Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

Лади Михайла Романовича

на здобуття ступеня вищої освіти Бакалавра

Система управління ризиками інформаційної безпеки на основі експертних оцінок

Галузь знань 12 – Інформаційні технології
Спеціальність 125 – Кібербезпека
Освітня програма Кібербезпека

Шифр КРБКБ.220244.22.02.30 ПЗ

Виконав студент 4 курсу група КБ-22-2 Михайло ЛАДА
Керівник канд. техн. наук, доцент Віра ТІТОВА
Нормоконтролер д-р філософії Наталія ПЕТЛЯК

До захисту допускаю:
Завідувач кафедри кібербезпеки Юрій КЛЬОЦ

8 06 2026 р.

Хмельницький 2026

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформаційних технологій

Кафедра Кібербезпеки

Рівень вищої освіти Бакалавр

Галузь знань 12 – Інформаційні технології

Спеціальність 125 – Кібербезпека

Освітня програма Кібербезпека

ЗАТВЕРДЖУЮ

Завідувач кафедри кібербезпеки

Юрій КЛЬОЦ

9 січня 2026 р.

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Ладі Михайлу Романовичу

1 Тема роботи Система управління ризиками інформаційної безпеки на основі експертних оцінок

Керівник роботи канд. техн. наук, доцент Тітова Віра Юріївна

Затверджено на засіданні кафедри Кібербезпеки 8 січня 2026 № 7

2 Строк подання студентом кваліфікаційної роботи на кафедру _____

3 Вихідні дані до роботи Аналіз методів оцінювання захищеності, розробка математичної моделі обробки експертних оцінок та програмна реалізація системи управління ризиками інформаційної безпеки.

4 Зміст пояснювальної записки

Аналіз методів управління ризиками та обґрунтування моделі експертного оцінювання. Побудова математичного алгоритму агрегування думок експертів. Програмна реалізація системи на базі Python/Flask та тестування її функціональних можливостей..

5 Перелік графічного матеріалу (із зазначенням обов'язкових креслень)

«Алгоритм експертного оцінювання кіберризиків за методом Делфі». «Архітектура та взаємодія компонентів системи оцінювання кіберризиків».«Алгоритм комплексного аналізу та класифікації ризиків інформаційних активів».

6 Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7 Дата видачі завдання 12 січня 2026 р.

КАЛЕНДАРНИЙ ПЛАН

Назва етапів (розділів) кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
Вибір і затвердження теми кваліфікаційної роботи	лютий	
Ознайомлення з предметною областю	лютий	
Дослідження існуючих рішень	лютий	
Постановка задачі	березень	
Визначення загальних принципів рішення задачі	березень	
Деталізація принципів рішення задачі	квітень	
Розробка проєктних рішень	квітень	
Апробація проєктних рішень	травень	
Оформлення пояснювальної записки згідно вимог	травень	
Оформлення графічної частини	червень	
Захист КР	червень	

Студент _____ Михайло ЛАДА

Керівник кваліфікаційної роботи _____ Віра ТІТОВА

ABSTRACT

Subject of qualification work: Information security risk management system based on expert assessments.

Author: Lada Mykhailo Romanovych.

Head of work: Associate Professor Titova Vira Yuriivna.

Explanatory note: 76 pages, 2 appendices, 7 figures, 8 tables, 45 references.

Graphic part: 3 posters.

Keywords: risk management, information security, expert assessments, risk analysis, automated system, threat assessment, risk map, cybersecurity, decision support.

The bachelor's qualification work is devoted to the information security risk management process using an expert-based approach. The work analyzes modern risk assessment methods, the ISO/IEC 27000 series standards, and NIST recommendations. The main drawbacks of existing approaches are identified, which relate to the subjectivity of expert opinions, the complexity of their consensus building, and the insufficient automation of the risk analysis process.

An information security risk management system that provides automated collection, processing, and analysis of expert assessments has been designed. A mechanism for factoring in the experts' competence level during the integration risk index calculation, as well as algorithms for checking assessment consistency, have been implemented. The system's output includes the generation of a risk map and practical recommendations for responding to information security threats. The proposed solution allows for increasing the accuracy of risk evaluation, reducing the impact of the human factor, and accelerating the decision-making process in the field of information protection.

18.05.2026 _____

АНОТАЦІЯ

Тема кваліфікаційної роботи: Система управління ризиками інформаційної безпеки на основі експертних оцінок.

Автор роботи: Лада Михайло Романович

Керівник роботи: канд. техн. наук, доцент Тітова Віра Юріївна.

Пояснювальна записка: 76 сторінок, 2 додатки, 7 рисунків, 8 таблиць,45 джерел.

Графічна частина: 3 плакати.

Ключові слова: управління ризиками, інформаційна безпека, експертні оцінки, аналіз ризиків, автоматизована система, оцінювання загроз, карта ризиків, кібербезпека, підтримка прийняття рішень.

У кваліфікаційній роботі розглянуто процес управління ризиками інформаційної безпеки з використанням експертного підходу. Проведено аналіз сучасних методів оцінювання ризиків, стандартів серії ISO/IEC 27000 та рекомендацій NIST. Визначено основні недоліки існуючих підходів, пов'язані із суб'єктивністю експертних оцінок, складністю їх узгодження та недостатньою автоматизацією процесу аналізу ризиків.

У роботі спроектовано систему управління ризиками інформаційної безпеки, яка забезпечує автоматизований збір, обробку та аналіз експертних оцінок. Реалізовано механізм врахування компетентності експертів під час розрахунку інтегрального показника ризику та алгоритми перевірки узгодженості оцінок. Результатом роботи системи є формування карти ризиків і рекомендацій щодо реагування на загрози інформаційній безпеці. Запропоноване рішення дозволяє підвищити точність оцінювання ризиків, зменшити вплив людського чинника та прискорити процес прийняття рішень у сфері захисту інформації.

18.05.2026 _____

ЗМІСТ

ВСТУП

Актуальність цієї теми зумовлена глибокими змінами, які сьогодні відбуваються у світовій економіці та системі державного управління під впливом цифровізації. Активне впровадження хмарних сервісів, технологій великих даних і систем штучного інтелекту відкриває нові можливості для розвитку організацій, однак одночасно підвищує їхню вразливість до сучасних кіберзагроз[1].

У таких умовах інформаційна безпека вже давно перестала бути лише технічним завданням IT-відділів. Вона перетворилася на один із ключових чинників стабільного функціонування та розвитку будь-якої організації. Особливої актуальності це питання набуває через постійне зростання кількості цілеспрямованих кібератак і деструктивних впливів на критичну інфраструктуру[2]. Традиційні підходи до забезпечення безпеки, що ґрунтуються переважно на реагуванні після виникнення інцидентів, уже не можуть гарантувати належний рівень захисту. Сучасні умови потребують переходу до проактивних стратегій, основою яких є системне управління ризиками[3]. Водночас процес виявлення та оцінювання ризиків ускладнюється високим рівнем невизначеності. Організації часто не мають достатньої статистичної інформації про попередні інциденти, а нові види загроз виникають настільки швидко, що класичні математичні методи не дозволяють ефективно їх оцінити.

У зв’язку з цим особливого значення набуває використання експертних оцінок, які дають змогу врахувати практичний досвід фахівців, специфіку діяльності організації та приховані чинники, що не завжди можуть бути виявлені автоматизованими засобами аналізу[4]. Однак значна роль людського чинника створює проблему суб’єктивності, оскільки оцінки різних експертів можуть відрізнятися залежно від їхнього досвіду, компетентності чи особистого бачення ситуації.

Саме тому виникає потреба у створенні спеціалізованих автоматизованих систем, здатних інтелектуально обробляти інформацію, узагальнювати експертні судження та зменшувати вплив когнітивних упереджень під час прийняття рішень у сфері інформаційної безпеки. Створення такого інструментарію дає змогу

підвищити об’єктивність оцінювання ризиків, що, своєю чергою, дозволяє керівництву організації більш ефективно розподіляти ресурси та оптимізувати витрати на забезпечення інформаційної безпеки, концентруючи увагу на найбільш критичних напрямах захисту.

Об’єктом проєктування є автоматизовані системи управління ризиками інформаційної безпеки в сучасних організаціях. Предметом проєктування виступає архітектура, програмні модулі та математичні алгоритми агрегування експертних суджень у складі веб-орієнтованої системи оцінювання ризиків.

Метою роботи є проєктування та програмна реалізація системи управління ризиками, яка автоматизує процеси збирання, обробки та аналізу експертної інформації з метою визначення пріоритетних напрямів захисту інформаційних активів. Для досягнення поставленої мети у роботі вирішуються такі інженерні та практичні завдання:

- проведення аналізу теоретичних засад і міжнародних стандартів управління ризиками інформаційної безпеки, зокрема ISO/IEC 27005 та NIST[5];
- порівняльний аналіз існуючих програмних аналогів та обґрунтування вибору технологічного стеку розробки;
- розробка математичного алгоритму агрегування та перевірки узгодженості експертних оцінок з метою зменшення впливу суб’єктивних чинників;
- проєктування архітектури програмної системи, реалізація її функціональних модулів (серверної логіки, клієнтського інтерфейсу) та проведення тестування;
- розгортання системи та оцінювання її працездатності в умовах виконання практичних тестових сценаріїв.

Методологічну основу розробки становлять принципи системного аналізу, теорія прийняття рішень, алгоритми математичної статистики та сучасні підходи до проєктування програмного забезпечення .

Практичне значення отриманих результатів полягає у створенні готового програмного продукту, який може бути використаний службами інформаційної безпеки для проведення регулярного аудиту, моніторингу та оцінювання ризиків. Запропоноване рішення сприяє підвищенню рівня кібербезпеки організації,

забезпечує більш обґрунтоване прийняття управлінських рішень і підвищує загальну стійкість підприємства до сучасних кіберзагроз.

Важливою перевагою запропонованої системи є можливість адаптації до специфіки діяльності різних організацій та галузей. Завдяки модульній архітектурі система може бути інтегрована у вже існуючу інфраструктуру інформаційної безпеки підприємства та доповнюватися новими механізмами аналізу й оцінювання ризиків. Зменшення впливу людського фактору дозволяє уникнути випадкових помилок під час розрахунків. У підсумку підприємство отримує надійний інструмент, який допомагає захистити бізнес від фінансових та репутаційних втрат через кібератаки. Це забезпечує гнучкість використання програмного продукту та дозволяє враховувати зміни у характері кіберзагроз, нормативно-правових вимогах і внутрішніх політиках безпеки організації.

Крім того, впровадження автоматизованої системи підтримки експертного оцінювання сприяє підвищенню оперативності прийняття рішень у сфері інформаційної безпеки. Автоматизація процесів збору, обробки та аналізу даних дозволяє значно скоротити час проведення оцінювання ризиків, зменшити ймовірність помилок та забезпечити більш високий рівень достовірності результатів. У результаті організація отримує ефективний інструмент для своєчасного реагування на потенційні загрози та формування стратегій захисту інформаційних ресурсів в умовах постійної трансформації цифрового середовища.

1 ОГЛЯД ПРЕДМЕТНОЇ ОБЛАСТІ ТА ПОСТАНОВКА ЗАДАЧІ

1.1 Управління ризиками інформаційної безпеки: сутність, основні поняття та підходи

У сучасному цифровому суспільстві інформація є одним із найцінніших ресурсів будь-якої організації. Вона виступає основою для прийняття управлінських рішень, забезпечення конкурентоспроможності та ефективного функціонування бізнес-процесів. Разом із цим зростає і кількість загроз, пов’язаних із її збереженням, обробкою та передачею. Саме тому управління ризиками інформаційної безпеки стає ключовим елементом загальної системи безпеки організації. Інформаційна безпека визначається як стан захищеності інформації, за якого забезпечуються її основні властивості: конфіденційність, цілісність та доступність[6].

- конфіденційність полягає у забезпеченні доступу до даних лише тим суб’єктам (користувачам, процесам), які мають на це законні права. Порушення конфіденційності призводить до несанкціонованого розголошення інформації, що є критичним для персональних даних або комерційної таємниці[7].

- цілісність передбачає захист інформації від несанкціонованої або випадкової зміни чи знищення. Це гарантує, що дані залишаються точними, повними та достовірними протягом усього циклу їхньої обробки та зберігання.

- доступність характеризує можливість отримання інформації та використання необхідних сервісів авторизованими користувачами у будь-який потрібний їм час. Мова йде про стійкість систем до відмов обладнання або DoS-атак.

Порушення хоча б однієї з цих властивостей призводить до виникнення інцидентів безпеки, що можуть спричинити фінансові втрати, репутаційні ризики або навіть зупинку діяльності організації. Ризик інформаційної безпеки є ймовірністю реалізації певної загрози, яка використовує наявні вразливості системи та призводить до негативних наслідків. У загальному вигляді ризик можна розглядати як функцію трьох складових: активу, загрози та вразливості. Активи - це інформаційні ресурси, програмне забезпечення, апаратні засоби, а також

людські ресурси, що мають цінність для організації. Загрози - це потенційні події або дії, які можуть завдати шкоди активам. Вразливості - це слабкі місця в системі, які можуть бути використані для реалізації загроз. Управління ризиками інформаційної безпеки являє собою систематичний процес виявлення, аналізу, оцінювання та мінімізації ризиків з метою зниження їх впливу до прийнятного рівня.

Цей процес є безперервним і повинен бути інтегрований у загальну систему управління організацією. Для більш детального розуміння структури ризику інформаційної безпеки доцільно розглянути основні складові, що формують його сутність, а також їх характеристики та взаємозв'язки. Систематизація цих елементів дозволяє спростити процес аналізу ризиків і підвищити ефективність їх оцінювання. З цією метою узагальнену характеристику основних складових ризику інформаційної безпеки наведено в таблиці 1.1.

Таблиця 1.1 - Характеристика компонентів ризику інформаційної безпеки

Складова	Опис	Приклад
Актив	Будь-який ресурс (матеріальний чи цифровий), що має цінність для організації та її бізнес-процесів.	База даних клієнтів, фінансова звітність, програмний код.
Загроза	Потенційна подія, дія або обставина, яка у разі реалізації здатна завдати шкоди інформаційним активам.	Хакерська атака (SQL-ін'єкція), вірусне ПЗ, стихійне лихо.
Вразливість	Слабке місце в системі, архітектурі, фізичному захисті чи процедурах управління, яке може бути використане загрозою.	Слабкий пароль адміністратора, відсутність двохфакторної автентифікації.
Ризик	Ймовірність того, що конкретна загроза успішно використає наявну вразливість, призводячи до негативних наслідків.	Витік персональних даних через несанкціонований доступ.

Управління ризиками інформаційної безпеки являє собою систематичний процес виявлення, аналізу, оцінювання та мінімізації ризиків з метою зниження їх впливу до прийнятного рівня. Цей процес включає послідовне виконання

взаємопов’язаних етапів, кожен з яких спрямований на забезпечення ефективного контролю та зниження рівня ризиків. Основними етапами управління ризиками є:

- ідентифікація ризиків. На цьому етапі визначаються всі можливі загрози, вразливості та активи, що можуть бути піддані ризику. Ідентифікація включає аналіз внутрішніх і зовнішніх факторів, таких як технічні збої, людський фактор, кібератаки, природні катастрофи тощо. Результатом є перелік потенційних ризиків.
- аналіз ризиків. Аналіз передбачає визначення причин виникнення ризиків та оцінку їх характеристик. Він може бути якісним або кількісним. Якісний аналіз базується на експертних оцінках і дозволяє класифікувати ризики за рівнями (високий, середній, низький). Кількісний аналіз використовує математичні моделі та статистичні дані для точнішого визначення рівня ризику;
- оцінювання ризиків. На цьому етапі визначається пріоритетність ризиків шляхом порівняння їх рівнів із заданими критеріями прийнятності. Це дозволяє визначити, які ризики потребують першочергового реагування;
- обробка ризиків. Обробка ризиків передбачає вибір і реалізацію заходів щодо їх зниження. Основні стратегії включають: уникнення ризику, зниження ризику, передача ризику та прийняття ризику;
- моніторинг та контроль. Цей етап передбачає постійне спостереження за станом ризиків і ефективністю впроваджених заходів. У разі змін у середовищі або появи нових загроз проводиться повторна оцінка ризиків.

Існують різні підходи до управління ризиками інформаційної безпеки. Одним із них є процесний підхід, який розглядає управління ризиками як безперервний цикл, інтегрований у всі бізнес-процеси організації[8]. Такий підхід дозволяє забезпечити системність і узгодженість дій.

Системний підхід передбачає розгляд інформаційної безпеки як комплексної системи, де всі елементи взаємопов’язані. Це дозволяє враховувати вплив змін в одній частині системи на інші її складові. Ризик-орієнтований підхід базується на принципі пріоритетності - основна увага приділяється найбільш критичним ризикам.

Також важливим є використання міжнародних стандартів у сфері управління ризиками, зокрема серії стандартів ISO/IEC 27000. Вони визначають загальні

принципи, підходи та рекомендації щодо побудови системи управління інформаційною безпекою[9]. Особливу роль у процесі управління ризиками відіграє людський фактор. Помилки персоналу, недостатня обізнаність або навмисні дії можуть стати причиною реалізації загроз. Тому важливим є проведення навчання, підвищення кваліфікації та формування культури інформаційної безпеки. Таким чином, управління ризиками інформаційної безпеки є складним багаторівневим процесом, що включає ідентифікацію, аналіз, оцінювання та мінімізацію ризиків. Його ефективна реалізація дозволяє забезпечити надійний захист інформаційних ресурсів, знизити ймовірність виникнення інцидентів та мінімізувати їх наслідки.

Особливу, а часто і вирішальну роль у процесі управління ризиками відіграє людський фактор, який є найбільш динамічним та найменш прогнозованим елементом системи. Помилки персоналу, недостатня обізнаність щодо актуальних методів соціальної інженерії або навмисні зловмисні дії можуть стати причиною успішної реалізації загрози навіть за наявності досконалих технічних засобів захисту[10]. Саме тому критично важливим є проведення регулярного навчання, підвищення кваліфікації та формування зрілої культури інформаційної безпеки всередині колективу.

Управління ризиками інформаційної безпеки в сучасному розумінні є складним багаторівневим процесом, що потребує поєднання математичної точності та глибокого експертного розуміння бізнес-контексту. Своєчасна ідентифікація, глибокий аналіз та стратегічно правильна мінімізація ризиків дозволяють не лише знизити ймовірність виникнення інцидентів, а й гарантувати стійкість організації до зовнішніх та внутрішніх впливів.

Для досягнення цієї мети необхідно впроваджувати автоматизовані інструменти аналізу, які допомагають оперативно обробляти великі обсяги безпекових даних. Використання таких рішень дозволяє мінімізувати суб'єктивні чинники та підвищити точність прогнозів. У результаті керівництво отримує надійне підґрунтя для прийняття стратегічних рішень для бюджету на кіберзахист.

1.2 Використання експертних оцінок у задачах аналізу ризиків інформаційної безпеки

У процесі управління ризиками інформаційної безпеки важливе місце займає оцінювання ризиків, яке дозволяє визначити їх рівень, пріоритетність та необхідність впровадження захисних заходів. Однак у багатьох випадках отримання точних кількісних даних є складним або неможливим через невизначеність, відсутність статистики або унікальність інформаційних систем. У таких умовах доцільним є використання експертних оцінок. Експертні оцінки являють собою метод отримання інформації на основі знань, досвіду та інтуїції фахівців у певній предметній області.

Вони широко застосовуються в задачах аналізу ризиків, де необхідно оцінити ймовірність реалізації загроз, рівень вразливостей або можливі наслідки інцидентів інформаційної безпеки. Основною перевагою експертних оцінок є можливість врахування якісних факторів, які важко формалізувати або виміряти кількісно. До таких факторів належать рівень підготовки персоналу, організаційна культура безпеки, складність інформаційної інфраструктури та інші аспекти, що впливають на загальний рівень ризику[11].

Процес отримання експертних оцінок зазвичай включає декілька етапів: формування групи експертів, розробку анкети або методики опитування, проведення оцінювання та обробку отриманих результатів. Важливо також зазначити, що ефективність методів отримання експертних оцінок значною мірою залежить від правильної організації процесу опитування та подальшої обробки результатів. Зокрема, значну роль відіграє чітке формулювання критеріїв оцінювання, які повинні бути зрозумілими та однозначними для всіх експертів. Це дозволяє зменшити рівень неоднозначності у відповідях та підвищити порівнюваність отриманих результатів[12].

Крім того, важливим є використання стандартизованих шкал оцінювання, наприклад бальної або лінгвістичної, що забезпечує можливість подальшого математичного опрацювання даних. Додатковим аспектом є необхідність контролю узгодженості експертних оцінок, оскільки значні розбіжності між думками

експертів можуть свідчити про недостатню визначеність предметної області або різний рівень компетентності учасників. У таких випадках доцільним є повторне проведення оцінювання або застосування додаткових методів узгодження результатів, що дозволяє підвищити їх достовірність та обґрунтованість. Це допомагає отримати максимально точні та об'єктивні фінальні результати, на які можна впевнено спиратися при захисті системи.

Таблиця 1.2 - Основні методи отримання експертних оцінок

Метод	Опис та процедура	Головні переваги	Основні недоліки
Анкетування	Індивідуальне заповнення експертами опитувальних листів.	Висока швидкість та простота організації процесу.	Високий рівень суб’єктивізму та ризик помилок.
Колективне обговорення	Спільний пошук рішення групою фахівців у форматі дискусії.	Можливість генерації нових ідей та узгодженість думок.	Психологічний тиск та вплив авторитетних учасників.
Метод Делфі	Багатоетапне анонімне опитування з аналітичною обробкою.	Відсутність впливу групи, висока достовірність результатів.	Складність організації та великі часові витрати.
Зважене оцінювання	Розрахунок результату з урахуванням ваги (досвіду) кожного експерта.	Підвищена об’єктивність за рахунок пріоритету знань.	Необхідність розробки критеріїв оцінки самих експертів.

Як видно з таблиці 1.2, існує кілька підходів до отримання експертних оцінок, кожен з яких має свої переваги та недоліки. Вибір конкретного методу залежить від характеру задачі, доступності експертів та вимог до точності результатів.

Особливе місце серед існуючих підходів займає метод Делфі, який базується на принципах багатоетапного анонімного опитування експертів із обов’язковим наданням їм узагальнених результатів попередніх раундів для ознайомлення. Така ітераційна процедура дозволяє фахівцям переглянути власні позиції у світлі аргументів колег, що суттєво зменшує вплив деструктивних суб’єктивних факторів

та допомагає досягти високого рівня узгодженості думок без прямого психологічного тиску всередині групи[13].

Результати експертного оцінювання на початкових етапах зазвичай мають якісний характер і подаються у вигляді лінгвістичних шкал, наприклад: низький, середній або високий рівень ризику. Для забезпечення можливості подальшого аналізу такі якісні оцінки підлягають формалізації та перетворенню у числові значення, що відкриває шлях до застосування потужного математичного апарату статистики та методів інтелектуальної обробки даних[14].

Поряд із очевидними перевагами, експертні оцінки як інструмент аналізу мають і певні системні недоліки. До них традиційно відносять суб'єктивність сприйняття, ризики прихованої упередженості, можливість домінування авторитету окремих лідерів думок, а також високу складність верифікації достовірності отриманих результатів у реальному часі. Саме тому критично важливо застосовувати комплексні методи підвищення об'єктивності, до яких належать повна анонімність опитування, залучення зовнішніх незалежних експертів, які не мають власних інтересів всередині організації, та глибока статистична обробка результатів для виявлення аномальних відхилень.

У процесі практичного застосування експертних оцінок ключовим фактором успіху є не лише вибір конкретного методу їх отримання, а й сувора організація всієї процедури оцінювання. Якість кінцевого аналітичного продукту безпосередньо залежить від логічної послідовності виконання етапів, глибини підготовки експертної групи та методологічної коректності обробки зібраних даних. Зазвичай цей процес охоплює підготовчий етап, де чітко формулюються цілі дослідження, розробляються критерії оцінювання та проводиться верифікація кандидатів у експертну групу.

Наступний, основний етап, передбачає безпосередню взаємодію з фахівцями для отримання їхніх суджень щодо ймовірності реалізації загроз та оцінки вразливостей системи. Завершальний етап присвячений обробці та інтелектуальному узагальненню результатів із використанням алгоритмів агрегування, що мінімізує вплив людського фактора та максимізує обґрунтованість підсумкових оцінок. Таким чином, процедура експертного оцінювання постає як

складна, багатоступенева технологія, що забезпечує необхідну достовірність аналізу ризиків інформаційної безпеки, особливо в умовах дефіциту точних статистичних даних. Для кращого розуміння архітектури цієї процедури, її узагальнену структурно-логічну схему доцільно подати у вигляді рисунка 1.2. Ця схема наочно демонструє послідовність дій та взаємозв'язок між усіма кроками оцінювання. Завдяки такому підходу користувач може чітко простежити, як саме формуються фінальні висновки безпеки.

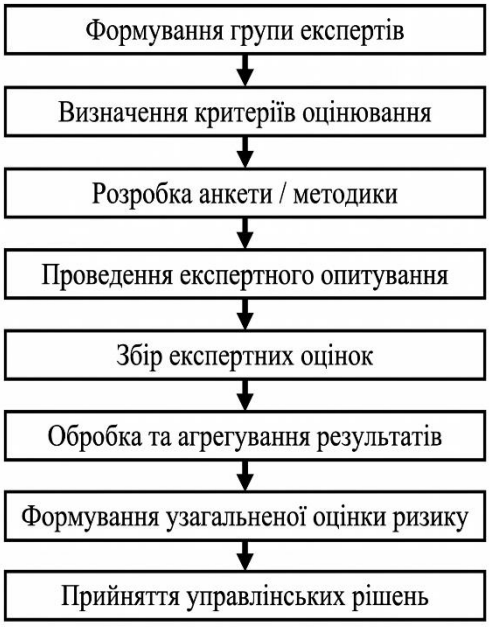


Рисунок 1.2 – Схема експертної оцінки ризиків

Як видно з рисунка, процес експертного оцінювання ризиків інформаційної безпеки є чітко структурованим і включає послідовність взаємопов’язаних етапів. Кожен із цих етапів виконує окрему функцію та впливає на кінцеву якість отриманих результатів. Початкові етапи забезпечують підготовку вихідних даних та організацію процесу оцінювання, зокрема формування групи експертів, визначення критеріїв та розробку інструментів збору інформації.

Важливим аспектом, який визначає спроможність усієї системи експертного оцінювання, є об’єктивне визначення рівня компетентності фахівців, залучених до аналізу. У науковій практиці компетентність розглядається не лише як сукупність теоретичних знань, а й як здатність фахівця надавати достовірну інформацію в умовах високої невизначеності. Для підвищення точності результатів доцільно впроваджувати багаторівневу перевірку кожного експерта.

По-перше, оцінюється професійний бекграунд, що включає стаж роботи в галузі інформаційної безпеки, досвід роботи з конкретними класами інформаційних систем (наприклад, банківськими чи промисловими), а також наявність міжнародних сертифікатів, які підтверджують кваліфікацію на глобальному рівні. По-друге, значну роль відіграє коефіцієнт самооцінки, коли фахівець самостійно визначає ступінь своєї обізнаності у вузьких питаннях, таких як криптографічний захист, хмарна безпека або протидія соціальній інженерії. Такий комбінований підхід дозволяє впровадити механізм пріоритетності знань, де думка експерта з більшим досвідом у конкретному питанні має вагоміше значення для підсумкового результату[15].

Окрім оцінки компетенцій, критичною фазою є забезпечення узгодженості думок. Навіть група висококваліфікованих фахівців може продемонструвати значний розкид оцінок через різне бачення внутрішніх пріоритетів організації. Проблема розбіжностей часто виникає через різну спеціалізацію: системний адміністратор може фокусуватися на технічних збоях, тоді як менеджер з безпеки - на ризиках витоку конфіденційних даних.

Для розв'язання цієї проблеми в автоматизованих системах використовуються методи логічного порівняння. Якщо думки експертів щодо конкретного ризику занадто сильно розходяться, система повинна ініціювати процедуру перегляду оцінок. Це не обов’язково означає помилку - навпаки, «окрема думка» одного фахівця може вказувати на приховану вразливість, яку проігнорувала більшість. Тому інтелектуальна обробка даних повинна бути спрямована на виявлення причин таких відхилень, а не на їх автоматичне видалення[16].

Також варто приділити увагу психологічним аспектам, що виникають під час групової роботи. Навіть при анонімному опитуванні існує ризик когнітивних упереджень, таких як «ефект недавніх подій» (коли експерт переоцінює загрозу лише тому, що нещодавно читав про неї в новинах) або надмірна самовпевненість. Мінімізація цих факторів досягається шляхом правильної побудови опитувальних листів, де питання формулюються максимально нейтрально та конкретно, виключаючи можливість подвійного тлумачення.

Підсумовуючи, можна стверджувати, що ефективне управління ризиками сьогодні неможливе без поєднання людської інтуїції та системного підходу до обробки даних. Експертні оцінки перетворюють розрізнені думки фахівців на структурований фундамент для побудови комплексної системи захисту. Саме цей синергетичний підхід - де людина визначає контекст, а система забезпечує об'єктивність аналізу - стає основою для розробки сучасних інструментів кібербезпеки, що розглядаються у даному дослідженні.

Основний етап передбачає безпосереднє проведення експертного оцінювання, під час якого формується первинна інформація щодо рівня загроз, вразливостей та можливих наслідків реалізації ризиків. Важливо, що на цьому етапі значною мірою проявляється суб'єктивний характер оцінок, тому особливого значення набуває правильний підбір експертів та використання формалізованих методик збору даних.

Завершальні етапи процесу спрямовані на обробку та узагальнення отриманих результатів. Застосування методів агрегування дозволяє зменшити вплив індивідуальних думок експертів і сформувати більш об'єктивну інтегральну оцінку ризику. Отримані результати використовуються для подальшого аналізу рівня інформаційної безпеки та підтримки прийняття управлінських рішень.

Таким чином, представлена схема дозволяє наочно відобразити логіку та послідовність проведення експертного оцінювання, що є важливим елементом у системі аналізу ризиків інформаційної безпеки. Її використання забезпечує більш структурований підхід до оцінювання та підвищує обґрунтованість отриманих результатів, що є що є критично важливим при розробці та впровадженні систем управління ризиками, оскільки дозволяє мінімізувати вплив суб'єктивних чинників.

Завдяки автоматизації розрахунків на фінальній стадії, аналітики можуть оперативно коригувати вхідні дані при зміні ландшафту кіберзагроз. Це перетворює статичну оцінку на динамічний процес безперервного контролю стану захищеності компанії. Зрештою, підприємство отримує прозорий механізм прогнозування збитків, який дозволяє оптимізувати витрати на купівлю технічних засобів захисту інфраструктури.

1.3 Аналіз існуючих методів і систем управління ризиками

У сучасних умовах цифрової трансформації суспільства та стрімкого розвитку інформаційних технологій питання забезпечення інформаційної безпеки набуває особливої актуальності. Постійне ускладнення інформаційних систем, розширення мережевої інфраструктури, використання хмарних сервісів, мобільних платформ та технологій Інтернету речей призводять до суттєвого зростання кількості потенційних вразливостей. У таких умовах управління ризиками інформаційної безпеки стає не лише допоміжною функцією, а ключовим елементом загальної системи управління організацією.

- ISO/IEC 27005 є частиною сімейства стандартів ISO 27000. Його ключова філософія полягає в циклічності. Цей стандарт не пропонує конкретної математичної моделі, але встановлює жорсткі рамки того, що має бути зроблено на кожному етапі: від встановлення контексту до прийняття залишкового ризику[3];
- NIST Risk Management Framework (RMF) (зокрема спеціальні публікації SP 800-37 та SP 800-30) орієнтований на інтеграцію безпеки в життєвий цикл розробки систем (SDLC). Цей підхід вважається одним із найбільш деталізованих у світі, оскільки він пов’язує управління ризиками безпосередньо з технічними контролями та постійним моніторингом[17];
- OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) розроблений в університеті Карнегі-Меллон. На відміну від техніко-центричних підходів, OCTAVE фокусується на організаційних активах та експертних знаннях персоналу. Це робить його ідеальним для організацій, де людський фактор та внутрішні процеси є критичними[18].

Дані методики передбачають формалізований процес управління ризиками, який включає ідентифікацію активів, загроз і вразливостей, оцінювання рівня ризиків, а також визначення заходів реагування. Їх основною перевагою є структурованість та відповідність міжнародним вимогам у сфері інформаційної безпеки. Зазначені методології відрізняються не лише підходами до організації процесу управління ризиками.

Варто зауважити, що сучасний ландшафт кіберзагроз, який характеризується появою вразливостей нульового дня та складними цілеспрямованими атаками , вимагає перегляду традиційних підходів. Сучасні системи управління ризиками все частіше відходять від концепції періодичного оцінювання (наприклад, раз на рік) на користь безперервного моніторингу.

Ефективність обраного підходу до управління ризиками значною мірою визначається його адаптивністю до внутрішніх бізнес-процесів організації. На сьогоднішній день не існує єдиної «універсальної» методики, яка була б однаково ефективною для державного сектору, великих промислових об’єктів та малого бізнесу. Кожна з існуючих стратегій має свій унікальний вектор спрямованості: від жорсткої нормативної регламентації до гнучкого експертного прогнозування. Це створює перед фахівцями з інформаційної безпеки складну задачу вибору оптимального інструментарію, який повинен балансувати між точністю отриманих результатів та витратами ресурсів на їх досягнення.

Вибір конкретної методології управління ризиками у сучасних умовах базується на аналізі трьох ключових параметрів:

- складність IT-ландшафту: для гетерогенних мереж із великою кількістю хмарних сервісів та віддалених робочих місць необхідні стандарти з детальним технічним контролем.

- регуляторні вимоги: наявність специфічних законодавчих норм у певних галузях (наприклад, банківська таємниця або захист критичної інфраструктури) часто робить використання міжнародних стандартів, таких як ISO/IEC 27005, обов'язковим елементом комплаєнсу.

- доступність експертного капіталу: якщо організація володіє штатом досвідчених аналітиків, доцільним стає використання методологій типу OCTAVE, що базуються на глибокій внутрішній самооцінці, тоді як за умови дефіциту кадрів перевага надається автоматизованим рішенням.

Важливо підкреслити, що сучасна концепція «динамічного ризику» вимагає від організацій відмови від статичних звітів, які готуються раз на рік. Замість цього відбувається перехід до інтегрованих систем, де результати оцінювання ризиків безпосередньо впливають на налаштування засобів захисту. Це дозволяє реагувати

на зміни в профілі загрози в режимі реального часу, що є критично важливим для підтримки актуального стану захищеності в умовах стрімкої еволюції кіберзагроз.

Різноманітність методологій визначає не лише порядок дій, а й набір інструментів, що будуть задіяні для збору та аналізу інформації. Для великих організацій доцільним є використання максимально формалізованих підходів, що дозволяють мінімізувати вплив «людського фактора», тоді як для невеликих підприємств більш ефективними виявляються спрощені або адаптовані методики, що не потребують значних фінансових вкладень. З метою порівняльного аналізу ключових характеристик, переваг та обмежень найбільш відомих світових підходів, основні дані узагальнено у наступній таблиці[19].

Таблиця 1.3 - Порівняльна характеристика методів управління ризиками

Методологія	Основні характеристики	Переваги	Недоліки
ISO/IEC 27005	Інтеграція в систему управління ІБ	Стандартизованість, універсальність	Складність впровадження
NIST RMF	Життєвий цикл управління ризиками	Деталізований підхід, контроль процесів	Висока ресурсомісткість
OCTAVE	Орієнтація на експертні оцінки	Гнучкість, незалежність	Суб’єктивність оцінок
GRC-системи	Автоматизоване управління ризиками	Автоматизація, централізація	Висока вартість, складне налаштування

Як видно з таблиці 1.3, кожна з розглянутих методологій має свої переваги та недоліки, що визначають доцільність її застосування залежно від умов функціонування організації. Вибір конкретного підходу повинен здійснюватися з урахуванням ресурсів, рівня складності інформаційної системи та вимог до забезпечення інформаційної безпеки.

Методологія ISO/IEC 27005 орієнтована на інтеграцію процесів управління ризиками у загальну систему менеджменту інформаційної безпеки організації. Вона передбачає безперервний процес ідентифікації, аналізу, оцінювання та перегляду ризиків із урахуванням змін у внутрішньому та зовнішньому середовищі

функціонування. Особливістю даного підходу є його тісний зв’язок із іншими стандартами серії ISO/IEC 27000, що забезпечує комплексність і узгодженість управління інформаційною безпекою. Підхід NIST Risk Management Framework, у свою чергу, акцентує увагу на життєвому циклі інформаційних систем та включає етапи класифікації систем, вибору засобів захисту, їх впровадження, оцінювання ефективності та подальшого моніторингу. Методологія OCTAVE відрізняється тим, що значну увагу приділяє організаційним аспектам та залученню експертів безпосередньо всередині компанії, що забезпечує гнучкість, але може призводити до підвищення суб’єктивності оцінок.

Узагальнена оцінка ризику розраховується за формулою:

$$R = P * I, \tag{1.1}$$

де R - рівень ризику;

P - ймовірність реалізації загрози;

I - величина можливих збитків або впливу.

Застосування даного підходу дозволяє формалізувати процес оцінювання ризиків та забезпечити можливість їх кількісного порівняння.

Методи управління ризиками інформаційної безпеки можна класифікувати за рядом ознак, що дозволяє систематизувати існуючі підходи та обґрунтувати вибір найбільш доцільного з них залежно від специфіки діяльності організації, цінності її інформаційних активів. Зокрема, виділяють такі основні класифікаційні групи:

- за способом оцінювання: якісні, кількісні та комбіновані;
- за рівнем формалізації: формалізовані та неформалізовані;
- за ступенем автоматизації: ручні та автоматизовані;
- за джерелом отримання даних: статистичні та експертні.

Така класифікація дозволяє більш чітко визначити особливості кожного підходу та оцінити можливості їх застосування в конкретних умовах. Зокрема, кількісні методи забезпечують більшу точність, однак потребують наявності достовірних даних, тоді як якісні методи є більш гнучкими та широко

використовуються в умовах невизначеності. Незважаючи на широкий вибір існуючих методів і систем управління ризиками, більшість із них мають певні обмеження. Вони можуть бути складними, вимагати ресурсів або недостатньо враховувати специфіку конкретної організації. Крім того, формалізовані підходи не завжди ефективно враховують експертні знання та якісні характеристики ризиків.

Таким чином, аналіз існуючих методів і систем управління ризиками свідчить про необхідність поєднання формалізованих підходів із використанням експертних оцінок, що дозволяє підвищити точність оцінювання ризиків. Крім того, важливим є врахування специфіки конкретної організації та адаптація методів оцінювання до змін у зовнішньому та внутрішньому середовищі, що забезпечує більш гнучке та ефективне управління ризиками інформаційної безпеки. Водночас доцільним є впровадження сучасних автоматизованих систем моніторингу, які дозволяють оперативно виявляти нові загрози та підвищувати швидкість реагування на інциденти.

Сучасні тенденції розвитку систем управління ризиками свідчать про поступовий перехід від статичних моделей оцінювання до адаптивних та динамічних підходів. Це зумовлено тим, що традиційні методології, такі як ISO/IEC 27005 або NIST RMF, хоча й забезпечують високу структурованість процесу, не завжди дозволяють оперативно реагувати на швидкі зміни кіберзагроз. У результаті виникає потреба у впровадженні гібридних моделей, які поєднують формалізовані стандарти з елементами автоматизованого аналізу даних у режимі реального часу[20].

Важливою складовою сучасних систем управління ризиками є використання засобів аналітики великих даних (Big Data) та технологій машинного навчання. Такі підходи дозволяють виявляти приховані закономірності у поведінці користувачів та мережевому трафіку, що значно підвищує точність прогнозування потенційних загроз. Крім того, інтеграція з системами моніторингу безпеки (SIEM-рішеннями) забезпечує можливість безперервного збору та аналізу подій, що відбуваються в інформаційній інфраструктурі організації.

Окремо слід зазначити, що значна частина сучасних організацій переходить до концепції ризик-орієнтованого управління безпекою, де основний акцент

робиться не лише на виявленні загроз, але й на оцінюванні їхнього впливу на бізнес-процеси. Такий підхід дозволяє більш ефективно розподіляти ресурси на заходи захисту та зосереджуватися на найбільш критичних активів організації. У цьому контексті ризик розглядається не лише як технічна, але й як економічна категорія, що безпосередньо впливає на прийняття управлінських рішень.

Також важливим напрямом розвитку є автоматизація процесів оцінювання ризиків. Використання програмних засобів дозволяє зменшити вплив людського фактору, підвищити швидкість обробки даних та забезпечити більш об’єктивні результати. Автоматизовані системи можуть інтегруватися з існуючою інфраструктурою організації та виконувати постійний моніторинг стану інформаційної безпеки, що є критично важливим в умовах сучасного динамічного кіберсередовища. Додатково це сприяє своєчасному виявленню відхилень у рівні захищеності та оперативному реагуванню на потенційні інциденти.

Таким чином, можна зробити висновок, що розвиток методів управління ризиками інформаційної безпеки рухається у напрямі поєднання класичних міжнародних стандартів із сучасними технологіями автоматизації та аналітики даних. Це дозволяє підвищити ефективність виявлення, оцінювання та мінімізації ризиків, а також забезпечити більш високий рівень захисту інформаційних систем у цілому. Водночас це створює передумови для подальшої інтеграції інтелектуальних систем підтримки прийняття рішень у сфері кібербезпеки.

1.4 Постановка задачі

На основі проведеного аналізу сучасних підходів до управління ризиками інформаційної безпеки, а також вивчення міжнародних стандартів серії ISO та NIST, можна зробити висновок, що більшість організацій стикається з проблемою практичного застосування існуючих методик оцінювання ризиків. Сучасні кіберзагрози постійно змінюються: регулярно з’являються нові вразливості, поширюються фішингові атаки, активно використовуються методи соціальної інженерії та складні сценарії зламу інформаційних систем. У таких умовах

стандартні методи оцінювання ризиків часто не дають точного результату, особливо коли відсутня достатня статистика інцидентів або інформація є неповною. Тому важливу роль у процесі оцінювання відіграють експерти, які мають практичний досвід у сфері інформаційної безпеки.

Разом із тим, традиційний процес експертного оцінювання має низку проблем. Різні фахівці можуть по-різному оцінювати одну й ту саму загрозу через власний досвід, рівень підготовки чи бачення ситуації[21]. Крім того, у багатьох організаціях для оцінювання ризиків використовуються або складні та дорогі спеціалізовані системи, або звичайні електронні таблиці, які не дозволяють швидко перевіряти правильність оцінок та аналізувати узгодженість думок експертів. Це створює потребу у створенні зручної автоматизованої системи, яка допоможе збирати, обробляти та аналізувати експертні оцінки більш швидко й ефективно.

Основною метою даної роботи є створення системи управління ризиками інформаційної безпеки, яка дозволить автоматизувати процес збору та обробки експертних оцінок, визначати найбільш небезпечні загрози та допомагати у виборі оптимальних заходів захисту інформаційних активів організації.

Для досягнення поставленої мети необхідно вирішити такі основні завдання:

- розробити механізм обробки експертних оцінок. Система повинна перетворювати текстові або числові оцінки експертів у зрозумілі показники ризику. Також необхідно передбачити врахування рівня компетентності кожного експерта залежно від його досвіду роботи, посади та професійних навичок. Це дозволить отримувати більш точні результати та зменшити вплив помилкових або необ’єктивних оцінок.

- спроектувати структуру системи. Необхідно створити програмний комплекс, який буде містити модуль керування опитуваннями, інтерфейс для експертів, блок обробки результатів та систему формування звітів[22]. Програма повинна забезпечувати зручне зберігання інформації, надійність роботи та можливість подальшого розширення функціоналу.

- реалізувати перевірку узгодженості оцінок. Система має автоматично визначати, наскільки думки експертів збігаються між собою. Якщо результати оцінювання будуть суттєво відрізнятися, програма повинна повідомляти про це та

надавати можливість повторного аналізу для уточнення результатів[23,24]. Це допоможе досягти більш об’єктивної оцінки ризиків.

- створити засоби візуалізації результатів. Після обробки даних система повинна формувати зрозумілу карту ризиків, де буде показано рівень небезпеки для кожного інформаційного активу. Також програма має надавати рекомендації щодо можливих дій: зниження ризику, уникнення загрози або прийняття ризику у випадку його незначного впливу

Основою роботи системи стане алгоритм розрахунку інтегрального показника ризику. Він буде формуватися на основі всіх отриманих оцінок експертів із врахуванням рівня довіри до кожного спеціаліста. Такий підхід дозволить отримувати більш точні результати та мінімізувати вплив людського чинника.

Реалізація даної системи дозволить організаціям швидше та ефективніше проводити оцінювання ризиків інформаційної безпеки, своєчасно виявляти найбільш небезпечні загрози та приймати обґрунтовані рішення щодо захисту інформації. Керівництво організації зможе бачити, які саме напрямки потребують найбільших інвестицій у безпеку, а також планувати заходи захисту на основі реальних показників, а не припущень.

Оскільки система автоматизує процес збору та аналізу думок експертів, оцінювання ризиків можна буде проводити регулярно та значно швидше, ніж при ручній обробці даних. У результаті організація отримає зручний інструмент для підтримки стабільного рівня інформаційної безпеки та підвищення власної кіберстійкості в умовах сучасного цифрового середовища.

Додатковою перевагою розробленої системи стане можливість централізованого зберігання всієї інформації про ризики, проведені оцінювання та результати аналізу. Це дозволить формувати єдину базу знань організації у сфері інформаційної безпеки та відстежувати зміни рівня ризиків у часі. Завдяки накопиченню історичних даних керівництво зможе аналізувати ефективність уже впроваджених заходів захисту, визначати слабкі місця в інфраструктурі та оперативно реагувати на появу нових загроз. Крім того, автоматизація процесів значно зменшить витрати часу працівників на підготовку звітів і проведення повторних оцінювань.

Важливою особливістю системи також стане її універсальність та можливість адаптації під потреби різних організацій. Програмний комплекс можна буде використовувати як у невеликих компаніях, так і у великих установах із розгалуженою інформаційною інфраструктурою. Гнучкі налаштування дозволять змінювати критерії оцінювання ризиків, кількість експертів та параметри аналізу залежно від специфіки діяльності організації. Це зробить систему практичним інструментом для підвищення рівня захисту інформації та допоможе інтегрувати процес управління ризиками у щоденну діяльність підприємства. У контексті впровадження такої системи в роботу компанії, важливо, щоб вона допомагала виконувати реальні вимоги законодавства та правил безпеки, а не просто залишалася програмою для галочки чи бюрократії. Головна фішка автоматизації - перетворити нудне заповнення паперів на живий процес, який реально допомагає керівництву приймати рішення щодо захисту бізнесу.

Оскільки кожен спеціаліст оцінює загрози по-своєму і часто користується простими словами на кшталт «небезпечно» або «дуже небезпечно», система повинна вміти переводити ці суб'єктивні думки у конкретні й зрозумілі цифри. Для цього в алгоритми будуть закладені спеціальні математичні моделі, які згладжують такі розбіжності та враховують досвід кожного експерта: його стаж, наявність сертифікатів та те, наскільки точними були його прогнози в минулому. Саму програму краще розбити на окремі незалежні блоки - окремо інтерфейс для користувача, окремо логіка розрахунків та база даних. Це дозволить базі працювати швидко, легко оновлюватися та надійно зберігати інформацію як про самі комп'ютерні активи, так і про результати опитувань. Безпека самої системи теж буде на висоті, адже в ній зберігатимуться всі слабкі місця компанії, тому доступ розмежують за ролями, всі дані зашифрують, а кожен крок користувачів буде чітко записуватися в журнал аудиту.

2 МОДЕЛІ ТА МЕТОДИ ПОБУДОВИ СИСТЕМИ

2.1 Модель представлення та оцінювання ризиків інформаційної безпеки

Сучасний етап розвитку інформаційних технологій характеризується стрімким зростанням залежності суспільства, бізнесу та державних структур від інформаційних систем і цифрових сервісів. Інформація в таких умовах набуває статусу стратегічного ресурсу, а її захист стає критично важливою складовою функціонування будь-якої організації. Одночасно з цим зростає і кількість кіберзагроз, які стають більш складними, динамічними та цілеспрямованими.

У результаті цього інформаційна безпека перестає бути виключно технічною задачею і перетворюється на комплексну міждисциплінарну проблему, що включає технологічні, організаційні, економічні та управлінські аспекти. У таких умовах особливого значення набуває поняття ризику інформаційної безпеки, яке дозволяє кількісно та якісно оцінити рівень загроз для інформаційних ресурсів та визначити пріоритети захисту[25].

Ризик інформаційної безпеки розглядається як ймовірність виникнення події, що призводить до негативних наслідків для конфіденційності, цілісності або доступності інформації. Однак у сучасних умовах таке визначення є недостатнім, оскільки не враховує складність взаємодії між елементами інформаційної системи, а також вплив середовища, в якому вона функціонує.

Саме тому сучасні підходи до аналізу ризиків базуються на формалізованих моделях, які дозволяють враховувати множинність факторів, таких як джерела загроз, рівень захищеності системи, наявність вразливостей, критичність активів та ефективність заходів безпеки[26]. Використання таких моделей забезпечує перехід від інтуїтивного управління безпекою до структурованого та науково обґрунтованого підходу.

Важливо також враховувати, що ризики інформаційної безпеки мають динамічний характер. Вони змінюються у часі під впливом появи нових загроз, оновлення програмного забезпечення, зміни конфігурацій систем. Це вимагає постійного моніторингу та регулярного переоцінювання рівня ризиків, що є невід’ємною частиною сучасних систем управління інформаційною безпекою.

Однією з ключових особливостей сучасних систем оцінювання ризиків є необхідність врахування взаємозалежності між окремими компонентами інформаційної інфраструктури. У реальних умовах інформаційні системи функціонують як складні розподілені середовища, де компрометація одного елемента може спричинити каскадний вплив на інші компоненти системи. Наприклад, успішна атака на сервер автентифікації може надати зловмиснику доступ до великої кількості внутрішніх сервісів та ресурсів організації. У зв'язку з цим процес оцінювання ризиків повинен враховувати не лише окремі загрози, але й можливі сценарії їх поширення та комбінованого впливу.

Додатково слід враховувати, що сучасні кіберзагрози дедалі частіше мають багатовекторний характер. Це означає, що атаки можуть одночасно поєднувати технічні, соціальні та організаційні методи впливу. Прикладом є фішингові кампанії, які поєднують психологічний вплив на користувачів із використанням технічних вразливостей програмного забезпечення. У таких умовах ефективна модель ризику повинна враховувати не лише технічні параметри безпеки, але й поведінкові аспекти діяльності персоналу, рівень кібергігієни працівників та ефективність внутрішніх політик безпеки.

Важливим аспектом також є врахування економічної складової ризику. Для більшості організацій оцінювання ризиків інформаційної безпеки пов'язане не лише із забезпеченням технічного захисту, але й із необхідністю мінімізації фінансових втрат. Саме тому сучасні моделі оцінювання ризиків орієнтуються на визначення співвідношення між витратами на впровадження засобів захисту та можливими наслідками реалізації загроз. Такий підхід дозволяє формувати економічно обґрунтовану стратегію управління інформаційною безпекою та оптимізувати використання ресурсів організації.

З огляду на це, моделювання та оцінювання ризиків інформаційної безпеки розглядається як фундаментальний етап побудови систем захисту інформації. Воно дозволяє не лише виявляти потенційні загрози, але й визначати їх пріоритетність, оцінювати можливі наслідки та обґрунтовувати вибір захисних заходів.

Концептуально ризик інформаційної безпеки виникає лише за умови одночасної реалізації трьох взаємопов'язаних компонентів: існування загрози,

наявності відповідної вразливості та доступності інформаційного активу для впливу. Така тріада є базовою основою сучасного підходу до моделювання ризиків у сфері кібербезпеки. Відсутність хоча б одного з цих елементів або унеможливлює реалізацію інциденту, або суттєво знижує його ймовірність. Для більш детального аналізу доцільно розглянути кожен із компонентів моделі окремо.

- загрози визначають потенційні джерела небезпеки для інформаційної системи. Вони можуть бути як навмисними (атаки з боку зловмисників), так і ненавмисними (помилки персоналу, збої обладнання, природні явища). Загрози характеризуються різним рівнем складності, способом реалізації та цільовою спрямованістю. У моделі ризику саме загрози формують первинний імпульс, який може призвести до інциденту безпеки.

- вразливості є слабкими місцями інформаційної системи, які можуть бути використані для реалізації загроз. Вони можуть виникати на різних рівнях: програмному, апаратному, мережевому або організаційному. Особливу роль відіграє людський фактор, оскільки помилки користувачів часто створюють додаткові можливості для атак. Таким чином, вразливості не є прямою причиною інцидентів, але формують умови для їх реалізації.

- активи інформаційної системи є об’єктами, на які спрямовані загрози. До них належать дані, інформаційні системи, програмні сервіси, апаратні ресурси, а також бізнес-процеси та репутація організації. Кожен актив має певну цінність, яка визначає критичність наслідків у разі його порушення. Саме через оцінку активів визначається масштаб потенційних втрат.

- засоби захисту інформації виконують функцію зменшення рівня ризику шляхом впливу на інші компоненти моделі. Вони можуть знижувати ймовірність реалізації загроз, усувати або мінімізувати вразливості, а також обмежувати наслідки інцидентів. До них належать технічні, програмні та організаційні заходи безпеки. Ефективність захисту безпосередньо впливає на кінцевий рівень ризику.

- середовище функціонування інформаційної системи визначає зовнішній і внутрішній контекст виникнення ризиків. До зовнішніх факторів належать загальний рівень кіберзагроз, нормативно-правове регулювання та технологічні тенденції. Внутрішні фактори включають політики безпеки, рівень підготовки

персоналу та архітектуру системи. Сукупність цих факторів формує умови, в яких змінюється характер і рівень ризиків.

Засоби захисту інформації виконують функцію зменшення рівня ризику шляхом впливу на інші компоненти моделі. Вони можуть знижувати ймовірність реалізації загроз, усувати або мінімізувати вразливості, а також обмежувати наслідки інцидентів. До них належать технічні, програмні та організаційні заходи безпеки. Ефективність захисту безпосередньо впливає на кінцевий рівень ризику.

Оскільки наведена п'ятикомпонентна структура описує складні внутрішні зв'язки об'єкта захисту, базова модель оцінювання виявляється недостатньою для точного аналізу. Взаємодія зазначених компонентів формує цілісну модель ризику інформаційної безпеки, де кінцева величина залишкового ризику (R_R) визначається як функція від інтенсивності загроз, глибини вразливостей, критичності активів та ефективності впровадженого комплексу захисту. Математично цей взаємозв'язок та інтегральний вплив засобів протидії на рівень безпеки системи описується за допомогою такої розширеної формули:

$$R_R = \frac{T * V * I}{C}, \tag{2.1}$$

де:

T-ймовірність або частота реалізації загрози;

V-ступінь уразливості системи до даної загрози;

I-потенційні збитки;

C-коефіцієнт ефективності впроваджених засобів.

Така математична декомпозиція показує, що зміна одного елемента безпосередньо впливає на загальний рівень захищеності системи. Наприклад, поява нової вразливості (V) в програмному забезпеченні автоматично підвищує ймовірність реалізації певних загроз, а впровадження додаткових механізмів захисту (C), навпаки, суттєво знижує залишковий ризик виникнення інциденту, що дозволяє гнучко керувати безпекою активів у режимі реального часу.

Крім того, ефективність моделі ризику значною мірою залежить від актуальності та достовірності вхідних даних. У сучасних умовах інформація про загрози та вразливості швидко змінюється, що вимагає постійного оновлення баз знань і проведення регулярного моніторингу стану інформаційної системи. Для цього організації використовують системи управління подіями інформаційної безпеки (SIEM), засоби аналізу мережевого трафіку та автоматизовані сканери вразливостей. Інтеграція таких інструментів із моделями оцінювання ризиків дозволяє підвищити точність аналізу та забезпечити оперативне реагування на нові кіберзагрози.

Модель представлення та оцінювання ризиків інформаційної безпеки є фундаментом для побудови ефективної системи захисту, оскільки вона дозволяє трансформувати абстрактні загрози у конкретні показники, придатні для прийняття управлінських рішень. В основі такої моделі лежить взаємозв’язок між інформаційними активами, потенційними загрозами та існуючими вразливостями інформаційної системи. Ризик виникає лише у випадку, коли джерело загрози здатне використати наявну вразливість та через неї вплинути на цінний ресурс організації, спричиняючи негативні наслідки для її функціонування. Концептуально ризик інформаційної безпеки виникає за умови одночасної наявності трьох компонентів: загрози, вразливості та активу, доступного для впливу. Відсутність хоча б одного з цих елементів унеможливлює реалізацію інциденту або суттєво знижує його ймовірність. У зв’язку з цим процес побудови моделі ризику починається з детальної інвентаризації активів, яка охоплює не лише інформаційні ресурси, але й програмне забезпечення, апаратні засоби та людський фактор. Для кожного активу визначається рівень його критичності за критеріями конфіденційності, цілісності та доступності. Паралельно здійснюється аналіз середовища загроз, що включає дослідження можливих кіберінцидентів, оцінювання ймовірності технічних збоїв, а також аналіз ризиків, пов’язаних із помилками або навмисними діями персоналу.

Ключовим етапом моделювання є вибір методу оцінювання ризиків, який може бути якісним, кількісним або комбінованим. Якісне оцінювання базується на експертному аналізі, в рамках якого ризики класифікуються за рівнями (низький,

середній, високий, критичний) залежно від ймовірності їх реалізації та тяжкості наслідків. Кількісний підхід, у свою чергу, передбачає використання числових показників, що дозволяє оцінювати ризики у вимірюваних величинах, наприклад у вигляді фінансових втрат або часу простою системи. Це створює можливість більш обґрунтованого прийняття рішень щодо доцільності впровадження заходів захисту. У практиці управління ризиками інформаційної безпеки часто використовується комбінований підхід, який поєднує переваги якісного та кількісного оцінювання. На початковому етапі ризики можуть визначатися та класифікуватися за допомогою експертних оцінок, після чого найбільш критичні з них піддаються детальному кількісному аналізу. Такий підхід дозволяє забезпечити баланс між точністю результатів та складністю проведення оцінювання.

Для практичної реалізації процесу оцінювання ризиків широко використовується матричний підхід (табл. 2.1), який дозволяє поєднати показники ймовірності реалізації загроз та масштабу їх наслідків і представити результати у зручній для аналізу формі. Це дозволяє чітко пріоритезувати загрози та оперативно приймати рішення щодо першочергових заходів захисту.

Таблиця 2.1 – Матриця визначення рівнів ризику

Ймовірність / Наслідки	Низькі наслідки	Середні наслідки	Високі наслідки
Низька ймовірність	Низький ризик	Низький ризик	Середній ризик
Середня ймовірність	Низький ризик	Середній ризик	Високий ризик
Висока ймовірність	Середній ризик	Високий ризик	Критичний ризик

Практичне використання матриці ризиків дозволяє суттєво спростити процес прийняття управлінських рішень у сфері інформаційної безпеки. Завдяки наочному представленню результатів аналізу керівництво організації може швидко визначити найбільш небезпечні напрями та сформувати пріоритетний план впровадження заходів захисту. Особливо ефективним матричний підхід є на початкових етапах оцінювання ризиків, коли необхідно оперативно класифікувати значну кількість потенційних загроз. Водночас результати матричного аналізу значною мірою залежать від якості експертного оцінювання. Якщо оцінки

ймовірності або наслідків визначаються суб'єктивно, це може призвести до спотворення загальної картини ризиків. Саме тому у сучасних системах управління ризиками дедалі частіше застосовуються методи колективного експертного оцінювання, які дозволяють агрегувати думки кількох спеціалістів та зменшувати вплив індивідуальних когнітивних упереджень.

Крім того, матричний підхід часто використовується як основа для побудови автоматизованих систем підтримки прийняття рішень. У таких системах результати оцінювання можуть відображатися у вигляді інтерактивних панелей, графіків та динамічних карт ризиків, що забезпечує більш ефективний моніторинг стану інформаційної безпеки організації. Це особливо актуально для великих підприємств та державних установ, де кількість інформаційних активів і потенційних загроз є надзвичайно великою.

Матриця ризиків дозволяє здійснити класифікацію загроз за рівнем їх критичності та визначити пріоритетність впровадження заходів захисту. Поєднання низької ймовірності та незначних наслідків відповідає низькому рівню ризику, який, як правило, не потребує негайного втручання та контролюється у процесі моніторингу.

Ризики середнього рівня вимагають планового впровадження заходів безпеки, спрямованих на зниження їх впливу або ймовірності виникнення. Високі ризики потребують оперативного реагування, оскільки можуть суттєво вплинути на функціонування інформаційної системи. Критичні ризики є неприйнятними та вимагають негайного усунення або мінімізації шляхом впровадження комплексних технічних та організаційних заходів захисту.

Незважаючи на простоту та наочність матричного підходу, він має певні обмеження, пов'язані з суб'єктивністю оцінювання та відсутністю точних кількісних показників. У зв'язку з цим у сучасних системах управління інформаційною безпекою застосовуються більш складні кількісні моделі оцінювання ризиків, які дозволяють отримувати точніші результати та підвищують обґрунтованість управлінських рішень.

Подальший розвиток методів оцінювання ризиків інформаційної безпеки пов'язаний із переходом від якісних та напівкількісних підходів до повноцінних

кількісних моделей. Це зумовлено необхідністю отримання більш точних та обґрунтованих результатів, які можуть бути використані для прийняття управлінських рішень, зокрема у сфері інвестування в заходи захисту інформації. Однією з найбільш відомих кількісних моделей є методологія FAIR (Factor Analysis of Information Risk), яка дозволяє представити ризик як очікувану величину можливих втрат[27]. У межах цього підходу ризик розглядається як функція частоти виникнення загрозових подій та масштабу їх наслідків. Це дає змогу деталізувати процес оцінювання та перейти до аналізу окремих факторів, що впливають на рівень ризику.

Модель FAIR передбачає декомпозицію ризику на такі складові, як частота загрозових подій, ймовірність їх успішної реалізації та величина потенційних втрат. Завдяки цьому стає можливим оцінювання ризику у грошовому еквіваленті, що є важливим для бізнес-орієнтованого підходу до управління інформаційною безпекою. Крім того, FAIR дозволяє проводити сценарний аналіз, що дає змогу оцінювати вплив різних варіантів розвитку подій на загальний рівень ризику.

Поряд із кількісними моделями значну роль відіграють міжнародні стандарти, зокрема підхід, визначений стандартом ISO/IEC 27005, який регламентує процес управління ризиками інформаційної безпеки. Даний стандарт не обмежується лише методами оцінювання, а охоплює повний життєвий цикл управління ризиками, включаючи їх ідентифікацію, аналіз, оцінювання, обробку та моніторинг. Відповідно до ISO/IEC 27005, оцінювання ризиків здійснюється з урахуванням контексту організації, що включає її бізнес-цілі, нормативні вимоги, структуру інформаційної системи та допустимий рівень ризику. Це дозволяє адаптувати процес управління ризиками до специфіки конкретної організації та забезпечити його узгодженість із загальною стратегією безпеки.

Особливістю підходу ISO/IEC 27005 є поєднання якісних та кількісних методів оцінювання, що забезпечує гнучкість та універсальність його застосування. На практиці це означає, що організація може використовувати матричні моделі для первинної оцінки ризиків, а більш складні кількісні методи - для детального аналізу критичних загроз. Таким чином, сучасні підходи до оцінювання ризиків інформаційної безпеки базуються на інтеграції різних методів, що дозволяє

враховувати як технічні, так і організаційні аспекти функціонування системи.

Отже, модель представлення та оцінювання ризиків інформаційної безпеки є складною багаторівневою системою, що базується на аналізі взаємодії загроз, вразливостей, активів та засобів захисту. Використання концептуального, матричного та кількісного підходів дозволяє забезпечити комплексне оцінювання рівня ризиків та визначити пріоритетні напрями їх зниження. Застосування сучасних методологій, таких як FAIR та ISO/IEC 27005, сприяє підвищенню точності оцінювання ризиків і забезпечує можливість прийняття обґрунтованих управлінських рішень у сфері інформаційної безпеки[28]. Це, у свою чергу, створює основу для побудови ефективної системи захисту інформації та підвищення загального рівня безпеки інформаційних систем.

2.2 Методи отримання й агрегування експертних оцінок

У процесі оцінювання ризиків інформаційної безпеки важливу роль відіграє якість вихідних даних, на основі яких здійснюється аналіз. Проте на практиці часто виникають ситуації, коли точні статистичні дані щодо інцидентів безпеки відсутні або є недостатніми для проведення повноцінного кількісного аналізу. Це пов’язано з динамічністю кіберзагроз, унікальністю інформаційних систем та обмеженим доступом до достовірної інформації про інциденти.

У таких умовах одним із найбільш ефективних підходів є використання експертних оцінок, які базуються на знаннях, досвіді та професійній інтуїції фахівців. Експертні методи дозволяють формалізувати суб’єктивні судження та використовувати їх як вхідні дані для моделей оцінювання ризиків.

Експертні оцінки застосовуються для визначення ймовірності реалізації загроз, оцінювання ступеня вразливостей, визначення рівня критичності активів, а також прогнозування можливих наслідків інцидентів. Їх використання є особливо актуальним у випадках, коли аналізу підлягають нові або малодосліджені загрози.

Процес отримання експертних оцінок передбачає чітку організацію та включає декілька етапів. На першому етапі здійснюється відбір експертів, які

повинні мати достатній рівень компетентності у сфері інформаційної безпеки[29]. Важливо забезпечити різноманітність досвіду учасників, щоб охопити різні аспекти аналізованої проблеми. Наступним етапом є формування завдання для експертів, яке повинно бути чітко структурованим та однозначним. Невизначеність формулювання може призвести до значних відхилень у результатах оцінювання. Після цього здійснюється безпосередній збір експертних оцінок за допомогою відповідних методів. Завершальним етапом є обробка отриманих даних та їх агрегування.

Існує декілька основних методів отримання експертних оцінок, які відрізняються способом взаємодії між експертами та рівнем формалізації процесу[30]. Індивідуальні методи передбачають незалежне надання оцінок кожним експертом. До них належать анкетування та інтерв'ювання. Перевагою таких методів є відсутність впливу групової динаміки, що дозволяє отримати більш незалежні судження. Однак це може призводити до значної варіативності результатів. Колективні методи базуються на взаємодії експертів. До них належать групові обговорення, "мозковий штурм" та експертні комісії. Ці методи дозволяють сформувати більш узгоджену позицію, проте можуть бути схильні до впливу авторитету окремих учасників.

Особливе місце займає метод Делфі, який є одним із найбільш ефективних способів отримання узгоджених експертних оцінок[31]. Він передбачає проведення декількох раундів анонімного опитування, після кожного з яких результати узагальнюються та повертаються експертам для перегляду. Це дозволяє поступово зменшити розбіжності між оцінками та підвищити їх узгодженість. Крім того, застосовуються методи використання експертних шкал, які дозволяють переводити якісні оцінки у числову форму, що значно спрощує їх подальшу обробку.

Незважаючи на широке застосування в процесах оцінювання ризиків інформаційної безпеки, експертні оцінки мають низку суттєвих обмежень, які необхідно враховувати при їх використанні. Основною проблемою є їх суб'єктивний характер, оскільки результати значною мірою залежать від індивідуальних особливостей експертів, їх досвіду, знань та здатності інтерпретувати надану інформацію. Це може призводити до спотворення

результатів і зниження достовірності оцінювання. До основних факторів, що впливають на якість експертних оцінок, належать:

- рівень компетентності експертів. Якість результатів залежить від професійної підготовки та досвіду фахівців. Недостатній рівень знань або вузька спеціалізація можуть призвести до неповного врахування факторів ризику чи помилкових висновків. Водночас навіть досвідчені експерти можуть мати різні підходи до оцінювання.

- когнітивні упередження. Експерти можуть піддаватися психологічним викривленням, таким як ефект якоря, надмірна впевненість або схильність до підтвердження власних переконань, що знижує об'єктивність оцінок[32].

- вплив групової думки. Під час колективного оцінювання можливе формування "групового мислення", коли учасники орієнтуються на позицію більшості або авторитетних експертів, що обмежує різноманітність суджень.

- недостатня формалізація процесу оцінювання. Відсутність чітких критеріїв і шкал оцінювання ускладнює інтерпретацію результатів та знижує їх відтворюваність у подальшому аналізі.

Крім зазначених факторів, слід також враховувати такі аспекти, як обмеженість часу на проведення оцінювання, складність аналізу великої кількості параметрів, а також можливу неповноту або неточність вихідної інформації. Усі ці чинники можуть впливати на якість кінцевих результатів і потребують додаткової уваги при організації експертного оцінювання. З огляду на зазначені обмеження, важливим завданням є підвищення об'єктивності експертних оцінок шляхом використання формалізованих методів їх обробки та узагальнення.

Зокрема, застосування методів агрегування, статистичної обробки та перевірки узгодженості дозволяє зменшити вплив суб'єктивних факторів і підвищити достовірність результатів оцінювання. Таким чином, незважаючи на певні недоліки, експертні оцінки залишаються важливим інструментом аналізу ризиків інформаційної безпеки. Їх ефективне використання можливе за умови врахування існуючих обмежень та застосування відповідних методів підвищення надійності отриманих результатів що є основою для побудови стабільної системи захисту підприємства.

Важливим етапом обробки експертної інформації є агрегування отриманих оцінок, яке полягає у поєднанні індивідуальних суджень експертів у єдиний узагальнений показник.

Найпростішим методом агрегування є визначення середнього арифметичного значення, однак цей підхід не враховує відмінності у рівні компетентності експертів. Тому для реалізації в інформаційній системі оцінювання ризиків застосовано метод зваженого середнього, який враховує коефіцієнт компетентності кожного конкретного фахівця.

Математична модель агрегування експертних оцінок за методом зваженого середнього описується такою формулою:

$$\bar{X} = \frac{\sum_{i=1}^{n} w_i x_i}{\sum_{i=1}^{n} w_i}, \tag{2.2}$$

де $\bar{X}$- агрегована експертна оцінка конкретного параметра ризику;

x_i - оцінка надана, надана і-тим експертом;

w_i - ваговий коефіцієнт, що відображає рівень компетентності або значущості експерта;

n - загальна кількість експертів.

Для спрощення розрахунків у програмному модулі застосовується умова нормування вагових коефіцієнтів, за якої сума всіх ваг дорівнює одиниці:

$$\sum_{i=1}^{n} w_i = 1, \tag{2.3}$$

Враховуючи зазначені особливості та вимоги, за цієї умови формула математичного агрегування набуває оптимізованого алгоритмічного вигляду, який безпосередньо реалізується в програмному коді:

$$\bar{X} = \sum_{i=1}^{n} w_i * x_i, \tag{2.4}$$

Використання вагових коефіцієнтів дозволяє врахувати індивідуальні особливості експертів, зокрема їхній досвід та кваліфікацію.

Проте автоматичне агрегування є коректним лише за умови, що думки експертів є узгодженими. Для перевірки ступеня близькості суджень експертів та визначення правомірності обчислення зваженого середнього, в алгоритм системи впроваджено розрахунок коефіцієнта варіації (V_j) для кожного оцінюваного параметра ризику:

$$V_j = \frac{\sigma_j}{\bar{X}_j} * 100\%, \tag{2.5}$$

де σ_j середньоквадратичне відхилення оцінок j-го параметра, яке обчислюється як:

$$\sigma_j = \sqrt{\frac{\sum_{i=1}^{n} w_i * \left(x_{ij} - \bar{X}_J\right)^2}{\sum_{i=1}^{n} w_i}}, \tag{2.6}$$

Алгоритмічне правило прийняття рішень щодо узгодженості груп:

- якщо $V_j \leq 33\%$, думки експертів вважаються узгодженими, а отримане значення $\bar{X}_j$ приймається системою як репрезентативне вхідне значення для розширеної моделі ризику;

- якщо $V_j > 33\%$, у групі наявні суттєві розбіжності (неузгодженість). У цьому випадку автоматизована система відхиляє результати та ініціює новий раунд експертного опитування за методом Делфі для уточнення позицій.

Описаний підхід із розрахунком ваг та варіативності забезпечує об’єктивне відображення реального рівня знань експертів і дозволяє мінімізувати вплив менш обґрунтованих чи полярних суджень.

Застосування методу зваженого середнього разом із синергетичним контролем відхилень є критично важливим у випадках, коли група експертів є неоднорідною за рівнем компетентності, оскільки просте усереднення в таких умовах призводить до значного викривлення кінцевих результатів аналізу ризиків.

Окрім зваженого середнього, у практиці оцінювання ризиків застосовуються й інші методи агрегування. Зокрема, використання медіани дозволяє зменшити вплив крайніх або аномальних значень, що особливо важливо при наявності значних розбіжностей між оцінками експертів. Рангові методи застосовуються у випадках, коли необхідно впорядкувати альтернативи або визначити пріоритетність ризиків. Більш складні підходи, такі як метод аналізу ієрархій (AHP), дозволяють враховувати декілька критеріїв одночасно та визначати відносну важливість факторів.

Крім того, у сучасних дослідженнях все частіше використовуються методи нечіткої логіки, які дозволяють працювати з невизначеними, неточними або лінгвістичними оцінками (наприклад, “високий ризик”, “середня ймовірність”)[33]. Це особливо актуально для задач інформаційної безпеки, де значна частина параметрів не має чітко визначених кількісних значень.

Отже, агрегування експертних оцінок є ключовим етапом процесу аналізу ризиків інформаційної безпеки, який забезпечує перехід від індивідуальних суб’єктивних суджень до узагальнених кількісних показників. Використання формалізованих методів, зокрема зваженого середнього, медіани, рангових підходів та методів нечіткої логіки, дозволяє зменшити вплив суб’єктивних факторів і підвищити об’єктивність результатів. Застосування таких підходів у поєднанні з належною організацією експертного оцінювання створює основу для побудови надійних моделей оцінювання ризиків та підвищує ефективність системи управління інформаційною безпекою в цілому. Автоматизація цих розрахунків дозволяє значно прискорити процес прийняття рішень у компанії.

2.3 Метод визначення рівня ризику та підтримки прийняття рішень

Після отримання та агрегування експертних оцінок виникає задача переходу від окремих числових значень до інтегрального показника ризику, який може бути використаний для управлінських рішень. На цьому етапі здійснюється інтерпретація результатів оцінювання та їх трансформація у форму, придатну для

практичного застосування в системі управління інформаційною безпекою[34]. Це дозволяє звести різнорідні експертні судження щодо загрозового середовища та внутрішнього стану інфраструктури до єдиного консолідованого індексу. Автоматизація цього процесу в межах розроблюваного програмного забезпечення мінімізує вплив суб'єктивного фактора під час фінального розрахунку.

У межах запропонованого підходу інтегральний показник рівня ризику (R) для конкретного інформаційного активу розраховується на основі агрегованих експертних оцінок компонентів розширеної моделі, а також із врахуванням вагових коефіцієнтів критичності самого активу (за критеріями конфіденційності, цілісності та доступності). Така інтеграція забезпечує гнучкість моделі, оскільки кінцева оцінка ризику. Це дозволяє виділити найбільш вразливі зони системи та зосередити основні ресурси на їх першочерговому захисті. Крім того, такий підхід допомагає уникнути зайвих витрат на безпеку тих об'єктів.

Математично обчислення інтегрального показника ризику здійснюється за формулою:

$$R = \frac{\bar{T} * \bar{V} * \bar{I}}{C} * W_A, \tag{2.7}$$

де: R - підсумковий інтегральний показник рівня ризику;

R - підсумковий інтегральний показник рівня ризику;

T,V,I- агреговані за методом зваженого середнього експертні оцінки ймовірності загрози, ступеня вразливості та потенційного впливу відповідно, нормовані до інтервалу [0; 1];

C- коефіцієнт ефективності існуючих засобів захисту$(1 \leq C \leq 2)$;

Wa - інтегральний коефіцієнт критичності інформаційного активу.

Інтегральний коефіцієнт критичності активу (W_A) обчислюється як зважена сума його базових параметрів безпеки:

$$W_A = \alpha * C_{act} + \beta * I_{act} + \tau * A_{act}, \tag{2.8}$$

Де $C_{act}I_{act}A_{act}$- оцінки критичності активу за критеріями конфіденційності, цілісності та доступності, що виставляються за шкалою від 1 до 5;

α, β, τ - вагові коефіцієнті значущості цих критеріїв для організації, які задовольняють умову нормування $\alpha + \beta + \tau = 1$.

Для забезпечення однозначної інтерпретації обчисленого числового значення ризику R та автоматичного вибору стратегії реагування, в алгоритм системи впроваджено функцію інтервального розподілу. Оскільки максимальне теоретичне значення показника ризику за такою бальною шкалою становить R_{max} = 5, увесь простір рішень декомпоновано на чотири рівні діапазони:

$$R = \begin{cases} \text{Низький, якщо } 0 \leq R \leq 1.25 \\ \text{Середній, якщо } 1.25 < R \leq 2.50 \\ \text{Високий, якщо } 2.50 < R \leq 3.75 \\ \text{Критичний, якщо } 3.75 < R \leq 5.00 \end{cases}, \quad (2.9)$$

Отриманий вердикт цієї функції безпосередньо визначає логіку роботи системи підтримки прийняття рішень та автоматично зіставляється з узагальненою схемою стратегій реагування, яка наведена в таблиці 2.2.

Для узагальнення та наочного представлення повної послідовності дій аналітичного модуля - від моменту збору первинних експертних даних до автоматичного формування підсумкових рекомендацій - було розроблено загальну блок-схему алгоритму методу. Повний цикл математичного оброблення та прийняття рішень графічно зображено на рисунку 2.1. Ця схема деталізує кожен крок обчислювального процесу, включаючи агрегацію експертних оцінок, розрахунок інтегральних показників кіберризиків та їх ранжування за рівнем критичності. Завдяки такій візуалізації забезпечується прозорість алгоритму, що дозволяє чітко простежити трансформацію вхідних якісних параметрів у кількісні матричні значення для оптимізації подальших управлінських рішень.

Така структура спрощує перевірку правильності розрахунків на кожному етапі функціонування системи. Окрім цього, представлена графічна модель дозволяє швидко адаптувати алгоритм у разі появи нових критеріїв оцінювання. Це

робить розроблене рішення універсальним інструментом для побудови комплексних систем захисту інформації.

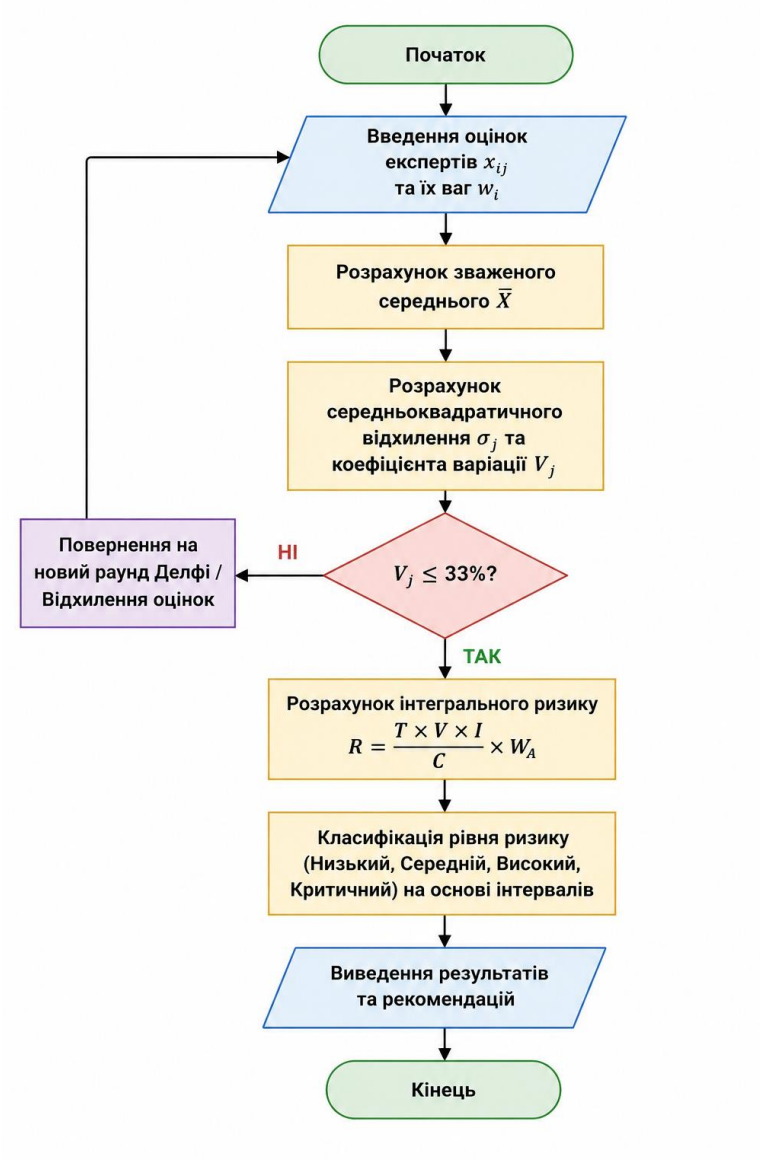


Рисунок 2.1 – Блок-схема алгоритму обробки експертної інформації та підтримки прийняття рішень

Представлений алгоритм дозволяє чітко простежити логіку функціонування системи у випадках виявлення розбіжностей у поглядах експертної групи. Циклічне повернення на новий раунд опитування за методом Делфі у разі перевищення порогу варіації ($V_j > 33\%$) гарантує високу точність та об'єктивність вихідних даних.

Крім того, у сучасних системах управління інформаційною безпекою важливу роль відіграє аналіз взаємозалежності ризиків. У багатьох випадках

реалізація однієї загрози може спричинити виникнення інших інцидентів або посилити їх наслідки. Наприклад, компрометація облікового запису адміністратора може призвести до порушення конфіденційності даних, зміни налаштувань безпеки та втрати доступності окремих сервісів. У зв'язку з цим оцінювання ризиків повинно враховувати можливість каскадного поширення інцидентів у межах інформаційної системи. Додатково слід враховувати фактор часу, оскільки рівень ризику не є статичним показником. Зміна конфігурації системи, поява нових вразливостей або оновлення програмного забезпечення можуть суттєво впливати на результати оцінювання. Тому ефективна система підтримки прийняття рішень повинна забезпечувати регулярне оновлення параметрів ризику та автоматичний перегляд рівня критичності активів відповідно до поточного стану інформаційного середовища.

Для забезпечення однозначної інтерпретації результатів вводиться шкала рівнів ризику, яка дозволяє виконати їх класифікацію. Як правило, така шкала містить чотири основні градації: низький, середній, високий та критичний рівень ризику. Кожен із рівнів відповідає певному діапазону значень інтегрального показника та відображає ступінь необхідності реагування з боку системи безпеки. Математичне розбиття загального інтервалу на рівні підмножини дозволяє системі підтримки прийняття рішень уникати невизначеності на стиках категорій.

Це дає змогу повністю автоматизувати процес класифікації без залучення додаткових людських ресурсів на етапі первинного аналізу. Низький рівень ризику свідчить про незначну ймовірність реалізації загрози та мінімальний вплив на функціонування інформаційної системи. У такому випадку достатнім є періодичний моніторинг без впровадження додаткових заходів захисту. Середній рівень ризику вимагає планового реагування, що може включати посилення окремих механізмів захисту або оптимізацію існуючих політик безпеки. Високий рівень ризику передбачає пріоритетне впровадження заходів зниження загрози, оскільки потенційні наслідки можуть суттєво вплинути на функціонування організації. Критичний уровень ризику є неприйнятним і потребує негайного реагування, включаючи усунення або ізоляцію відповідного активу чи загрози. Впровадження такого жорсткого алгоритму градації є основою для оптимізації

витрат на систему захисту інформації підприємства. Завдяки цьому адміністратор безпеки отримує чітко пріоритезований за рівнем загрози перелік вразливих вузлів інфраструктури.

Зрештою, це дозволяє раціонально розподіляти обмежені матеріальні та організації на ліквідацію лише найбільш небезпечних інцидентів. Для формалізації процесу вибору управлінських дій на основі рівня ризику використовується узагальнена схема стратегій реагування, яка наведена в таблиці 2.2.

Таблиця 2.2 – Стратегії реагування залежно від рівня ризику

Рівень ризику	Характеристика	Рекомендовані дії системи
Низький	Невелика ймовірність загрози, мінімальний вплив на систему	Прийняття ризику, періодичний моніторинг
Середній	Помірна ймовірність та вплив	Реалізація заходів зниження ризику (посилення контролів, оновлення політик безпеки)
Високий	Висока ймовірність або значний вплив	Пріоритетне зниження ризику, часткова передача (резервування, зовнішні сервіси)
Критичний	Неприйнятний рівень ризику, загроза функціонуванню системи	Негайне усунення джерела ризику або уникнення

Представлена класифікація стратегій реагування дозволяє стандартизувати процес управління ризиками та забезпечити єдиний підхід до прийняття рішень у межах організації. Це особливо важливо для великих інформаційних систем, де одночасно можуть існувати сотні потенційних загроз та вразливостей. Формалізація процесу реагування дозволяє уникнути хаотичних або несистемних дій та забезпечує узгодженість між технічними і управлінськими підрозділами організації, що значно підвищує загальну стійкість бізнесу до актуальних кіберзагроз.

Практична реалізація механізму підтримки прийняття рішень передбачає використання бази знань, у якій накопичуються правила реагування, шаблони дій та результати попередніх інцидентів[35]. Така база знань дозволяє не лише

автоматизувати вибір заходів безпеки, але й забезпечує накопичення досвіду організації у сфері управління ризиками. З часом система може використовувати історичні дані для оцінювання ефективності раніше впроваджених заходів та коригування майбутніх стратегій реагування. Важливим елементом підтримки прийняття рішень є також механізм пріоритезації ризиків. Оскільки ресурси організації є обмеженими, неможливо одночасно усунути всі потенційні загрози. Саме тому система повинна визначати, які ризики потребують негайного реагування, а які можуть бути прийняті або відкладені для подальшого аналізу. Пріоритезація здійснюється на основі інтегрального показника ризику, критичності активу та потенційного впливу інциденту на бізнес-процеси організації.

Для підвищення ефективності використання результатів оцінювання у системі передбачено механізм підтримки прийняття рішень. Його основою є набір формалізованих правил, які встановлюють відповідність між рівнем ризику та рекомендованими стратегіями реагування. Такий підхід дозволяє автоматизувати процес вибору управлінських дій та зменшити залежність від суб'єктивних рішень окремих фахівців[36].

Зокрема, для кожного рівня ризику формується типовий набір дій. Для низького рівня - ризик приймається без додаткових витрат ресурсів. Для середнього рівня - передбачаються заходи зниження ризику шляхом впровадження контрольних або організаційних механізмів. Для високого рівня - застосовується комбінація заходів зниження та передачі ризику, наприклад через резервування або зовнішні сервіси безпеки. Для критичного рівня - пріоритетним є уникнення ризику або негайне усунення джерела загрози[37].

Додатково результати оцінювання можуть використовуватись для побудови візуальних моделей ризиків, що дозволяє швидко ідентифікувати найбільш критичні елементи інформаційної системи та приймати обґрунтовані управлінські рішення щодо їх захисту. Таким чином, запропонований метод визначення рівня ризику та підтримки прийняття рішень забезпечує формалізацію процесу інтерпретації експертних оцінок та їх перетворення у практичні управлінські рекомендації, що підвищує ефективність системи управління інформаційною безпекою в цілому[38]. Крім того, використання такого підходу сприяє

підвищенню адаптивності системи безпеки до змін зовнішніх і внутрішніх загроз та забезпечує своєчасне реагування на потенційні ризики. Це також дозволяє оптимізувати розподіл ресурсів організації, зосереджуючи основну увагу на найбільш уразливих компонентах інформаційної інфраструктури.

2.4 Висновки до розділу

У другому розділі роботи було розглянуто теоретичні та методичні основи побудови системи управління ризиками інформаційної безпеки на основі експертних оцінок. Основну увагу приділено формалізації процесів представлення ризиків, методам отримання та обробки експертної інформації, а також підходам до визначення інтегрального рівня ризику та підтримки прийняття рішень. Було проаналізовано модель представлення ризику інформаційної безпеки, яка базується на взаємодії таких ключових компонентів, як загрози, вразливості, активи та засоби захисту. Показано, що ризик є багатофакторною категорією, яка залежить як від ймовірності реалізації загрози, так і від можливих наслідків для інформаційної системи.

Окрему увагу приділено експертним методам оцінювання, які застосовуються в умовах відсутності або недостатності статистичних даних. Розглянуто основні способи отримання експертних оцінок, включаючи індивідуальні та колективні методи, а також метод Делфі. Підкреслено, що ключовими проблемами експертного підходу є суб’єктивність оцінок та необхідність забезпечення їх узгодженості.

Важливим етапом є агрегування експертних оцінок, яке дозволяє перейти від індивідуальних суджень до узагальненого показника. Найбільш доцільним у межах даної роботи визначено використання методу зваженого середнього, що дозволяє враховувати рівень компетентності кожного експерта.

Також у розділі запропоновано метод визначення інтегрального рівня ризику та підхід до підтримки прийняття рішень. Встановлено, що класифікація ризиків за рівнями (низький, середній, високий, критичний) дозволяє формалізувати процес

реагування та автоматизувати вибір стратегій управління ризиками. Запропонована система правил реагування забезпечує відповідність між рівнем ризику та рекомендованими заходами безпеки. Отже, результати, отримані в другому розділі, формують теоретичну основу для подальшої практичної реалізації системи управління ризиками інформаційної безпеки. Розроблені моделі та методи дозволяють підвищити обґрунтованість оцінювання ризиків, зменшити вплив суб'єктивного фактора та забезпечити підтримку прийняття ефективних управлінських рішень у сфері інформаційної безпеки. Запропонований підхід може бути адаптований до різних типів інформаційних систем незалежно від їх масштабу та рівня складності.

Важливою перевагою методу є можливість інтеграції експертних оцінок із сучасними програмними засобами аналізу даних та моніторингу загроз. Це створює передумови для побудови автоматизованих систем підтримки прийняття рішень у сфері інформаційної безпеки. Крім того, застосування інтегрального показника ризику дозволяє здійснювати порівняльний аналіз стану безпеки різних компонентів інформаційної інфраструктури. Отримані результати можуть бути використані як основа для подальшого вдосконалення методів оцінювання ризиків та розробки комплексних систем захисту інформації.

3 РЕАЛІЗАЦІЯ ТА ТЕСТУВАННЯ СИСТЕМИ

3.1 Структура та програмна реалізація системи

Проєктування системи оцінювання ризиків інформаційної безпеки є складним багаторівневим процесом, що передбачає інтеграцію аналітичних методів, програмних рішень та зручного користувацького інтерфейсу[39]. У межах даної роботи реалізовано веб-орієнтовану систему «CyberRisk Pro», яка призначена для автоматизованого аналізу кіберризиків на основі експертно заданих параметрів.

В основу розробки покладено використання мови програмування Python, що зумовлено її широким застосуванням у сфері кібербезпеки та аналізу даних[40]. Вона характеризується зрозумілим синтаксисом, високою швидкістю розробки та широкими можливостями розширення функціоналу.

Серверна частина системи реалізована із використанням мікрофреймворку Flask, який забезпечує обробку HTTP-запитів та взаємодію між користувачем і програмною логікою. Архітектура додатку побудована за принципами розділення відповідальності, що дозволяє відокремити логіку обчислень, обробку запитів та інтерфейс користувача[41].

Клієнтська частина системи побудована з використанням сучасних технологій веб-розробки HTML5, CSS3 та фреймворку Bootstrap, що гарантує адаптивність та коректне відображення інтерфейсу на різних типах пристроїв. Для візуалізації результатів оцінювання та побудови наочних діаграм розподілу кіберризиків інтегровано JavaScript-бібліотеку Chart.js. Взаємодія між браузером та сервером реалізована за допомогою передачі POST-запитів із формами даних та зворотного отримання динамічних HTML-сторінок або JSON-відповідей. Для забезпечення збереження проміжних результатів та ведення історії розрахунків без перевантаження серверної бази даних розроблено рівень збереження на основі механізму Flask Sessions, що дозволяє безпечно та ефективно оперувати даними користувача в межах поточної сесії.Для забезпечення модульності, масштабованості та чіткої взаємодії між компонентами вебдодатку було розроблено загальну структурну схему системи, яка представлена на рисунку 3.1.

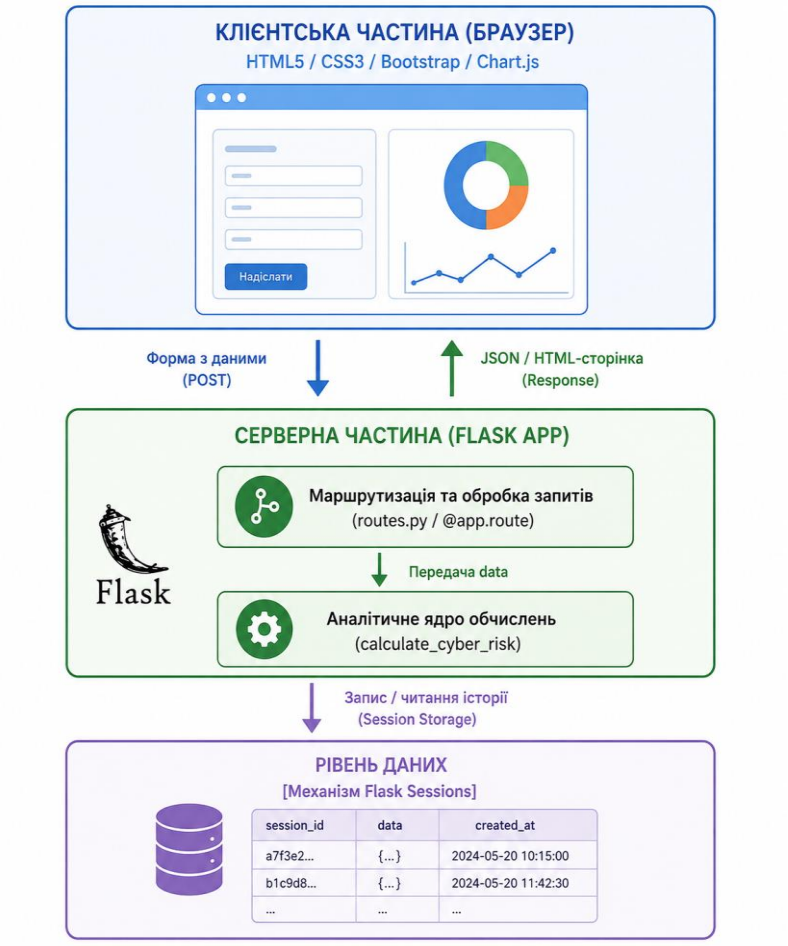


Рисунок 3.1 - Структурна схема функціонування системи

Представлена архітектурна структура наочно відображає рух інформаційних потоків у системі. Клієнтська частина відповідає за рендеринг інтерфейсу, валідацію введених користувачем даних та фінальну графічну візуалізацію ризиків. Серверна частина на базі Flask виступає диспетчером: приймає вхідний HTTP-запит, запускає алгоритм математичного оцінювання та взаємодіє з механізмом сесій для збереження результатів. Рівень даних ізольований у межах криптографічно захищених сесій, що виключає пряме втручання користувача у логіку збереження тимчасової історії оцінок. Така декомпозиція дозволяє модифікувати аналітичні алгоритми або інтерфейс незалежно один від одного.

Основна функціональність системи полягає у проведенні експертної оцінки ризиків для інформаційних активів. Користувач має можливість задати назву активу, визначити рівень його важливості, а також вказати характеристики, що впливають на рівень ризику. До таких характеристик належать доступність ресурсу з мережі Інтернет, наявність конфіденційних даних та кількість користувачів.

Обробка введених даних здійснюється на сервері після надсилання форми користувачем. Отримані параметри передаються до функції оцінювання ризику, яка виконує поетапний аналіз вхідних даних. Після завершення обчислень система формує результат оцінювання ризику та відображає користувачеві відповідні рекомендації щодо рівня інформаційної безпеки.

Лістинг 3.1 - Реалізація функції оцінювання кіберризику

```
def calculate_cyber_risk(data):
asset = data.get('asset_name', 'Unnamed Asset')
impact = int(data.get('importance', 5))
likelihood = 2
if data.get('internet_access'):
likelihood += 3
if data.get('confidential_data'):
likelihood += 3
users = int(data.get('users_count') or 0)
if users > 100:
likelihood += 2
elif users > 10:
likelihood += 1
likelihood = min(10, likelihood)
selected_controls = data.getlist('controls')
mitigation = len(selected_controls) * 1.5
score = max(5, min(100, int(((impact * likelihood) - mitigation) * 1.4)))
return score
```

Даний програмний фрагмент реалізує основну логіку оцінювання кіберризику та є ключовим елементом аналітичного ядра системи. На першому етапі здійснюється визначення рівня впливу активу, який задається користувачем і відображає його критичність для функціонування інформаційної системи або бізнес-процесів. Цей параметр є базовим, оскільки саме від нього залежить потенційний масштаб наслідків у разі реалізації загрози. Наступним кроком є обчислення ймовірності виникнення загроз. Даний показник формується

автоматично на основі введених характеристик, зокрема наявності доступу до системи через мережу Інтернет, обробки конфіденційних даних та кількості користувачів.

Завершальним етапом є формування інтегрального показника ризику, який узагальнює всі попередні розрахунки. Отримане значення нормалізується у визначеному діапазоні та використовується для подальшої класифікації рівня небезпеки. Такий підхід дозволяє отримати уніфікований показник, придатний для порівняння різних активів та прийняття управлінських рішень у сфері інформаційної безпеки.

Таблиця 3.1 - Основні параметри оцінювання кіберризику

Параметр	Опис	Тип даних	Вплив на результат
Назва активу	Унікальний ідентифікатор об’єкта аналізу	Рядок	Інформаційний показник
Важливість	Рівень критичності активу від 1 до 10	Ціле число	Прямий множник у формулі
Internet access	Доступ до системи з мережі Інтернет	Логічний	Підвищує ймовірність на 3 бали
Confidential data	Наявність конфіденційної інформації	Логічний	Підвищує ймовірність на 3 бали
Users count	Кількість користувачів із доступом	Ціле число	Коригує ймовірність на 1 або 2 бали
Security controls	Список впроваджених засобів захисту	Список	Знижує підсумковий бал ризику
Risk score	Підсумковий інтегральний показник	Число	Визначає категорію та стратегію

Описані параметри формують основу моделі оцінювання ризиків. Їх комплексне врахування дозволяє підвищити об’єктивність аналізу та адаптувати систему до реальних умов функціонування інформаційних систем. Клієнтська частина системи реалізована з використанням HTML5, CSS3 та фреймворку

Bootstrap, що забезпечує адаптивність інтерфейсу. Для побудови структури сторінки використано сучасні методи верстки, зокрема Flexbox.

Інтерфейс системи має темну кольорову гаму, що відповідає сучасним тенденціям розробки та покращує сприйняття інформації. Використання шаблонізатора Jinja2 дозволяє динамічно відображати результати обчислень. Для візуалізації результатів використано бібліотеку Chart.js, яка дозволяє будувати інтерактивні графіки. У системі реалізовано радарну діаграму, що відображає ключові параметри ризику.

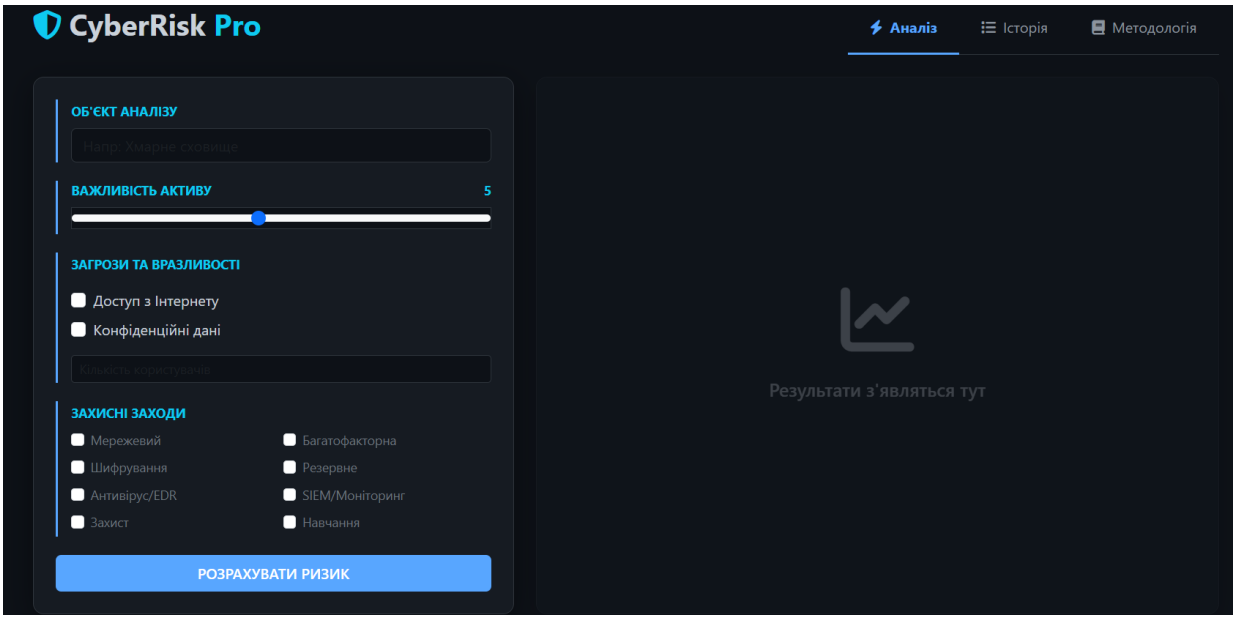


Рисунок 3.2 - Графічний інтерфейс системи

Інтерфейс системи складається з кількох функціональних вкладок, що забезпечують зручну організацію роботи користувача та логічне розділення основних функцій. До ключових розділів належать модуль аналізу, історія оцінок та довідковий блок.

Така структура дозволяє послідовно виконувати всі етапи роботи із системою: введення даних, отримання результатів та перегляд попередніх оцінок. Основна вкладка призначена для введення параметрів інформаційного активу та проведення розрахунку рівня кіберризику. Користувач задає характеристики об’єкта, зокрема його важливість, наявність доступу з мережі Інтернет, роботу з конфіденційними даними, кількість користувачів, а також обрані засоби захисту.

Після надсилання форми дані обробляються на серверній частині, і система формує результат у реальному часі.

Результати аналізу відображаються у вигляді числового значення ризику, що дозволяє кількісно оцінити рівень загрози. Додатково система визначає категорію ризику (низький, середній, високий або критичний), що спрощує інтерпретацію результатів для користувача.

Також формується блок рекомендацій, який залежить від рівня ризику та містить поради щодо підвищення рівня захисту або необхідності негайного реагування. Важливим елементом є кольорова індикація, яка дозволяє швидко візуально оцінити ступінь небезпеки без детального аналізу числових значень.

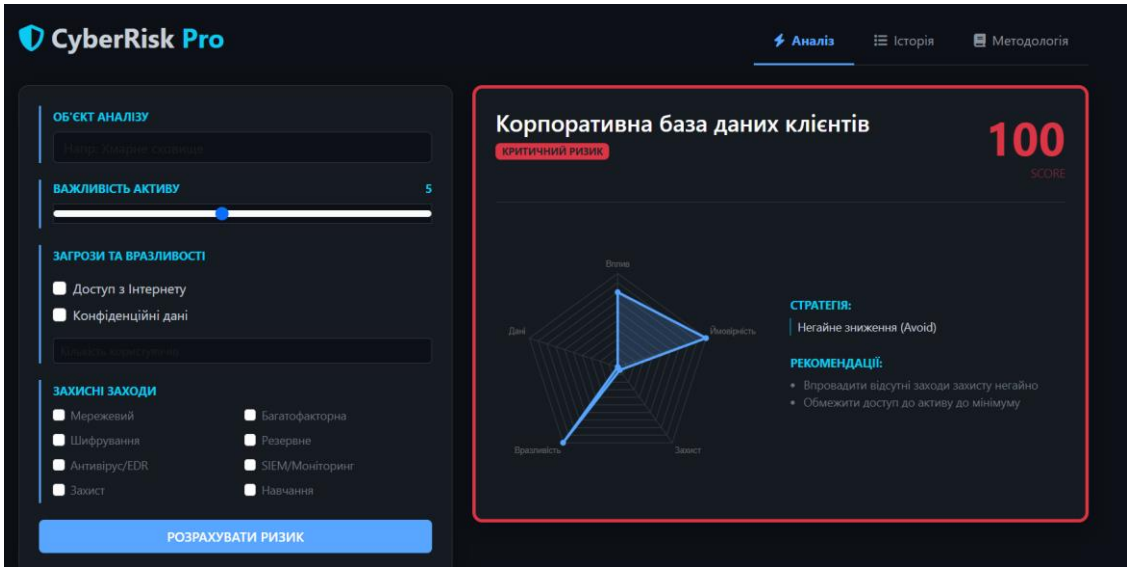


Рисунок 3.3 - Результати оцінки ризиків

Реалізована система забезпечує повний цикл обробки даних, який охоплює всі етапи роботи з інформацією: від введення користувачем початкових параметрів до формування кінцевого аналітичного висновку щодо рівня кіберризику[42]. На етапі введення даних користувач задає характеристики інформаційного активу, після чого система виконує їх автоматизовану обробку на серверній частині. Отримані результати проходять етап аналізу та класифікації, що дозволяє сформувати узагальнену оцінку стану інформаційної безпеки об’єкта.

Важливим елементом реалізації є використання механізму сесій, який дозволяє зберігати історію виконаних оцінок без необхідності застосування

зовнішньої бази даних. Це забезпечує простоту архітектури системи, зменшує навантаження на серверну частину та дозволяє оперативно відображати попередні результати користувача. Історія оцінок використовується для аналізу динаміки змін рівня ризику та порівняння різних сценаріїв безпеки.

Таким чином, обрана архітектура програмного продукту забезпечує високу гнучкість, швидкість обробки запитів та зручність у використанні. Розподіл логіки між серверною та клієнтською частинами дозволяє ефективно організувати процес обробки даних і спрощує подальше масштабування системи. Запропонований підхід дозволяє автоматизувати процес оцінювання ризиків інформаційної безпеки, підвищити точність аналізу та забезпечити більш обґрунтовану підтримку управлінських рішень у сфері кіберзахисту.

3.2 Реалізація основних функцій оцінювання та аналізу ризиків.

Реалізація функціональної частини системи «CyberRisk Pro» базується на використанні мови програмування Python та мікрофреймворку Flask, які забезпечують обробку вхідних даних, виконання розрахунків та формування результатів оцінювання кіберризиків. Основною метою реалізації є створення автоматизованого механізму аналізу ризиків інформаційної безпеки, який дозволяє оперативно оцінювати рівень загроз для інформаційних активів на основі введених параметрів.

Функціональна структура системи побудована за принципом розподілу логіки між серверною та клієнтською частинами. Серверна частина відповідає за аналіз параметрів активу, розрахунок ризику та класифікацію результатів, тоді як клієнтська частина забезпечує введення даних, візуалізацію результатів та взаємодію користувача із системою. Такий підхід дозволяє забезпечити високу швидкість обробки запитів, гнучкість архітектури та зручність подальшого масштабування програмного продукту.

Після запуску системи користувач отримує доступ до вебінтерфейсу, у межах якого задаються параметри інформаційного активу. До основних характеристик

належать назва активу, рівень його важливості, наявність доступу до мережі Інтернет, робота з конфіденційними даними, кількість користувачів та впроваджені засоби захисту. Введені дані передаються до серверної частини через HTTP-запит методом POST та обробляються функцією оцінювання кіберризику.

Лістинг 3.2 - Фрагмент функції оцінювання кіберризику

```
likelihood = 2
if data.get('internet_access'):
    likelihood += 3
if data.get('confidential_data'):
    likelihood += 3
selected_controls = data.getlist('controls')
mitigation = len(selected_controls) * 1.5
score = max(
    5,

    min(100, int(((impact * likelihood) - mitigation) * 1.4))
)
```

Представлений фрагмент коду демонструє основний механізм оцінювання кіберризику в системі «CyberRisk Pro». На першому етапі формується показник ймовірності виникнення загроз, який залежить від характеристик інформаційного активу. Якщо актив має доступ до мережі Інтернет, рівень ймовірності збільшується, оскільки це розширює поверхню потенційної атаки та підвищує ризик несанкціонованого доступу до системи.

Наявність конфіденційної інформації також підвищує показник ймовірності, оскільки подібні дані є пріоритетною ціллю для зловмисників. Таким чином, система враховує як технічні, так і організаційні фактори, що можуть впливати на загальний рівень загроз.

Після визначення рівня ймовірності система аналізує впроваджені засоби захисту. Користувач може обрати один або декілька механізмів безпеки, зокрема міжмережевий екран, багатофакторну автентифікацію, резервне копіювання, шифрування даних або системи моніторингу подій безпеки. Кожен із зазначених

механізмів знижує підсумковий рівень ризику шляхом формування коефіцієнта mitigation.

Отримані результати використовуються для формування інтегрального показника ризику score, який характеризує загальний рівень небезпеки для інформаційного активу. Для забезпечення стандартизації результатів система обмежує значення ризику визначеним діапазоном, що дозволяє спростити подальшу інтерпретацію результатів[43].

Після завершення розрахунків система виконує класифікацію отриманого результату. Якщо значення ризику перевищує критичний поріг, система автоматично визначає рівень небезпеки як критичний та рекомендує негайне застосування заходів захисту. Для високих значень ризику система пропонує стратегію активного керування ризиками, що передбачає посилення механізмів захисту та обмеження доступу до інформаційного активу. У випадку середнього або низького рівня ризику рекомендується підтримання поточного рівня безпеки та проведення регулярного моніторингу.

Крім того, система забезпечує можливість формування детального звіту, який містить вичерпну інформацію про всі етапи аналізу та розраховані показники ризику. Цей звіт є важливим інструментом для документування результатів оцінки та прийняття обґрунтованих рішень щодо стратегії керування ризиками, що дозволяє керівництву та фахівцям з безпеки мати чітке уявлення про поточний стан безпеки інформаційних активів та необхідні заходи захисту. Згенерований звіт може зберігатися в електронному вигляді та використовуватись для подальшого аналізу й аудиту системи інформаційної безпеки. Це дозволяє відстежувати динаміку зміни рівня ризиків упродовж певного періоду часу та оцінювати ефективність впроваджених заходів захисту. Додатково система може забезпечувати автоматичне формування рекомендацій щодо мінімізації виявлених загроз та усунення потенційних вразливостей. Використання автоматизованої звітності сприяє скороченню часу на підготовку аналітичної документації та зменшенню ймовірності помилок під час обробки даних.

Алгоритм роботи системи оцінювання кіберризиків можна представити у вигляді послідовності взаємопов’язаних етапів.

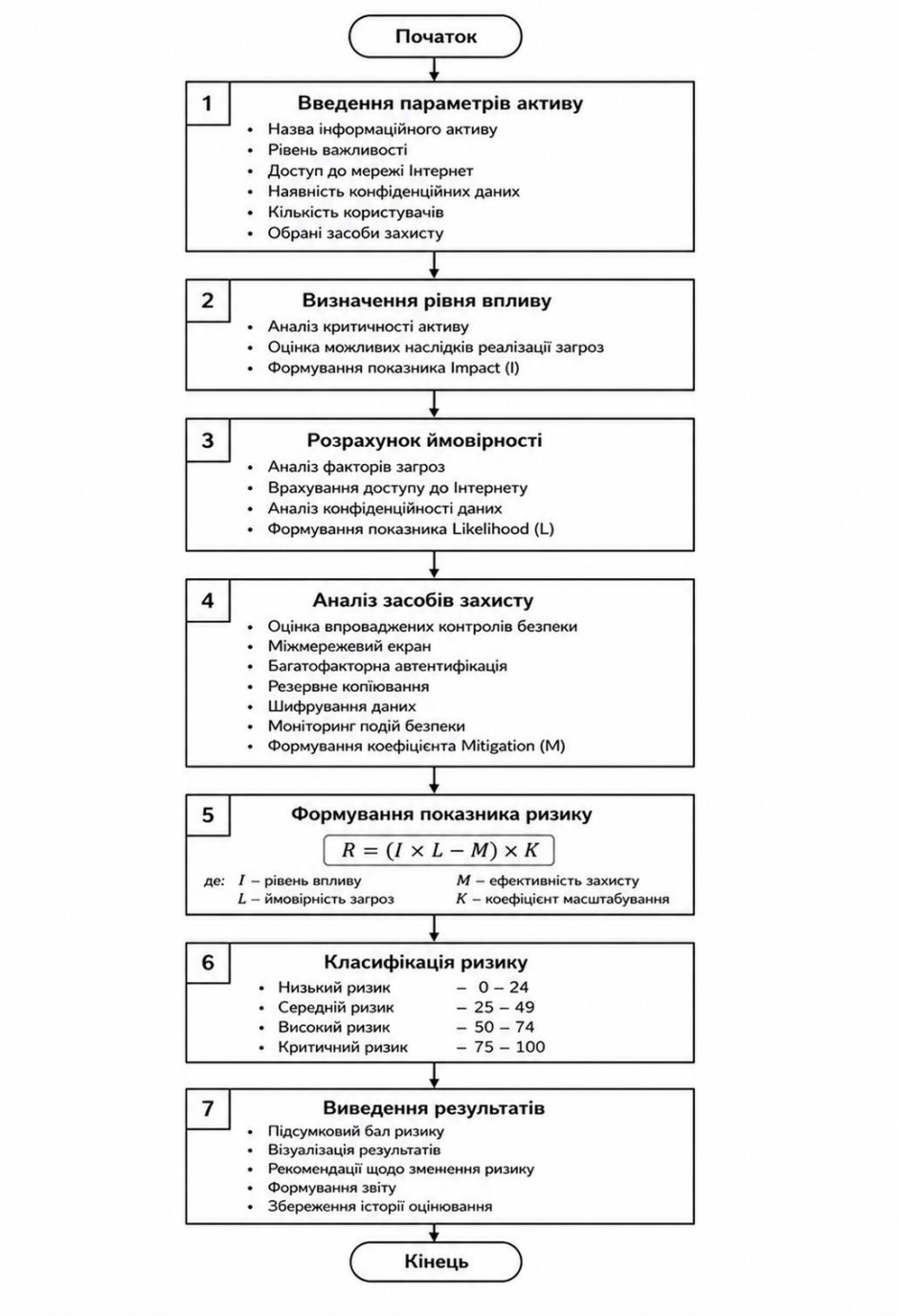


Рисунок 3.3 - Алгоритм оцінювання кіберризику

Подана блок-схема демонструє загальну логіку функціонування системи. На початковому етапі користувач вводить параметри інформаційного активу через вебінтерфейс. Далі система визначає рівень впливу активу та виконує оцінювання ймовірності виникнення загроз залежно від заданих характеристик.

Наступним етапом є аналіз засобів захисту, що дозволяє оцінити рівень захищеності інформаційної системи. Після цього формується інтегральний показник ризику, який класифікується відповідно до встановлених категорій

небезпеки. Завершальним етапом є відображення результатів оцінювання та рекомендацій щодо підвищення рівня інформаційної безпеки.

Важливою складовою функціональної реалізації системи є механізм обробки даних користувача. Flask забезпечує автоматичне приймання параметрів із HTML-форми та передачу їх до серверної логіки. Усі введені значення зберігаються у структурі request.form, після чого система виконує їх аналіз та формує результат оцінювання у режимі реального часу.

Окрему увагу приділено реалізації механізму збереження історії оцінок. Для цього використовується вбудований механізм сесій Flask, який дозволяє тимчасово зберігати результати аналізу без необхідності використання зовнішньої бази даних. Такий підхід спрощує архітектуру системи та дозволяє швидко відображати попередні результати користувача.

Історія оцінок використовується для перегляду попередніх результатів аналізу та порівняння різних сценаріїв захисту інформаційних активів. Система автоматично зберігає останні результати оцінювання, що дозволяє аналізувати зміни рівня ризику залежно від застосованих механізмів безпеки.

Для підвищення інформативності результатів у системі реалізовано механізм графічної візуалізації даних. Для цього використовується бібліотека Chart.js, яка дозволяє будувати інтерактивні графіки безпосередньо у веббраузері користувача. Основним елементом візуалізації є радарна діаграма, що відображає співвідношення між рівнем впливу, ймовірністю виникнення загроз, рівнем захищеності та фінальним показником ризику.

Використання графічної візуалізації дозволяє суттєво покращити сприйняття результатів оцінювання та спростити аналіз стану інформаційної безпеки. Користувач отримує можливість швидко визначити найбільш проблемні аспекти захисту та оцінити ефективність впроваджених заходів безпеки. Крім цього, система використовує кольорову індикацію рівнів ризику. Для низького рівня застосовується зелений колір, для середнього - синій, для високого - жовтий, а для критичного - червоний.

Такий підхід відповідає сучасним принципам UX/UI-дизайну та дозволяє швидко оцінити ступінь небезпеки навіть без детального аналізу числових

показників. Таким чином, реалізована система «CyberRisk Pro» забезпечує автоматизоване оцінювання ризиків інформаційної безпеки шляхом аналізу характеристик інформаційних активів, параметрів загроз та рівня захищеності. Використання Flask, Python та сучасних вебтехнологій дозволило створити гнучкий програмний продукт із можливістю подальшого масштабування функціоналу. Реалізовані алгоритми забезпечують швидке формування результатів оцінювання, їх класифікацію та візуальне представлення, що підвищує ефективність підтримки управлінських рішень у сфері кібербезпеки.

Важливим аспектом реалізованої системи є її адаптивність до різних сценаріїв використання, що досягається завдяки параметричному підходу до оцінювання ризиків. Усі вхідні характеристики інформаційного активу розглядаються як змінні фактори, які можуть бути легко модифіковані або доповнені без необхідності суттєвої зміни архітектури програмного продукту. Така гнучкість дозволяє використовувати систему не лише для базового аналізу кіберризиків, але й для розширених моделей оцінювання у корпоративних інформаційних системах. Окрему роль у функціонуванні системи відіграє механізм динамічного оновлення результатів. Після кожного нового запиту користувача система автоматично виконує перерахунок показників ризику та оновлює відображення результатів у вебінтерфейсі. Це забезпечує інтерактивний характер роботи застосунку, коли користувач одразу бачить вплив зміни будь-якого параметра на фінальний рівень ризику.

Важливим аспектом реалізованої системи є її адаптивність до різних сценаріїв використання, що досягається завдяки параметричному підходу до оцінювання ризиків. Усі вхідні характеристики інформаційного активу розглядаються як змінні фактори, які можуть бути легко модифіковані або доповнені без необхідності суттєвої зміни архітектури програмного продукту. Така гнучкість дозволяє використовувати систему не лише для базового аналізу кіберризиків, але й для розширених моделей оцінювання у корпоративних інформаційних системах. Окрему роль у функціонуванні системи відіграє механізм динамічного оновлення результатів. Після кожного нового запиту користувача система автоматично виконує перерахунок показників ризику та оновлює

відображення результатів у вебінтерфейсі. Це забезпечує інтерактивний характер роботи застосунку, коли користувач одразу бачить вплив зміни будь-якого параметра на фінальний рівень ризику.

З точки зору безпеки реалізованого рішення, важливим є те, що всі обчислення виконуються на серверній стороні, що виключає можливість маніпуляції результатами з боку клієнта. Користувач має доступ лише до інтерфейсу введення даних та перегляду результатів, тоді як логіка розрахунків залишається прихованою на сервері. Це відповідає базовим принципам побудови безпечних вебзастосунків. Додатково у системі реалізовано механізм обмеження значень ризику, що дозволяє уникнути некоректних або надмірно великих результатів. Навіть у випадку екстремальних значень вхідних параметрів фінальний показник приводиться до заданого діапазону, що забезпечує узгодженість результатів та їх придатність для подальшого аналізу.

З точки зору практичного застосування, розроблена система може бути використана як навчальний інструмент для вивчення основ оцінювання кіберризиків, а також як прототип для побудови більш складних систем управління інформаційною безпекою. Завдяки простій структурі та зрозумілому інтерфейсу вона може бути легко адаптована під потреби різних організацій. Таким чином, функціональна реалізація системи «CyberRisk Pro» демонструє можливість ефективного поєднання простих математичних моделей оцінювання ризику з сучасними вебтехнологіями. Використання Python та Flask дозволило реалізувати компактну, але функціонально повноцінну систему, яка забезпечує автоматизований аналіз кіберризиків, їх класифікацію та візуалізацію результатів у зручному для користувача форматі[44].

3.3 Організація та результати тестування системи

Тестування програмної системи є завершальним етапом розробки, який дозволяє перевірити коректність роботи алгоритму оцінювання кіберризиків, стабільність функціонування вебзастосунку та відповідність отриманих

результатів логіці реалізованої моделі. Основною метою тестування є підтвердження правильності обчислювальних процедур, перевірка взаємодії між клієнтською та серверною частинами системи.

Для забезпечення об’єктивності та відтворюваності результатів, комплекс випробувань розробленного вебдодатку «CyberRisk Pro» проводився у контрольованому тестовому середовищі, що мало наступні апаратні та програмні характеристики:

- апаратна платформа (Host PC): Процесор Intel Core i5 (4 ядра, 2.5 ГГц), 16 ГБ оперативної пам'яті DDR4, накопичувач SSD NVMe;
- операційна система: Microsoft Windows 11 Pro (версія 23H2) / Ubuntu 22.04 LTS;
- базове програмне оточення: Інтерпретатор Python 3.10.12, вебфреймворк Flask 3.0.2, Werkzeug 3.0.1;
- середовище виконання клієнтської частини: Веббраузер Google Chrome (версія 122.0) та Mozilla Firefox (версія 123.0) із увімкненою консоллю розробника (DevTools) для моніторингу HTTP-запитів.

У межах випробувань перевірялася здатність системи коректно обробляти різні сценарії використання, включаючи як повністю заповнені форми, так і частково введені дані. Це дозволило оцінити стійкість алгоритму до варіативності вхідної інформації та його поведінку в умовах неповної інформації.

Особливу увагу під час тестування було приділено перевірці базового математичного алгоритму розрахунку ризику. Для цього було спроєктовано та реалізовано п'ять цільових тестових сценаріїв, які імітують реальні умови експлуатації системи та різні типи інформаційних активів підприємства:

- сценарій №1 (Критичний незольований актив): Моделювання ситуації, коли актив має найвищу важливість (Impact=9), відкритий безпосередній доступ із мережі Інтернет (Internet=true), але при цьому на підприємстві повністю відсутні будь-які налаштовані засоби захисту (controls=0). Очікується максимальний сплеск рівня ризику до критичної зони.
- сценарій №2 (Захищений актив середньої критичності): Перевірка роботи системи компенсації ризиків. Задається середній рівень важливості (Impact=6),

проте користувач вказує наявність трьох активованих комплексних засобів безпеки (controls=3), наприклад, шифрування, 2FA та антивірус. Очікується зниження підсумкового бала до помірного (середнього) рівня.

- сценарій №3 (Локальний актив низького рівня ризику): Тестування внутрішнього ізольованого ресурсу з мінімальною важливістю (Impact=3) та невеликою кількістю локальних користувачів (users=10) за повної відсутності зовнішніх загроз. Очікується стійка фіксація низького рівня ризику.

- сценарій №4 (Надкритичний публічний ресурс): Найбільш агресивний сценарій «найгіршого випадку» (Worst-Case Scenario). Об'єкт має максимальну важливість (Impact=10), містить персональні або комерційні дані та підключений до глобальної мережі без використання міжмережевих екранів чи систем резервування. Очікується граничне значення Risk score.

- сценарій №5 (Критичний актив із максимальним захистом): Перевірка ефективності повноцінного комплексу безпеки (Defense in Depth). Об'єкт із високою важливістю (Impact=7) захищений максимальною кількістю доступних у формі контролів (controls=5). Перевіряється здатність системи адекватно нівелювати загрози за рахунок впроваджених технологій безпеки.

Логіка обробки цих сценаріїв спирається на програмний алгоритм, фрагмент якого наведено нижче.

Лістинг 3.3 - Фрагмент алгоритму оцінювання ризику

```
likelihood = 2
if data.get('internet_access'):
    likelihood += 3
if data.get('confidential_data'):
    likelihood += 3
selected_controls = data.getlist('controls')
mitigation = len(selected_controls) * 1.5
score = max(5, min(100, int(((impact * likelihood) - mitigation) * 1.4)))
```

Наведений фрагмент демонструє основну логіку формування інтегрального показника кіберризику. На першому етапі визначається рівень впливу активу, який

задається користувачем. Далі розраховується ймовірність виникнення загроз, що залежить від наявності доступу до Інтернету, конфіденційності даних та кількості користувачів. Після цього враховується рівень захисту, який зменшує фінальний показник ризику залежно від кількості активованих засобів безпеки. Отримане значення нормалізується у заданому діапазоні, що забезпечує уніфікованість результатів. Аналіз наведених даних свідчить, що автоматизована система коректно реагує на зміну вхідних параметрів та забезпечує стабільну збіжність результатів оцінювання. Для перевірки коректності роботи системи було сформовано набір тестових сценаріїв, які відображають типові варіанти використання програмного продукту. Результати тестування наведені в таблиці 3.2.

Таблиця 3.2 - Результати тестування системи

№	Вхідні дані	Очікуваний результат	Фактичний результат	Статус
1	Impact=9, Internet=true, controls=0	Критичний ризик	80+ балів, критичний	✓
2	Impact=6, controls=3	Середній ризик	~40 балів	✓
3	Impact=3, users=10	Низький ризик	~15–20 балів	✓
4	Impact=10, Internet=true, no controls	Критичний ризик	>85 балів	✓
5	Impact=7, controls=5	Середній ризик	~30–35 балів	✓

Результати тестування підтверджують, що система коректно реагує на зміну вхідних параметрів. Додатково було встановлено, що система демонструє стабільну роботу навіть при відсутності окремих вхідних параметрів, оскільки передбачено використання значень за замовчуванням. Це дозволяє уникнути помилок виконання та підвищує надійність програмного продукту в реальних умовах експлуатації. Зокрема, збільшення рівня важливості активу та наявність факторів ризику призводить до зростання фінального показника, тоді як

збільшення кількості засобів захисту знижує загальний рівень ризику. Це свідчить про правильність реалізації математичної моделі оцінювання.

Також було перевірено коректність роботи механізму класифікації ризику, який поділяє результати на чотири рівні: низький, середній, високий та критичний. Усі тестові сценарії були класифіковані відповідно до встановлених порогових значень, що підтверджує стабільність логіки прийняття рішень у системі.

Окремо проведено тестування користувацького інтерфейсу, включаючи введення даних через вебформу, перемикання вкладок та відображення результатів. Інтерфейс працює стабільно, елементи відображаються коректно, а результати аналізу з'являються одразу після виконання розрахунку. Особливу увагу було приділено перевірці модуля історії оцінок, який реалізує журнал останніх результатів аналізу. Даний модуль дозволяє користувачу переглядати попередні оцінки без повторного введення даних. Реалізація базується на використанні механізму сесій Flask, що дозволяє зберігати дані без застосування зовнішньої бази даних. У ході тестування встановлено, що кожна нова оцінка автоматично додається до списку історії, а кількість записів обмежується останніми десятьма результатами.

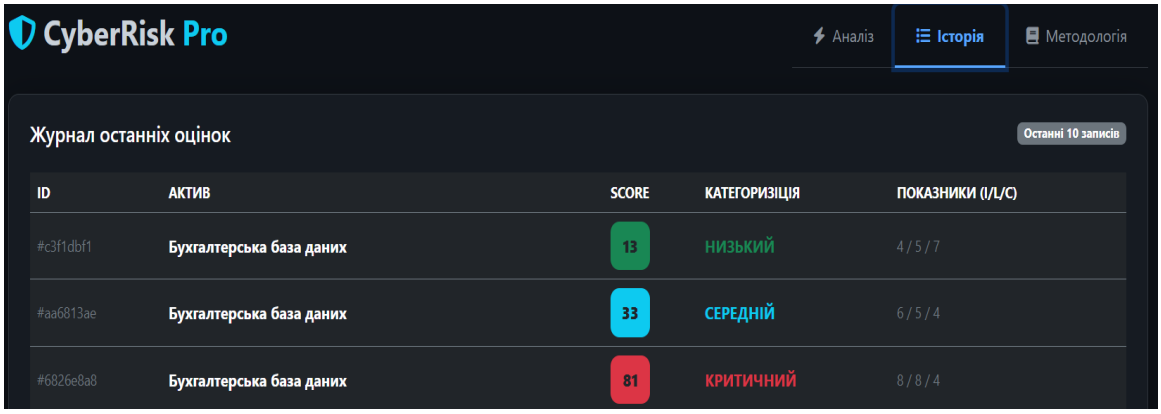


Рисунок 3.3 - Журнал останніх оцінок ризику (вкладка Історія)

Результати перевірки показали, що модуль історії працює стабільно та дозволяє аналізувати зміну рівня ризику для різних сценаріїв використання системи. Це підвищує аналітичну цінність програмного продукту та робить його зручним для практичного застосування[45].

Загалом проведене тестування підтвердило, що програмна система функціонує стабільно, усі основні модулі працюють коректно, алгоритм оцінювання є логічно узгодженим, а інтерфейс забезпечує зручну взаємодію користувача із системою. Отримані результати свідчать про готовність системи до практичного використання та можливість її подальшого вдосконалення.

Додатково слід відзначити, що реалізована система має достатній рівень гнучкості та може бути адаптована до розширення функціональних можливостей у майбутньому. Зокрема, архітектура програми дозволяє інтеграцію нових типів захисних механізмів, ускладнення моделі оцінювання ризику, а також підключення зовнішніх джерел даних для більш точного аналізу загроз. Це створює передумови для подальшого розвитку програмного продукту.

Крім того, результати тестування підтвердили коректність реалізації логіки взаємодії між вхідними параметрами та фінальним показником ризику. Зокрема, було встановлено, що система демонструє передбачувану поведінку при зміні окремих факторів, що свідчить про правильність побудованої моделі та її узгодженість із принципами оцінювання ризиків інформаційної безпеки. Це дозволяє розглядати систему як надійний інструмент для первинної експрес-оцінки стану захищеності інформаційних активів.

Також доцільним напрямом подальшого розвитку є удосконалення аналітичної складової системи шляхом застосування більш складних методів оцінювання ризиків, зокрема ймовірнісних або статистичних моделей. Це дозволить підвищити точність результатів та забезпечити більш глибокий аналіз стану інформаційної безпеки. Крім того, потенційним напрямом є впровадження механізмів машинного навчання для адаптивного коригування вагових коефіцієнтів моделі залежно від накопиченої історії оцінок. Таким чином, можна стверджувати, що реалізована система не лише виконує поставлені завдання з оцінювання кіберризиків, але й має значний потенціал для подальшого вдосконалення. Перспективним кроком також є автоматизація формування звітів за результатами моделювання ризиків для полегшення роботи аудиторів. Це дозволить суттєво скоротити час на підготовку підсумкової документації та спростить ухвалення рішень керівництвом.

3.4 Висновки до розділу

У межах третього розділу було здійснено практичну реалізацію та тестування веборієнтованої системи оцінювання кіберризиків. Розглянуто структуру програмного забезпечення, описано основні принципи побудови серверної та клієнтської частин, а також наведено логіку взаємодії між ними. Особливу увагу приділено реалізації алгоритму оцінювання ризику, який базується на врахуванні впливу активу, ймовірності виникнення загроз та рівня впроваджених засобів захисту. У процесі розробки було також приділено увагу забезпеченню масштабованості системи, що дозволяє в подальшому розширювати її функціональні можливості без суттєвих змін архітектури. Окремо враховано принцип модульності, який забезпечує логічне розділення основних компонентів системи та спрощує їх супровід. Крім того, реалізовані рішення сприяють підвищенню надійності обробки даних та зменшують ймовірність виникнення помилок під час виконання розрахунків. Важливим аспектом є також забезпечення швидкої реакції системи на дії користувача, що позитивно впливає на загальну зручність її використання.

У процесі реалізації було використано мову програмування Python та мікрофреймворк Flask, що забезпечило простоту розробки та гнучкість архітектури. Клієнтська частина системи побудована із застосуванням HTML, CSS та Bootstrap, що дозволило створити адаптивний та зручний інтерфейс користувача. Для візуалізації результатів використано бібліотеку Chart.js, яка забезпечує наочне представлення ключових показників ризику у вигляді графічних елементів.

Окремо реалізовано функціонал збереження історії оцінок ризику за допомогою механізму сесій, що дозволяє користувачу переглядати попередні результати без використання зовнішньої бази даних. Алгоритм оцінювання ризику демонструє логічно узгоджену поведінку при зміні вхідних параметрів, а результати розрахунків відповідають очікуваній моделі. Перевірка крайових сценаріїв показала стабільність роботи системи навіть при максимальних та мінімальних значеннях вхідних даних.

ВИСНОВКИ

У ході виконання дипломної роботи було розглянуто та реалізовано веборієнтовану систему оцінювання кіберризиків, призначену для автоматизованого аналізу рівня загроз інформаційних активів. Актуальність теми зумовлена постійним зростанням кількості кіберзагроз та необхідністю використання інструментів, які дозволяють швидко, формалізовано та об’єктивно оцінювати рівень ризику в інформаційних системах і підтримувати прийняття управлінських рішень у сфері кібербезпеки.

У першому розділі було проведено аналіз предметної області, розглянуто основні поняття та підходи до оцінювання кіберризиків, а також визначено ключові фактори, що впливають на рівень загрози. Серед них: критичність інформаційного активу, наявність вразливостей, доступність системи через мережу Інтернет, обсяг користувачів та рівень впроваджених засобів захисту. На основі проведеного аналізу обґрунтовано доцільність розробки автоматизованої системи, яка дозволяє уніфікувати процес оцінювання ризиків та зменшити суб’єктивність експертних рішень.

У другому розділі було розроблено математичну модель оцінювання кіберризику, яка базується на взаємодії трьох основних компонентів: впливу активу, ймовірності реалізації загроз та рівня захищеності. Запропонований підхід дозволяє отримати інтегральний числовий показник ризику, що забезпечує можливість порівняння різних інформаційних активів між собою. Також визначено принципи нормалізації результатів та їх подальшої класифікації за рівнями небезпеки, що спрощує інтерпретацію отриманих значень.

У третьому розділі було здійснено програмну реалізацію системи з використанням мови програмування Python та мікрофреймворку Flask. Розроблено серверну та клієнтську частини вебзастосунку, реалізовано алгоритм розрахунку кіберризику, механізм класифікації результатів, а також функціонал збереження історії оцінок. Проведене тестування підтвердило коректність роботи всіх основних модулів системи та стабільність її функціонування в різних сценаріях використання.

Результати тестування показали, що система адекватно реагує на зміну вхідних параметрів: при збільшенні рівня загроз значення ризику зростає, тоді як при впровадженні додаткових засобів захисту - зменшується. Це підтверджує правильність реалізованої логіки розрахунку та її відповідність теоретичній моделі. Також встановлено, що користувацький інтерфейс є зручним та інтуїтивно зрозумілим, забезпечує коректне відображення результатів та швидку взаємодію з системою.

Загалом розроблена система дозволяє автоматизувати процес оцінювання кіберризиків, підвищує швидкість та об’єктивність аналізу інформаційних активів, а також забезпечує наочне представлення результатів. Отримані результати підтверджують, що поставлені завдання дипломної роботи виконано у повному обсязі, а мета досягнута. Система може бути використана як навчальний інструмент або як базова платформа для подальшого розширення функціональних можливостей у сфері інформаційної безпеки.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2163-VIII / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 21.05.2026).

2. Про критичну інфраструктуру: Закон України від 16.11.2021 р. № 1882-IX / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/1882-20 (дата звернення: 21.05.2026).

3. ДСТУ ISO/IEC 27005:2024 (ISO/IEC 27005:2022, IDT) Інформаційні технології. Методи захисту та забезпечення безпеки. Керівні вказівки щодо управління ризиками інформаційної безпеки. [Чинний від 2024-01-01]. Київ: ДП «УкрНДНЦ», 2024. 72 с.

4. Складанний П. М. Підхід до оцінювання ризиків інформаційної безпеки для автоматизованої системи класу «1». Кібербезпека: освіта, наука, техніка. 2020. URL: https://www.csecurity.kubg.edu.ua/index.php/journal/article/view/224 (дата звернення: 21.05.2026).

5. NIST Special Publication 800-30 Revision 1. Guide for Conducting Risk Assessments / National Institute of Standards and Technology. Gaithersburg, MD, 2012. 95 p. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf (дата звернення: 21.05.2026).

6. ДСТУ EN ISO/IEC 27000:2022 Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Огляд і словник термінів. URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=103330 (дата звернення: 21.05.2026).

7. Правила забезпечення інформаційної безпеки в банківській системі України: Затверджено Постановою Правління Національного банку України від 30.12.2023 р. № 195. URL: https://bank.gov.ua/ (дата звернення: 21.05.2026).

8. ДСТУ ISO 9001:2015 (ISO 9001:2015, IDT) Системи управління якістю. Вимоги. Видання офіційне. Київ: ДП «УкрНДНЦ», 2016. 32 с.

9. Баранов О. А. Інформаційне право та кібербезпека: монографія. Харків: Право, 2023. 288 с.

10. Шніцер М. Й., Скулиш М. А. Соціальна інженерія як загроза інформаційній безпеці: методи протидії та аналіз ризиків. Кібербезпека: освіта, наука, техніка. 2024. Т. 3, № 15. С. 84–97.

11. ДСТУ IEC 31010:2022 (IEC 31010:2019, IDT) Керування ризиками. Методи оцінювання ризиків. Київ: ДП «УкрНДНЦ», 2023. 96 с.

12. Rowe G., Wright G. The Delphi technique: Past, present, and future. International Journal of Forecasting. 2011. Vol. 27, No. 1. P. 1–11. URL: https://doi.org/10.1016/j.ijforecast.2010.05.019 (дата звернення: 18.05.2026).

13. Довгий С. О., Бідюк П. І., Трофимчук О. М. Системи підтримки прийняття рішень на основі статистично-імовірнісних та нечітких методів: монографія. Київ: КВІЦ, 2021. 416 с. URL: https://ela.kpi.ua/server/api/core/bitstreams/2ee0fdc1-0914-4ec7-886a-9cd8d3de50ef/content (дата звернення: 21.05.2026).

14. Субач І. Є., Оленєв Д. Г. Комбінована методика оцінювання компетентності експертів при виборі сценарію організації інформаційно-психологічного впливу. Реєстрація, зберігання і обробка даних. 2020. Т. 22, № 1. С. 64–75. URL: https://surl.li/iexrhh (дата звернення: 21.05.2026).

15. Тітова В., Кльоц Ю., Колба К., Сиротенко Д. Методика оцінювання ризиків інформаційної безпеки фінансової установи. Measuring and computing devices in technological processes. 2025. № 84-14. DOI: 10.31891/2219-9365-2025-84-14. URL: https://www.researchgate.net/publication/399630221_METODIKA_OCINUVANNA_RIZIKIV_INFORMACIJNOI_BEZPEKI_FINANSOVOI_USTANOVI (дата звернення: 22.05.2026).

16. Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy / National Institute of Standards and Technology. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf (дата звернення: 22.05.2026).

17. Caralli R. A., Stevens J. F., Young L. R. Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process. Pittsburgh: Carnegie

Mellon University, Software Engineering Institute, 2007. URL: https://www.sei.cmu.edu/documents/786/2007_005_001_14885.pdf (дата звернення: 22.05.2026).

18. Цілюрик В. Г. Управління ризиками інформаційної безпеки: навчальний посібник. Київ: КПІ ім. Ігоря Сікорського, 2021. 142 с.

19. Управління ризиками в кібербезпеці: навчальний посібник / В. Б. Толубко, Л. Н. Беркман, В. О. Хорошко, С. В. Чиж. Київ: ДУІКТ, 2023. 246 с. URL: https://duikt.edu.ua/uploads/p_2626_38605375.pdf (дата звернення: 22.05.2026).

20. Моделі та методи прийняття рішень: навчальний посібник / В. Б. Толубко, Л. Н. Беркман, В. О. Хорошко, В. М. Назаренко. Київ: ДУІКТ, 2023. 204 с. URL: https://duikt.edu.ua/ua/lib/1/category/2327/view/2038 (дата звернення: 22.05.2026).

21. Брановицький І. С., Сєвєрінов О. В. Проектування та реалізація інформаційних систем на основі мікросервісної архітектури. Сучасні інформаційні системи. 2022. Т. 6, № 2. С. 45–52.

22. Saaty T. L. Decision Making with the Analytic Hierarchy Process. International Journal of Services Sciences. 2008. Vol. 1, No. 1. P. 83–98. URL: https://www.inderscienceonline.com/doi/abs/10.1504/IJSSCI.2008.017590 (дата звернення: 22.05.2026).

23. Гайдур Г. І., Скубак О. М. Моделювання ризиків інформаційної безпеки в корпоративних системах. Наукоємні технології. 2021. Т. 50, № 2. С. 143–151. DOI: 10.18372/2310-5461.50.15582.

24. Landoll D. J. The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments. 3rd ed. Boca Raton: CRC Press, 2021. 512 p.

25. FAIR Institute. Factor Analysis of Information Risk (FAIR) Framework. URL: https://www.fairinstitute.org/what-is-fair (дата звернення: 22.05.2026).

26. NIST Risk Management Framework (RMF) Overview / National Institute of Standards and Technology. URL: https://csrc.nist.gov/projects/risk-management/risk-management-framework-rmf-overview (дата звернення: 22.05.2026).

27. Петровський О. В., Кузнецова Т. М. Метод експертних оцінок: теорія та практика застосування в інформаційних системах. Комп’ютерні науки та

інженерія. 2022. Т. 14, № 1. С. 45–53.

28. Керування ризиком. Методи загального оцінювання ризику URL: https://antycorportal.nazk.gov.ua/images/data/upravlinna-rizikami/korisni-materiali/UA-dstu-31010.pdf (Дата звернення: 22.05.2026).

29. Методи експертних оцінок // Теорія систем і системний аналіз: навчальні матеріали. URL: https://stud.com.ua/98112/informatika/metodi_ekspertnih_otsinok (дата звернення: 22.05.2026).

30. Метод експертної оцінки інформаційних ризиків в ІТ-проєктах // Репозитарій Черкаського державного технологічного університету. URL: https://er.chdtu.edu.ua/handle/ChSTU/4631 (дата звернення: 23.05.2026).

31. Ротштейн О. П. Інтелектуальні технології моделювання: нечітка логіка, генетичні алгоритми, нейронні мережі. Вінниця: ВНТУ, 2017. 342 с.

32. Фінансове прогнозування: електронний посібник. URL: https://surl.li/jhfdsx (дата звернення: 23.05.2026).

33. Коефіцієнт конкордації // Wiki ТНТУ. URL: https://wiki.tntu.edu.ua/%D0%9A%D0%BE%D0%B5%D1%84%D1%96%D1%94%D0%BD%D1%82_%D0%BA%D0%BE%D0%BD%D0%BA%D0%BE%D1%80%D0%B4%D0%B0%D1%86%D1%96%D1%97 (дата звернення: 23.05.2026).

34. Синявська О. О., Тегза А. М. Застосування рангових коефіцієнтів для оцінки узгодженості рейтингів за різними факторами. URL: https://ela.kpi.ua/server/api/core/bitstreams/b999a81f-bb9c-4b87-a101-470e253ae578/content (дата звернення: 21.05.2026).

35. Фінансове прогнозування : електронний посібник. URL: https://surl.li/jhfdsx (дата звернення: 21.05.2026).

36. Сейсебаєва К. В. Системний аналіз ризиків інформаційної безпеки: моделі, методи та засоби автоматизації. Захист інформації. 2022. Т. 24, № 3. С. 145–154.

37. Лебідь О. В., Самохвалов Ю. Я. Обґрунтування управлінських рішень у сфері кібербезпеки на основі агрегованих експертних знань. Сучасні інформаційні технології у сфері безпеки та оборони. 2023. № 1 (46). С. 67–74. DOI:

10.33099/2311-7249.2023.1.67-74.

38. Тімошин А., Каленіченко Л., Гнусов Ю., Хавіна І., Цуранов М., Довгань І. Інтегрована модель управління ризиками інформаційної безпеки на основі AHP та Байєсових мереж. Innovative technologies and scientific solutions for industries. 2025. No. 3 (33). P. 166–175. DOI: https://doi.org/10.30837/2522-9818.2025.3.166

39. Бурячок В. Л., Толубко В. Б., Хорошко В. О., Толюпа С. В. Інформаційна та кібербезпека: соціотехнічний аспект: підручник. Київ: Державний университет телекомунікацій, 2015. 288 с.

40. Grinberg M. Flask Web Development: Developing Web Applications with Python. 2nd ed. Sebastopol: O'Reilly Media, 2018. 316 p.

41. Bootstrap Documentation. URL: https://getbootstrap.com/docs/ (дата звернення: 21.05.2026).

42. Chart.js Documentation. URL: https://www.chartjs.org/docs/latest/ (дата звернення: 21.05.2026).

43. Flask Documentation. URL: https://flask.palletsprojects.com/ (дата звернення: 21.05.2026).

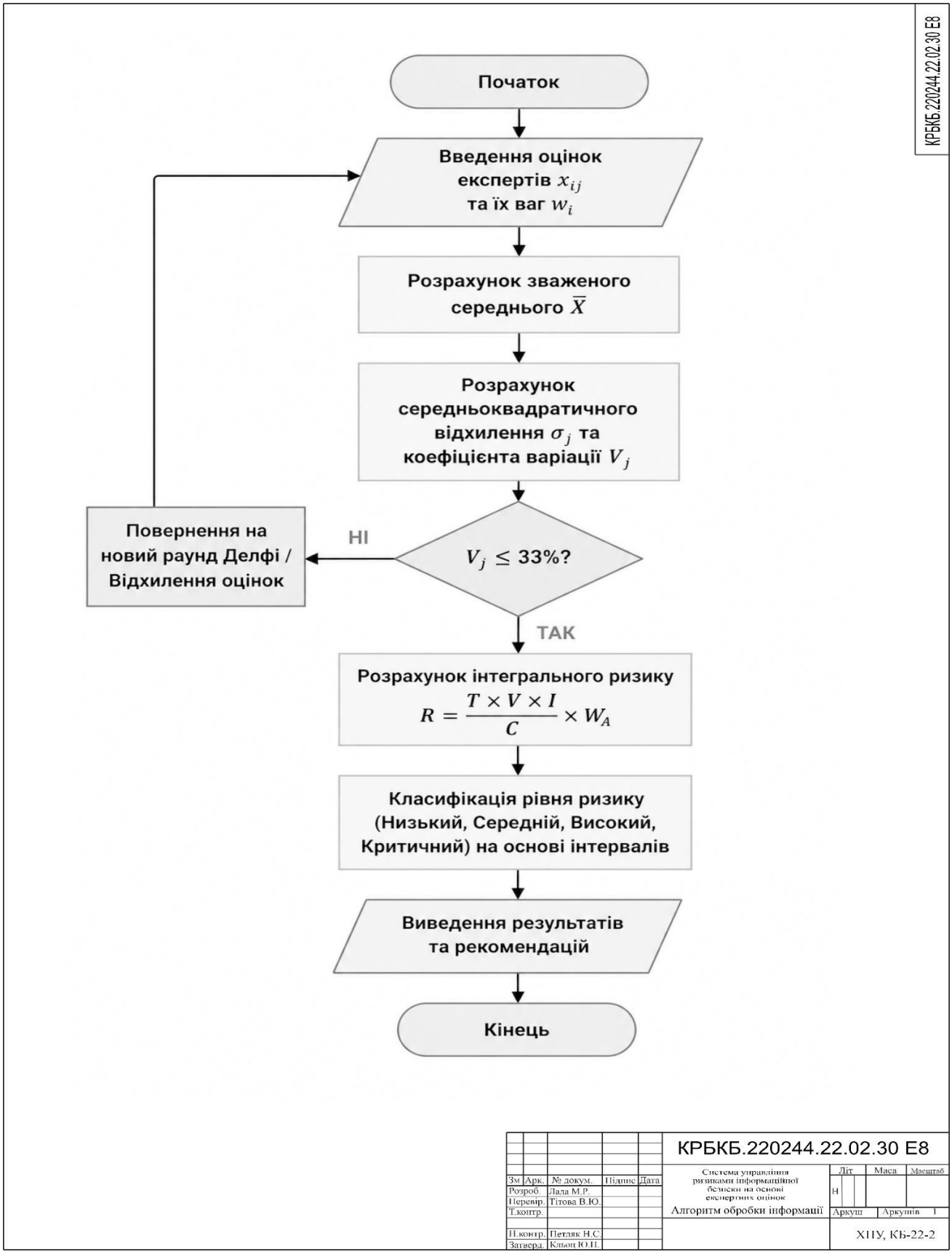
44. Jinja Documentation. URL: https://jinja.palletsprojects.com/ (дата звернення: 21.05.2026).

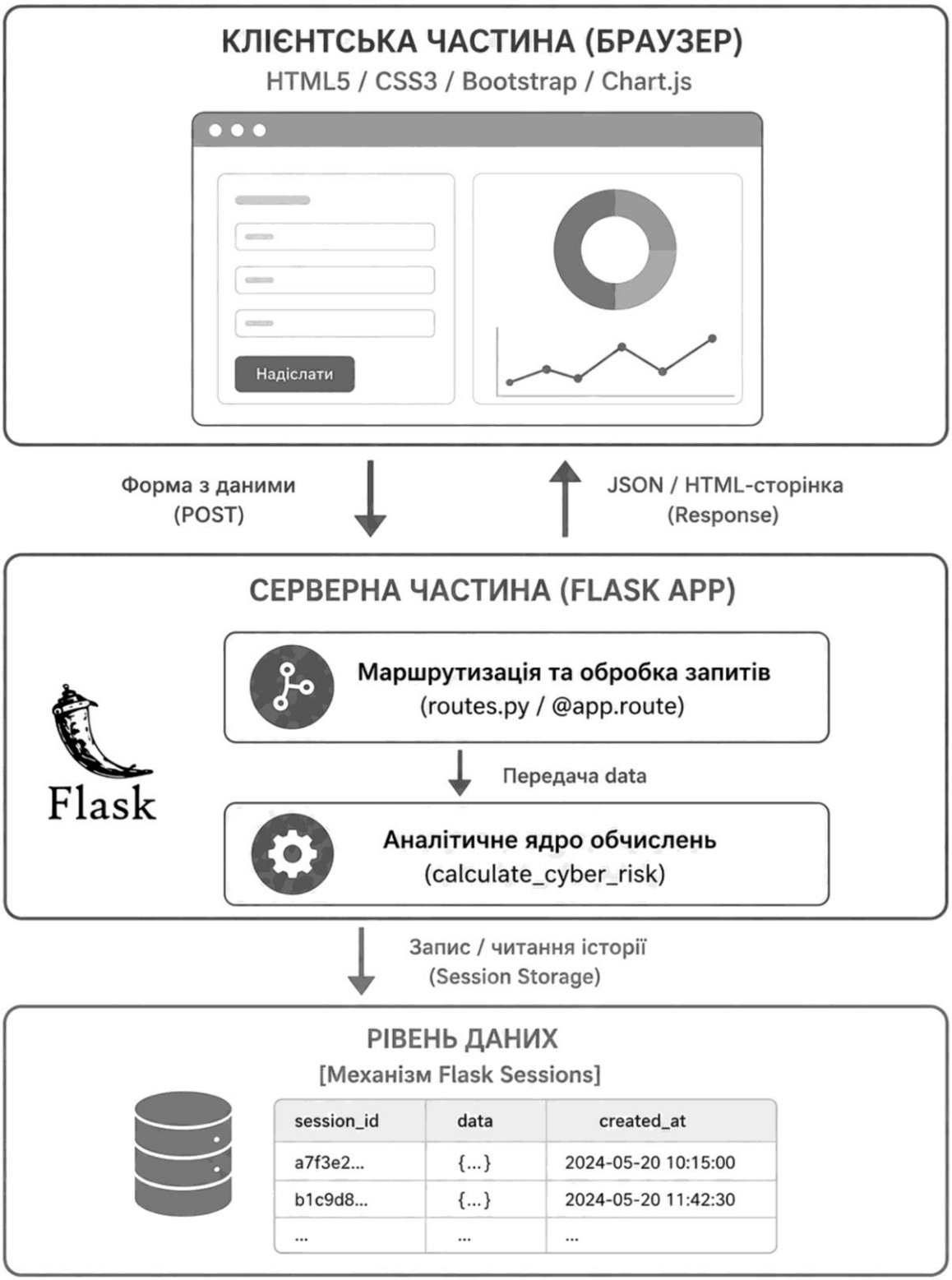
45. Катренко А. В., Пасічник В. В. Тестування та забезпечення якості програмного забезпечення: підручник. Львів: Новий Світ-2000, 2020. 280 с.

Додаток А

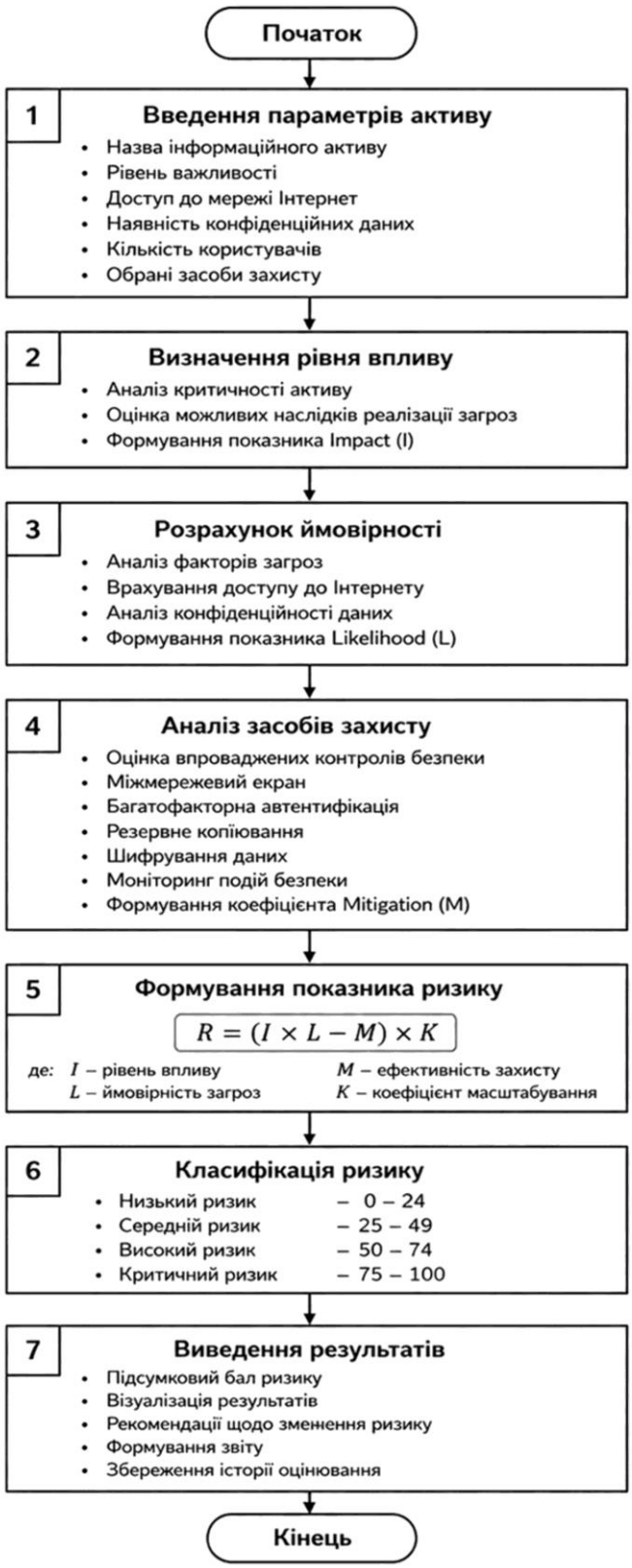
(обов’язковий)

Копія графічної частини





					КРБКБ.220244.22.02.30 Е8	
Зм	Арк.	№ докум.	Підпис	Дата	Система управління ризиками інформаційної безпеки на основі експертних оцінок	Літ / Маса / Масштаб
Розроб.		Лада М.Р.				Н
Перевір.		Тітова В.Ю.			Структурна схема	Аркуш / Аркушів 1
Т.контр.						
Н.контр.		Петляк Н.С.				ХНУ, КБ-22-2
Затверд.		Кльоц Ю.П.				



					КРБКБ.220244.22.02.30 Е8	
Зм	Арк.	№ докум.	Підпис	Дата	Система управління ризиками інформаційної безпеки на основі експертних оцінок	Літ / Маса / Масштаб
Розроб.		Лада М.Р.				Н
Перевір.		Тітова В.Ю.				
Т.контр.					Алгоритм оцінювання кіберризику	Аркуш / Аркушів 1
Н.контр.		Петляк Н.С.				ХНУ, КБ-22-2
Затверд.		Кльоц Ю.П.				

Додаток Б

Код програми

```
from flask import Flask, render_template, request, session
import uuid

app = Flask(__name__)
app.secret_key = 'cyber_security_pro_key' # Ключ для збереження історії в браузері

# Доступні засоби контролю (Security Controls)
SECURITY_CONTROLS = {
    'firewall': 'Мережевий екран (Firewall)',
    'mfa': 'Багатофакторна автентифікація',
    'encryption': 'Шифрування (AES-256)',
    'backup': 'Резервне копіювання (3-2-1)',
    'antivirus': 'Антивірус/EDR система',
    'logging': 'SIEM/Моніторинг подій',
    'ips': 'Захист від вторгнень (IPS)',
    'training': 'Навчання персоналу'
}

def calculate_cyber_risk(data):
    """Логіка розрахунку ризику"""
    asset = data.get('asset_name', 'Unnamed Asset')
    impact = int(data.get('importance', 5))

    # Розрахунок ймовірності (Likelihood)
    likelihood = 2
    if data.get('internet_access'): likelihood += 3
    if data.get('confidential_data'): likelihood += 3

    users = int(data.get('users_count') or 0)
    if users > 100: likelihood += 2
    elif users > 10: likelihood += 1
    likelihood = min(10, likelihood)

    # Вплив засобів захисту (Mitigation)
    selected_controls = data.getlist('controls')
    mitigation = len(selected_controls) * 1.5

    # Формула ризику
```

```
    score = max(5, min(100, int(((impact * likelihood) - mitigation) * 1.4)))

    # Категоризація
    if score >= 75:
        cat, col, strat = "КРИТИЧНИЙ", "danger", "Негайне зниження (Avoid)"
    elif score >= 45:
        cat, col, strat = "ВИСОКИЙ", "warning", "Активне керування (Mitigate)"
    elif score >= 20:
        cat, col, strat = "СЕРЕДНІЙ", "info", "Постійний моніторинг (Accept)"
    else:
        cat, col, strat = "НИЗЬКИЙ", "success", "Прийняття ризику (Accept)"

    return {
        'id': str(uuid.uuid4())[:8],
        'asset': asset,
        'risk_score': score,
        'category': cat,
        'color': col,
        'strategy': strat,
        'impact': impact,
        'likelihood': likelihood,
        'controls_count': len(selected_controls),
        'controls_list': [SECURITY_CONTROLS[c] for c in selected_controls]
    }

@app.route('/', methods=['GET', 'POST'])
def index():
    if 'history' not in session:
        session['history'] = []

    current_result = None
    if request.method == 'POST':
        current_result = calculate_cyber_risk(request.form)
        # Оновлюємо історію
        temp_history = session['history']
        temp_history.insert(0, current_result)
        session['history'] = temp_history[:10]
        session.modified = True

    return render_template('index.html',
                           controls=SECURITY_CONTROLS,
                           result=current_result,
                           history=session['history'])
```

```
if __name__ == '__main__':
    app.run(debug=True)


<!DOCTYPE html>
<html lang="uk">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>CyberRisk Pro | Аналітична платформа</title>
    <link rel="stylesheet" href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css">
    <link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/font-awesome/6.4.0/css/all.min.css">
    <script src="https://cdn.jsdelivr.net/npm/chart.js"></script>
    <style>
        :root { --bg: #0d1117; --card: #161b22; --border: #30363d; --text: #c9d1d9; --accent: #58a6ff; }
        body { background-color: var(--bg); color: var(--text); font-family: 'Segoe UI', system-ui, sans-serif; }

        /* Glassmorphism Cards */
        .glass-card {
            background: var(--card);
            border: 1px solid var(--border);
            border-radius: 12px;
            box-shadow: 0 8px 32px rgba(0,0,0,0.4);
        }

        /* Tabs Styling */
        .nav-tabs { border-bottom: 1px solid var(--border); }
        .nav-link { color: #8b949e; border: none !important; transition: 0.3s; padding: 1rem 1.5rem; }
        .nav-link:hover { color: white; }
        .nav-link.active {
            background: transparent !important;
            color: var(--accent) !important;
            border-bottom: 3px solid var(--accent) !important;
            font-weight: bold;
        }

        /* Form Elements */
        .form-control, .form-range {
            background: #0d1117 !important;
            border: 1px solid var(--border) !important;
            color: white !important;
        }
```

```
        .form-control:focus { border-color: var(--accent) !important; box-shadow: none; }

        /* Risk Badge for History */
        .risk-badge {
            width: 45px; height: 45px;
            display: flex; align-items: center; justify-content: center;
            border-radius: 10px; font-weight: 800;
        }

        /* Sidebar accent line */
        .sidebar-line { border-left: 3px solid var(--accent); padding-left: 15px; margin-bottom: 20px; }
        .btn-primary { background-color: var(--accent); border: none; font-weight: 600; padding: 10px; }
        .btn-primary:hover { background-color: #4493f8; transform: translateY(-1px); }
    </style>
</head>
<body>

<div class="container py-4">
    <!-- Header with Tabs -->
    <div class="d-flex justify-content-between align-items-center mb-4">
        <h2 class="fw-bold m-0"><i class="fas fa-shield-halved text-info me-2"></i>CyberRisk <span class="text-info">Pro</span></h2>
        <ul class="nav nav-tabs" id="mainTabs" role="tablist">
            <li class="nav-item">
                <button class="nav-link active" data-bs-toggle="tab" data-bs-target="#calc-tab"><i class="fas fa-bolt me-2"></i>Аналіз</button>
            </li>
            <li class="nav-item">
                <button class="nav-link" data-bs-toggle="tab" data-bs-target="#history-tab"><i class="fas fa-list me-2"></i>Історія</button>
            </li>
            <li class="nav-item">
                <button class="nav-link" data-bs-toggle="tab" data-bs-target="#guide-tab"><i class="fas fa-book me-2"></i>Методологія</button>
            </li>
        </ul>
    </div>

    <div class="tab-content">
        <!-- ТАБ 1: АНАЛІЗ -->
        <div class="tab-pane fade show active" id="calc-tab">
            <div class="row g-4">
                <!-- Form Column -->
```

```
        <div class="col-lg-5">
          <form method="POST" class="glass-card p-4">
            <div class="sidebar-line">
              <label class="form-label small text-uppercase fw-bold text-info">Об'єкт аналізу</label>
              <input type="text" name="asset_name" class="form-control" placeholder="Напр: Хмарне сховище" required>
            </div>

            <div class="sidebar-line">
              <label class="form-label small text-uppercase fw-bold text-info d-flex justify-content-between">
                Важливість активу <span id="impVal" class="badge bg-info text-dark">5</span>
              </label>
              <input type="range" name="importance" class="form-range" min="1" max="10" value="5" oninput="impVal.innerText=this.value">
            </div>

            <div class="sidebar-line">
              <label class="form-label small text-uppercase fw-bold text-info mb-3">Загрози та вразливості</label>
              <div class="form-check mb-2">
                <input class="form-check-input" type="checkbox" name="internet_access" id="ch1">
                <label class="form-check-label" for="ch1">Доступ з Інтернету</label>
              </div>
              <div class="form-check mb-3">
                <input class="form-check-input" type="checkbox" name="confidential_data" id="ch2">
                <label class="form-check-label" for="ch2">Конфіденційні дані</label>
              </div>
              <input type="number" name="users_count" class="form-control form-control-sm" placeholder="Кількість користувачів">
            </div>

            <div class="sidebar-line">
              <label class="form-label small text-uppercase fw-bold text-info mb-2">Захисні заходи</label>
              <div class="row g-1">
                {% for key, label in controls.items() %}
                <div class="col-6">
                  <div class="form-check small">
                    <input class="form-check-input" type="checkbox" name="controls" value="{{ key }}" id="{{ key }}">
                    <label class="form-check-label text-secondary" for="{{ key }}">{{ label.split(' ')[0] }}</label>
                  </div>
                </div>
                {% endfor %}
              </div>
```

```
            </div>
            <button type="submit" class="btn btn-primary w-100 shadow-sm mt-2 text-dark">РОЗРАХУВАТИ РИЗИК</button>
          </form>
        </div>

        <!-- Result Column -->
        <div class="col-lg-7">
          {% if result %}
          <div class="glass-card p-4 border-top border-4 border-{{ result.color }} h-100">
            <div class="d-flex justify-content-between">
              <div>
                <h3 class="mb-1 text-white">{{ result.asset }}</h3>
                <span class="badge bg-{{ result.color }} text-dark fw-bold text-uppercase">{{ result.category }} РИЗИК</span>
              </div>
              <div class="text-end text-{{ result.color }}">
                <div class="display-4 fw-bold">{{ result.risk_score }}</div>
                <div class="small text-uppercase opacity-50">Score</div>
              </div>
            </div>
            <hr class="border-secondary my-4">
            <div class="row align-items-center">
              <div class="col-md-6 text-center">
                <canvas id="radarChart"></canvas>
              </div>
              <div class="col-md-6">
                <h6 class="fw-bold text-info small text-uppercase">Стратегія:</h6>
                <p class="small border-start border-info ps-2 mb-4">{{ result.strategy }}</p>
                <h6 class="fw-bold text-info small text-uppercase">Рекомендації:</h6>
                <ul class="small ps-3 text-secondary">
                  {% if result.risk_score > 50 %}
                  <li class="mb-2">Впровадити відсутні заходи захисту негайно</li>
                  <li>Обмежити доступ до активу до мінімуму</li>
                  {% else %}
                  <li class="mb-2">Підтримувати поточний рівень контролів</li>
                  <li>Регулярний моніторинг логів доступу</li>
                  {% endif %}
                </ul>
              </div>
            </div>
          </div>
          <script>
```

```
                new Chart(document.getElementById('radarChart'), {
                    type: 'radar',
                    data: {
                        labels: ['Вплив', 'Ймовірність', 'Захист', 'Вразливість', 'Дані'],
                        datasets: [{
                            label: 'Профіль ризику',
                            data: [{{ result.impact }}, {{ result.likelihood }}, {{ result.controls_count * 1.3 }}, {{ result.risk_score/10 }}, 5],
                            backgroundColor: 'rgba(88, 166, 255, 0.2)',
                            borderColor: '#58a6ff',
                            pointBackgroundColor: '#58a6ff',
                            pointBorderColor: '#fff'
                        }]
                    },
                    options: {
                        scales: { r: { grid: {color: '#30363d'}, angleLines: {color: '#30363d'}, ticks: {display: false}, suggestedMax: 10 } },
                        plugins: { legend: {display: false} }
                    }
                });
            </script>
            {% else %}
            <div class="glass-card p-5 h-100 d-flex flex-column align-items-center justify-content-center opacity-25">
                <i class="fas fa-chart-line fa-5x mb-4"></i>
                <h5>Результати аналізу з'являться тут</h5>
                <p class="small text-center mt-2">Заповніть форму зліва для розрахунку.</p>
            </div>
            {% endif %}
        </div>
    </div>

    <!-- ТАБ 2: ІСТОРІЯ -->
    <div class="tab-pane fade" id="history-tab">
        <div class="glass-card p-4 shadow-lg">
            <div class="d-flex justify-content-between align-items-center mb-4 text-white">
                <h5 class="mb-0">Журнал останніх оцінок</h5>
                <span class="badge bg-secondary">Останні 10 записів</span>
            </div>
            {% if history %}
            <div class="table-responsive">
                <table class="table table-dark table-hover border-secondary align-middle">
                    <thead>
```

```
                    <tr class="text-secondary small">
                      <th>ID</th>
                      <th>АКТИВ</th>
                      <th>SCORE</th>
                      <th>КАТЕГОРИЗІЦІЯ</th>
                      <th>ПОКАЗНИКИ (I/L/C)</th>
                    </tr>
                  </thead>
                  <tbody>
                    {% for item in history %}
                    <tr>
                      <td class="text-secondary small">#{{ item.id }}</td>
                      <td class="fw-bold">{{ item.asset }}</td>
                      <td><div class="risk-badge bg-{{ item.color }} text-dark">{{ item.risk_score }}</div></td>
                      <td><span class="text-{{ item.color }} fw-bold">{{ item.category }}</span></td>
                      <td class="text-secondary small">{{ item.impact }} / {{ item.likelihood }} / {{ item.controls_count }}</td>
                    </tr>
                    {% endfor %}
                  </tbody>
                </table>
              </div>
              {% else %}
              <div class="text-center py-5 opacity-50">
                <i class="fas fa-folder-open fa-3x mb-3"></i>
                <p>Історія оцінок порожня</p>
              </div>
              {% endif %}
            </div>
          </div>

          <!-- ТАБ 3: МЕТОДОЛОГІЯ -->
          <div class="tab-pane fade" id="guide-tab">
            <div class="glass-card p-4">
              <h4 class="text-white mb-4">Опис математичної моделі</h4>
              <div class="row g-4 text-secondary">
                <div class="col-md-4">
                  <div class="p-4 rounded h-100" style="background: rgba(0,0,0,0.2);">
                    <h6 class="text-info fw-bold text-uppercase small mb-3">Вплив (Impact)</h6>
                    <p class="small">Суб'єктивна оцінка цінності активу. Чим важливіший актив для безперервності бізнес-процесів, тим вищий Impact.</p>
                  </div>
                </div>
```

```
            <div class="col-md-4">
              <div class="p-4 rounded h-100" style="background: rgba(0,0,0,0.2);">
                <h6 class="text-info fw-bold text-uppercase small mb-3">Ймовірність (Likelihood)</h6>
                <p class="small">Розраховується автоматично на основі поверхні атаки (Internet access), типу даних та кількості користувачів.</p>
              </div>
            </div>
            <div class="col-md-4">
              <div class="p-4 rounded h-100" style="background: rgba(0,0,0,0.2);">
                <h6 class="text-info fw-bold text-uppercase small mb-3">Захист (Mitigation)</h6>
                <p class="small">Кожен впроваджений технічний чи адміністративний захід захисту лінійно знижує фінальний бал ризику.</p>
              </div>
            </div>
          </div>
        </div>
      </div>
    </div>
</div>

<script src="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/js/bootstrap.bundle.min.js"></script>
</body>
</html
```