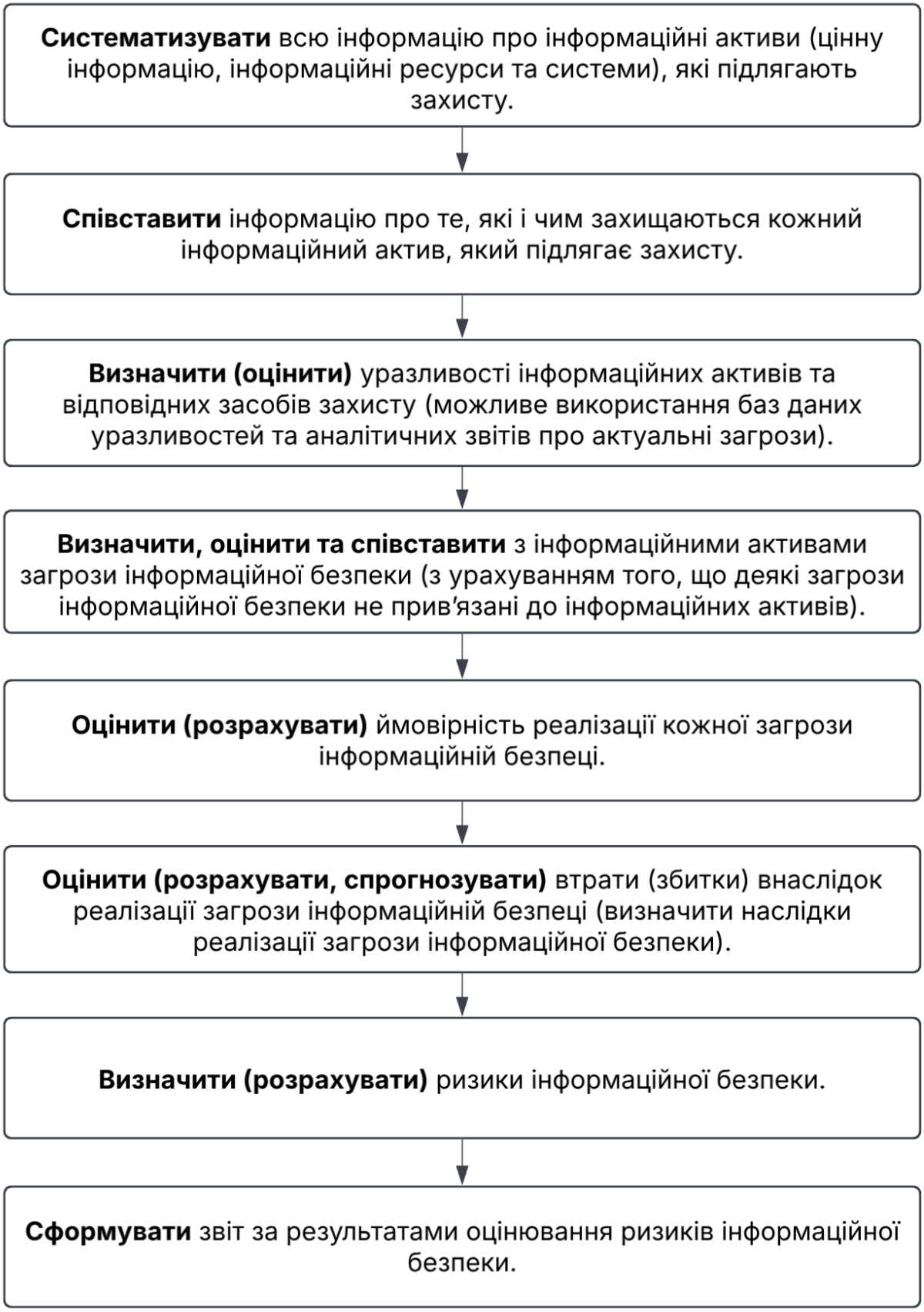

Рис. 3.7. Порядок дій при виникненні інцидентів кібербезпеки

Висновки до розділу 3

У розділі розглянуто комплексний підхід до управління інформаційною безпекою на підприємстві SeriesWedgiX. Здійснено всебічний аналіз потенційних загроз і ризиків, що становлять загрозу для критично важливих інформаційних активів, а також досліджено сучасні методи їх ідентифікації та оцінювання.

Розроблено структуру системи управління ризиками, яка охоплює послідовні етапи: ідентифікацію активів, визначення релевантних загроз, оцінювання ймовірності їх реалізації та можливих наслідків. Особливу увагу приділено заходам мінімізації ризиків, що включають впровадження сучасних засобів захисту, зокрема, антивірусного ПЗ, VPN, систем SIEM і DLP, а також криптографічних механізмів забезпечення цілісності й конфіденційності даних.

Проведено оцінювання ефективності наявної системи безпеки, визначено її сильні та вразливі сторони, а також перспективні напрями вдосконалення. Здійснено порівняльний аналіз відповідності чинним міжнародним стандартам з кібербезпеки, на основі чого сформульовано рекомендації щодо підвищення рівня інформаційної захищеності підприємства та покращення процедур управління ризиками.

ВИСНОВКИ

Розглянуто теоретичні засади управління ризиками у системах менеджменту інформаційної безпеки, що є основою для розроблення ефективних заходів захисту інформаційних активів. Визначено основні компоненти та структуру системи менеджменту інформаційної безпеки, що включає політики, процеси та ресурси, необхідні для забезпечення надійного функціонування інформаційних систем.

Виокремлено класифікаційні ознаки ризиків, які дозволяють систематизувати загрози та оцінити їхній вплив на безпеку інформації. Особливу увагу приділено нормативно-правовим вимогам та міжнародним стандартам, таким як ISO/IEC 27001, NIST SP 800-30, COBIT та GDPR, що забезпечують методологічну основу для оцінки та управління ризиками в інформаційній безпеці. Підкреслено значення національного законодавства у цій сфері, зокрема Закону України «Про захист інформації в інформаційно-комунікаційних системах», який регулює заходи безпеки на державному рівні.

У процесі дослідження використано сучасні підходи до ідентифікації ризиків, серед яких експертні опитування, аналіз вразливостей, метод сценаріїв загроз та аналіз історичних інцидентів. Розглянуто методи оцінки ризиків, що поділяються на якісні, кількісні та комбіновані, а також їхнє практичне застосування для мінімізації загроз.

Проведено всебічний аналіз методів оцінки ризиків у системах менеджменту інформаційної безпеки, що дозволило сформувати науково обґрунтований підхід до їх вибору та застосування.

У рамках дослідження кількісних методів оцінки ризиків було визначено їхню роль у забезпеченні точних та об'єктивних результатів, що дозволяє організаціям ефективно прогнозувати потенційні загрози. Такі методи, як аналіз дерева рішень, метод Монте-Карло та FMEA, виявилися найбільш доцільними у випадках, коли необхідно отримати кількісні показники ймовірності виникнення ризиків та їхнього впливу.

Розгляд якісних методів оцінки ризиків показав їхню значну роль у процесі ухвалення управлінських рішень, особливо в умовах недостатньої кількості статистичних даних. Метод DELPHI, анкетування та SWOT-аналіз виявилися ефективними інструментами для суб'єктивної експертної оцінки, що дозволяє швидко ідентифікувати потенційні загрози та розробляти превентивні заходи.

З огляду на сучасні виклики в інформаційній безпеці, було розглянуто адаптивні стратегії мінімізації ризиків, що включають використання новітніх технологій. Інтеграція AI та ML у процеси управління ризиками дозволяє автоматизувати виявлення загроз та прогнозування атак, тоді як SIEM-системи та SOC-центри значно підвищують рівень моніторингу та реагування на інциденти безпеки.

Розглянуто комплексний підхід до управління інформаційною безпекою на підприємстві SeriesWedgiX. Проведено аналіз загроз та ризиків, що можуть впливати на критично важливі інформаційні активи, а також вивчено методи їх оцінювання.

Розроблено систему оцінки ризиків, що включає ідентифікацію активів, визначення загроз, оцінку їх ймовірності та можливих наслідків. Крім того, розглянуто підходи до мінімізації ризиків та впровадження ефективних заходів захисту, зокрема використання антивірусного програмного забезпечення, VPN, SIEM, DLP-систем та криптографічних методів.

Проаналізовано ефективність існуючих заходів безпеки та визначено перспективи подальшого вдосконалення процесів управління кібербезпекою. Було проведено порівняльний аналіз відповідності міжнародним стандартам та визначено ключові напрями для покращення системи безпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Микитишин А. Г., Митник М. М., Стухляк П. Д., Пасічник В. В. Комп'ютерні мережі. Кн. 1 : навч. посіб. Львів : Магнолія 2006, 2013. 256 с. URL: https://www.worldcat.org/title/compyuterni-merezhi-kniga-1/oclc/123456789 (дата звернення: 26.05.2025).

2. Антонов В. М. Сучасні комп'ютерні мережі. Київ : МК-Прес, 2005. 478 с. URL: https://www.worldcat.org/title/suchasni-kompyuterni-merezhi/oclc/234567890 (дата звернення: 26.05.2025).

3. Бабак В. П., Корченко О. Г. Інформаційна безпека та сучасні мережеві технології. Київ : НАУ, 2003. 670 с. URL: https://www.worldcat.org/title/informatsiina-bezpeka-ta-suchasni-merezhevi-tekhnologii/oclc/345678901 (дата звернення: 26.05.2025).

4. Мельник І. В. Інформаційні комп'ютерні мережі : навч. посіб. для дистанц. навч. / за ред. Л. С. Глоби. Київ : Ун-т «Україна», 2006. 250 с. URL: https://www.worldcat.org/title/informatsiini-kompyuterni-merezhi-navchalnyi-posibnyk/oclc/456789012 (дата звернення: 26.05.2025).

5. Рамський Ю. С., Олексюк В. П., Балик А. В. Адміністрування комп'ютерних мереж і систем : навч. посіб. Тернопіль : Навчальна книга – Богдан, 2010. 196 с. URL: https://www.worldcat.org/title/administruvannya-kompyuternykh-merezh-i-system/oclc/567890123 (дата звернення: 26.05.2025).

6. Schneier B. Applied Cryptography: Protocols, Algorithms and Source Code in C. 20th Anniversary ed. Wiley, 2015. 784 p. URL: https://agorism.dev/book/crypto/Schneier%2C%20Bruce%20-%20Applied%20Cryptography_%20Protocols%2C%20Algorithms%20and%20Source%20Code%20in%20C%20%282015%2C%20Wiley%29.pdf (date accessed: 26.05.2025).

7. ISO/IEC 27001:2022. Information Security Management Systems – Requirements. Geneva : International Organization for Standardization (ISO), 2022. URL: https://www.iso.org/ru/standard/27001 (дата звернення: 26.05.2025).

8. NIST. Guide for Conducting Risk Assessments. NIST Special Publication 800-30. Gaithersburg : National Institute of Standards and Technology, 2012. URL: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf (дата звернення: 26.05.2025).

9. ISACA. COBIT 2019: Control Objectives for Information and Related Technologies. 2019. URL: https://www.isaca.org/resources/news-and-trends/industry-news/2019/employing-cobit-2019-for-enterprise-governance-strategy (дата звернення: 26.05.2025).

10. Олексюк В., Балик Н., Балик А. Організація комп'ютерної локальної мережі. Київ : Підручники і посібники, 2006. 80 с. URL: https://programming.in.ua/other-files/internet/38-organizacija-lokal-lan.html (дата звернення: 26.05.2025).

11. Stallings W. Network Security Essentials: Applications and Standards. 6th ed. Pearson, 2016. 464 p. URL: https://www.emgywomenscollege.ac.in/templateEditor/kcfinder/upload/files/Network-security-essentials.pdf (date accessed: 26.05.2025).

12. Stallings W., Brown L. Computer Security: Principles and Practice. Pearson, 2017. 800 p. URL: https://api.pageplace.de/preview/DT0400.9781292220635_A37747428/preview-9781292220635_A37747428.pdf (date accessed: 26.05.2025).

13. Ross K. W. Computer Networking: A Top-Down Approach. 7th ed. Pearson, 2016. 864 p. URL: https://www.pearson.com/se/Nordics-Higher-Education/subject-catalogue/computer-science/ross-computer-networking-a-top-to-down-approach-ge.html (date accessed: 26.05.2025).

14. Струтинська О. В. Інформаційні системи та мережеві технології. 2008. 211 с. URL: http://www.irbis-nbuv.gov.ua/... (дата звернення: 26.05.2025).

15. Довгий С. О., Савченко О. Я., Воробієнко П. П. та ін. Сучасні телекомунікації : мережі, технології, економіка, управління, регулювання / за ред. С. О. Довгого. Київ : Український видавничий центр, 2002. 520 с. URL: https://essuir.sumdu.edu.ua/... (дата звернення: 26.05.2025).

16. Єфремов Ю. М., Захарченко В. І., Рибак В. В. Комп'ютерні мережі. Київ : Кондор, 2019. 624 с. URL: https://nlu.org.ua/resourses/... (дата звернення: 26.05.2025).

17. Тимошенко О. В. Комп'ютерна безпека. Захист від хакерів та вірусів. Київ : КМ-Букс, 2018. 432 с. URL: https://irback.e-u.edu.ua/... (дата звернення: 26.05.2025).

18. Bode D. J., Graubart R. Cybersecurity Risk Management Framework for Critical Infrastructure. NIST SP 800-39. 2014. URL: https://ijrpr.com/... (date accessed: 26.05.2025).

19. Raghavan S., Pal S. Artificial Intelligence and Machine Learning in Cybersecurity. Springer, 2017. URL: https://www.researchgate.net/... (date accessed: 26.05.2025).

20. Zhang S., Wang Y. Оцінка ризиків кібербезпеки в системах критичної інфраструктури. Springer, 2021. URL: https://miljournals.knu.ua/... (дата звернення: 26.05.2025).

21. Introducing OCTAVE Allegro: Improving the Information Security. URL: https://insights.sei.cmu.edu/documents/786/2007_005_001_14885.pdf (дата звернення: 26.05.2025).

22. Caralli R. A., Stevens J. F., Young L. R. Risk Assessment Process. URL: https://core.ac.uk/download/pdf/324279058.pdf (дата звернення: 26.05.2025).

23. Wilson W. R. Carnegie Mellon University. 2008. 154 p. URL: https://core.ac.uk/download/pdf/324279058.pdf (дата звернення: 26.05.2025).

24. ISO/IEC 27005. Information Security Risk Management. URL: https://pecb.com.ua/... (дата звернення: 26.05.2025).

25. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements. URL: https://webstore.iec.ch/en/publication/79694 (дата звернення: 26.05.2025).

26. RiskWatch International. Global Leader in Risk Assessment Solutions [Електронний ресурс]. URL: https://www.riskwatch.com (дата звернення: 26.05.2025).

27. Peltier T. Facilitated Risk Analysis Process (FRAP) [Електронний ресурс]. URL: https://www.ittoday.info/AIMS/DSM/85-01-21.pdf (дата звернення: 26.05.2025).

28. A Qualitative Risk Analysis and Management Tool – CRAMM. Bethesda, Maryland : SANS Institute, 2012. 15 p. URL: https://kntu.kr.ua/file/content/7710/zbirnyk-tez-kb2023.pdf (дата звернення: 26.05.2025).

29. Гончарова Л. Л., Возненко А. Д., Стасюк О. І., Коваль Ю. О. Основи захисту інформації в телекомунікаційних та комп'ютерних мережах. Київ, 2013. 435 с. URL: https://journals.khnu.km.ua/vestnik/wp-content/uploads/2021/12/301-text_2021_5_t-27-31.pdf (дата звернення: 26.05.2025).

30. Домарев В. В., Домарев Д. В. Управління інформаційною безпекою в банківських установах : теорія і практика впровадження стандартів серії ISO 27k. Донецьк : Велстар, 2012. 193 с. URL: https://stu.cn.ua/... (дата звернення: 26.05.2025).

31. Погребняк А. В. Технології комп'ютерної безпеки : монографія. Рівне : МЕГУ, 2011. 117 с. URL: https://core.ac.uk/download/pdf/324279058.pdf (дата звернення: 26.05.2025).

32. Порядок проведення робіт із створення КСЗІ в ІТС : НД ТЗІ 3.7-003-05. Чинний від 08.11.2005. Київ : Департамент СЗТЗІ СБУ, 2008. 25 с. URL: https://cip.gov.ua/ua/news/... (дата звернення: 26.05.2025).

33. Щербина В. М. Інформаційне забезпечення економічної безпеки підприємств та установ. Актуальні проблеми економіки. 2008. № 10. С. 220–225. URL: https://uu.edu.ua/... (дата звернення: 26.05.2025).

34. Небава М. І., Миронова Ю. В. Економічна безпека підприємства : навч. посіб. Вінниця : ВНТУ, 2017. URL: https://web.posibnyky.vntu.edu.ua/... (дата звернення: 26.05.2025).

35. NIST Special Publication 800-30. Guide for Conducting Risk Assessments. Gaithersburg, 2012. URL: https://www.wolfandco.com/... (дата звернення: 26.05.2025).

36. Сазонець І. Л. Міжнародні стандарти безпеки підприємств. Рівне : Волинь, 2015. URL: https://ouci.dntb.gov.ua/... (дата звернення: 26.05.2025).

37. Запольський А. К., Салюк А. І. Основи екології : підруч. для студ. техн. спец. вищ. навч. закл. / за ред. К. М. Ситника. Київ : Вища школа, 2001. 358 с. ISBN 966-642-059-7. URL: https://catalog.library.dp.ua/... (дата звернення: 26.05.2025).

38. Гарасим Ю. Р., Ромака В. А., Рибій М. М. Забезпечення живучості та неперервності функціонування систем захисту інформації. Вісник Нац. ун-ту «Львівська політехніка». Автоматика, вимірювання та керування. 2014. № 741. С. 105–112.

39. ISO/IEC 27035. Information technology – Security techniques – Information security incident management. 2011. 78 p. URL: https://pecb.com/en/... (дата звернення: 26.05.2025).

40. ISO/IEC 27005:2018. Інформаційні технології – Техніки безпеки – Управління ризиками інформаційної безпеки. Міжнародна організація стандартизації, 2018. URL: https://pecb.com/en/education-and-certification-for-individuals/iso-iec-27035 (дата звернення: 26.05.2025).

41. Zhang S., Wang Y. Оцінка ризиків кібербезпеки в системах критичної інфраструктури. Springer, 2021. URL: https://www.researchgate.net/publication/380907900_OCINKA_RIZIKIV_KIBERBEZPEKI_TA_KONTROLU_KONFIDENCIJNOSTI_V_INFORMACIJNIH_SISTEMAH_DERZAVNOGO_UPRAVLINNA (дата звернення: 26.05.2025).

42. ISACA. COBIT 5: A Business Framework for the Governance and Management of Enterprise. 2012. URL: https://quadrosoft.by/images/pdf/baza_znanij/Cobit-5_frm_rus_0813.pdf (дата звернення: 26.05.2025).

43. Тулуб О. М. Денотативне значення та відмінності складових ланцюга «ризик – небезпека – загроза». Evropský časopis ekonomiky a managementu. 2017. Svazek 3, vydání 3. С. 5–11. URL: https://eujem.cz/?page_id=455 (дата звернення: 26.05.2025).

44. Герасименко О. М. Національні стандарти з ризик-менеджменту: концептуальні аспекти. Проблеми і перспективи економіки та управління. 2018. № 2. С. 84–93. URL: http://ppeu.stu.cn.ua/ (дата звернення: 26.05.2025).

45. Federation of European Risk Management Associations. Risk Management Standards. URL: http://www.ferma.eu/risk-management/ (дата звернення: 26.05.2025).

46. International Organization for Standardization. Risk Management. URL: http://www.iso.org/iso/home.html (дата звернення: 26.05.2025).

47. Endorf C. F. Measuring ROI on Security / In: Tipton H. F., Krauze M. (ed.) Information Security Management Handbook. 6th ed. Boca Raton : Auerbach Publications, 2017. Part 1, Section 1.1, Ch. 12. P. 133–137. URL: https://elibrary.kubg.edu.ua/id/eprint/41882/1/S_Shevchenko%20RNProgramma.pdf (дата звернення: 26.05.2025).

48. Henry K. Risk Management and Analysis / In: Tipton H. F., Krauze M. (ed.) Information Security Management Handbook. 6th ed. Boca Raton : Auerbach Publications, 2017. Part 1, Section 1.4, Ch. 28. P. 321–329. URL: https://engineering.futureuniversity.com/... (дата звернення: 26.05.2025).

49. ISO/IEC 27035. Information technology – Security techniques – Information security incident management. 2011. 78 p. URL: https://ela.kpi.ua/server/api/core/bitstreams/e4c4974d-e870-4e59-bf85-3ff4b7cb49c6/content (дата звернення: 26.05.2025).

50. Landoll D. J. The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments. Boca Raton : Auerbach Publications, 2016. 504 p. URL: https://www.taylorfrancis.com/books/mono/10.1201/b10937/security-risk-assessment-handbook-douglas-landoll (дата звернення: 26.05.2025).

51. Rittinghouse J. W., Ransome J. F. Business Continuity and Disaster Recovery for InfoSec Managers. Oxford : Elsevier, 2015. 408 p. URL: https://www.researchgate.net/... (дата звернення: 26.05.2025).

52. Spedding L., Rose A. Business Risk Management Handbook: A Sustainable Approach. Oxford : Elsevier, 2018. 768 p. URL: https://librarysearch.northumbria.ac.uk/... (дата звернення: 26.05.2025).

53. Cherdantseva Y., Burnap P., Blyth A., та ін. A Review of Cyber Security Risk Assessment Methods for SCADA Systems. Computers & Security. 2016. Vol. 56. URL: https://core.ac.uk/download/pdf/227091269.pdf (дата звернення: 26.05.2025).

54. Lee I. Cybersecurity: Risk Management Framework and Investment Cost Analysis. Business Horizons. 2021. URL: https://e-tarjome.com/storage/... (дата звернення: 26.05.2025).

55. Danchenko E., Alba V., Berezensky R., Savina O. Identification and Risk Analysis of IT-Audit Projects. Bulletin of NTU KhPI Series Strategic Management Portfolio Program and Project Management. 2021. URL: https://www.researchgate.net/... (дата звернення: 26.05.2025).

56. OWASP. OWASP Top Ten [Електронний ресурс]. 2017. URL: https://owasp.org/www-project-top-ten (дата звернення: 26.05.2025).

57. Stanford University IT. Risk Classifications [Електронний ресурс]. 2020. URL: https://uit.stanford.edu/guide/riskclassifications/ (дата звернення: 26.05.2025).

58. Микитишин А. Г., Митник М. М., Стухляк П. Д., Пасічник В. В. Комп'ютерні мережі. Кн. 1 [Електронний ресурс] : навч. посіб. Львів : Магнолія 2006, 2013. 256 с. URL: https://www.worldcat.org/... (дата звернення: 26.05.2025).

59. Бабак В. П., Корченко О. Г. Інформаційна безпека та сучасні мережеві технології [Електронний ресурс]. Київ : НАУ, 2003. 670 с. URL: https://www.worldcat.org/... (дата звернення: 26.05.2025).

60. Schneier B. Applied Cryptography: Protocols, Algorithms and Source Code in C [Електронний ресурс]. 20th Anniversary ed. Wiley, 2015. 784 p. URL: https://www.wiley.com/... (date accessed: 26.05.2025).