КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БУДІВНИЦТВА І АРХІТЕКТУРИ

Автоматизації і інформаційних технологій
(факультет)

Кібербезпеки та комп'ютерної інженерії
(назва випускової кафедри)

КВАЛІФІКАЦІЙНА РОБОТА
ЗДОБУВАЧА СТУПЕНЯ ВИЩОЇ ОСВІТИ БАКАЛАВР

на тему:
Оцінка цінності інформаційних активів в системі управління ризиками компанії малого та середнього бізнесу.

Лещенко Дмитро Сергійович
(прізвище, ім'я та по батькові здобувача повністю)

Київ 2026 р.

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БУДІВНИЦТВА І АРХІТЕКТУРИ

Автоматизації і інформаційних технологій

(факультет)

Кібербезпеки та комп'ютерної інженерії

(назва кафедри)

ЗАТВЕРДЖУЮ

Завідувач кафедри

Делембовський М.М.

„ ” _____2026 року

КВАЛІФІКАЦІЙНА РОБОТА ЗДОБУВАЧА СТУПЕНЯ ВИЩОЇ ОСВІТИ БАКАЛАВР

Оцінка цінності інформаційних активів в системі управління ризиками компанії малого та середнього бізнесу.

(назва)

Я як здобувач вищої освіти КНУБА розумію і підтримую політику закладу з академічної доброчесності.Я не надавав(-ла) і не одержував(-ла) недозволену допомогу під час підготовки цієї роботи. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.

Здобувач Лещенко Дмитро Сергійович

(прізвище, ім'я та по батькові повністю)

125 «Кібербезпека»

(спеціальність)

«Безпека інформаційних і комунікаційних систем»

(освітня програма)

Група: БІКС-22

Керівник: Ізмайлова О. В.

(прізвище та ініціали)

Кондидат технічних наук, доцент

(вчене звання, науковий ступінь)

Рецензент: Гончаренко Т.А

(прізвище та ініціали)

Ідентичність підтверджую

Київ 2026 р.

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БУДІВНИЦТВА І АРХІТЕКТУРИ

Факультет: автоматизації і інформаційних технологій
Випускова кафедра: Кібербезпеки та комп'ютерної інженерії
Ступінь вищої освіти: «Бакалавр»
Спеціальність: 125 «Кібербезпека»
Освітня програма: Безпека інформаційних і комунікаційних систем

ЗАТВЕРДЖУЮ

Завідувач кафедри
Делембовський М.М.
_____
„ ” _____2026 року

З А В Д А Н Н Я
ДО ВИКОНАННЯ КВАЛІФІКАЦІЙНОЇ РОБОТИ ЗДОБУВАЧА
СТУПЕНЯ ВИЩОЇ ОСВІТИ БАКАЛАВР

Лещенко Дмитро Сергійович
(прізвище, ім'я та по батькові здобувача)

1. Тема роботи Оцінка цінності інформаційних активів в системі управління ризиками компанії малого та середнього бізнесу.
   затверджена наказом ректора КНУБА № 576/52-15/13.2/26 від «14» травня 2026 року.
2. Керівник роботи
   Ізмайлова Ольга Василівна доцент кафедри кібербезпеки та комп'ютерної інженерії, кандидат технічних наук, доцент
   (прізвище, ім'я та по батькові, науковий ступінь, вчене звання)

3.Термін подання здобувачем роботи до захисту Червень 2026 р.

4. Зміст пояснювальної записки за розділами:

Р. 1. Аналіз задачі оцінки цінності інформаційних активів у системі управління ризиками компанії малого та середнього бізнесу.

Р. 2. Аналіз існуючої реалізації оцінювання цінності інформаційних активів та напрями її оптимізації.

Р. 3. Розробка гібридного методу та програмного модуля оцінювання цінності інформаційних активів і очікуваних втрат при реалізації загроз.

6. Консультанти розділів кваліфікаційної випускної роботи:

Розділ	Прізвище, ініціали та посада	Перевірив	
		дата	підпис
Розділ 1.			
Розділ 2.			
Розділ 3.			

7. Календарний план виконання роботи:

Види робіт та їх зміст	Дата виконання
Розділ 1	Квітень 2026 р.
Розділ 2	Квітень 2026 р.
Розділ 3	Травень 2026 р.
Остаточне оформлення роботи	Червень 2026 р.
Направлення роботи для перевірки на плагіат	Червень 2026 р.
Попередній захист роботи	Червень 2026 р.
Направлення роботи на рецензування	Червень 2026 р.

8. Дата видачі завдання 10.02.2026

Керівник Ізмайлова О.В. _____

Здобувач Лещенко.Д.С. _____

РЕЗЮМЕ (SUMMARY) до кваліфікаційної випускової роботи здобувача	ПІБ здобувача українською та англійською мовами Лещенко Дмитро Сергійович Leshchenko Dmytro Serhiiovych		
ЗВО	Київський національний університет будівництва і архітектури		
Тема (українською та англійською)	Оцінка цінності інформаційних активів в системі управління ризиками компанії малого та середнього бізнесу. Assessment of the Value of Information Assets in the Risk Management System of Small and Medium-Sized Business Companies.		
Освітній ступінь	Бакалавр		
Факультет	Факультет автоматизації та інформаційних технологій		
Випускова кафедра	Кафедра кібербезпеки та комп'ютерної інженерії		
Спеціальність	125 «Кібербезпека»		
Освітня програма	«Безпека інформаційних та комунікаційних систем»		
Керівник	Ізмайлова Ольга Василівна		
Обсяг роботи:	Поснювальна записка, стор.	Розділів	Презентація, кількість слайдів
	115	3	18
Розділ 1	Аналіз задачі оцінки цінності інформаційних активів у системі управління ризиками компанії малого та середнього бізнесу.		
Розділ 2	Аналіз існуючої реалізації оцінювання цінності інформаційних активів та напрями її оптимізації.		
Розділ 3	Розробка гібридного методу та програмного модуля оцінювання цінності інформаційних активів і очікуваних втрат при реалізації загроз.		
Розділ 4	Не передбачено структурою роботи.		
Розділ 5	Не передбачено структурою роботи.		

Висновки по роботі	У роботі обґрунтовано актуальність оцінювання цінності інформаційних активів для компаній малого та середнього бізнесу, проаналізовано існуючі підходи до управління ризиками, запропоновано гібридний метод оцінювання активів, очікуваних втрат і контрзаходів та реалізовано програмний модуль підтримки прийняття управлінських рішень.
Ключові слова: Keywords:	інформаційний актив; цінність активу; ризик; інформаційна безпека; очікувані втрати; SLE; ALE; контрзаходи; малий та середній бізнес; управління ризиками. information asset; asset value; risk; information security; expected losses; SLE; ALE; countermeasures; small and medium-sized business; risk management.

Здобувач _____/ _____

Керівник _____/ _____

АНОТАЦІЯ

Кваліфікаційна випускна робота присвячена дослідженню підходів до оцінювання цінності інформаційних активів у системі управління ризиками компанії малого та середнього бізнесу. У роботі розглянуто роль інформаційних активів у діяльності підприємства, проаналізовано основні загрози, ризики та можливі очікувані втрати при порушенні конфіденційності, цілісності або доступності даних.

Запропоновано гібридний підхід до оцінювання, який поєднує бальну оцінку активів, грошову оцінку, сценарний аналіз загроз, розрахунок очікуваних втрат і визначення ефективності контрзаходів. Практичним результатом роботи є програмний модуль, що дозволяє вести реєстр активів, оцінювати ризикові сценарії, порівнювати контрзаходи та формувати аналітичні результати для підтримки управлінських рішень.

Ключові слова: інформаційний актив, цінність активу, ризик, інформаційна безпека, очікувані втрати, SLE, ALE, контрзаходи, малий та середній бізнес, управління ризиками.

ABSTRACT

The qualification thesis is devoted to the study of approaches to assessing the value of information assets within the risk management system of small and medium-sized businesses. The work analyzes the role of information assets in enterprise operations, main threats, risks, and possible expected losses caused by violations of confidentiality, integrity, or availability of data.

A hybrid assessment approach is proposed, combining asset scoring, monetary valuation, threat scenario analysis, expected loss calculation, and evaluation of countermeasure effectiveness. The practical result of the work is a software module that supports asset registration, risk scenario assessment, countermeasure comparison, and analytical reporting for management decision-making.

Keywords: information asset, asset value, risk, information security, expected losses, SLE, ALE, countermeasures, small and medium-sized business, risk management.

Зміст

ВСТУП

У сучасних умовах стабільність роботи підприємства значною мірою залежить від захищеності його інформаційних активів: баз даних, технологічної документації, облікових записів, мережевих конфігурацій, журналів подій, резервних копій і програмних комплексів. Порушення конфіденційності, цілісності або доступності таких активів може спричинити простій виробництва, втрату або спотворення даних, додаткові витрати на відновлення, штрафні санкції.

Актуальність теми кваліфікаційної роботи зумовлена потребою у прозорому й економічно обґрунтованому оцінюванні цінності інформаційних активів та очікуваних втрат при реалізації загроз. На практиці рішення щодо захисту часто приймаються фрагментарно: без повного паспорта активу, урахування його ролі в бізнес-процесах, розрахунку ризику та порівняння ефективності контрзаходів. Для виробничого підприємства ця проблема є особливо важливою, оскільки інформаційні системи безпосередньо пов’язані з плануванням продукції, технологічними параметрами, обліком, логістикою та контролем якості.

Метою роботи є розроблення та апробація підходу до оцінювання цінності інформаційних активів і очікуваних втрат при реалізації загроз для підвищення обґрунтованості рішень щодо захисту інформаційної інфраструктури підприємства.

Об’єктом дослідження є процес оцінювання цінності інформаційних активів та очікуваних втрат від реалізації загроз.

Предметом дослідження є методи, моделі, критерії та засоби якісного й кількісного оцінювання критичності активів, імовірності загроз, величини очікуваних втрат і ефективності контрзаходів.

Для досягнення мети передбачено: проаналізувати роль інформаційних активів у діяльності підприємства, підходи оцінювання активів, ризиків і очікуваних втрат; визначити недоліки спрощеного оцінювання; розробити паспорт активу, багатокритеріальну модель, перехід від грошової оцінки до бальної шкали, алгоритм розрахунку очікуваних втрат; реалізувати програмний модуль і виконати його апробацію.

РОЗДІЛ 1

АНАЛІЗ ЗАДАЧІ ОЦІНКИ ЦІННОСТІ ІНФОРМАЦІЙНИХ АКТИВІВ В СИСТЕМІ УПРАВЛІННЯ РИЗИКАМИ КОМПАНІЇ МАЛОГО ТА СЕРЕДНЬОГО БІЗНЕСУ.

Актуальність дослідження та постановка проблеми

У сучасних організаціях інформаційні активи виступають не допоміжним, а базовим ресурсом забезпечення безперервності бізнесу, стабільності виробничих процесів, фінансової стійкості та виконання договірних зобов’язань. Для компаній малого та середнього бізнесу виробничого профілю ця теза має особливе значення, оскільки інформаційні потоки безпосередньо пов’язані з технологічною документацією, плануванням випуску продукції, бухгалтерським і складським обліком, логістикою, кадровими процесами та підтримкою обладнання. Втрата конфіденційності, цілісності або доступності таких ресурсів призводить не лише до інформаційного інциденту, а й до простою виробництва, зриву постачань, штрафних санкцій, зростання експлуатаційних витрат і репутаційних втрат.

Практика експлуатації корпоративних інформаційних систем показує, що підприємства часто інвестують у засоби захисту без достатньо чіткого економічного обґрунтування. У результаті частина ресурсів спрямовується на захист активів із низькою критичністю, тоді як найбільш важливі дані та сервіси залишаються недостатньо прикритими. Причина такої ситуації полягає у відсутності узгодженої методики, яка одночасно дає змогу оцінити реальну цінність активу для підприємства, врахувати специфіку загроз і визначити очікувані втрати від реалізації небажаних подій у зрозумілій для керівництва формі.

З методичної точки зору тема дослідження належить до перетину управління інформаційною безпекою, аналізу ризиків і підтримки управлінських рішень. Саме тому завдання оцінювання цінності інформаційних активів не може зводитися лише до бухгалтерського підходу або лише до технічної експертної оцінки. На

практиці доводиться поєднувати якісні характеристики активів, їхню роль у бізнес-процесах, масштаби потенційної шкоди, імовірність реалізації загроз і тривалість відновлення нормальної роботи. Такий комбінований підхід є особливо важливим для об’єктів, де одна подія інформаційної безпеки здатна запустити ланцюг виробничих і організаційних наслідків.

За матеріалами переддипломної практики предметна область дипломної роботи пов’язана з IT-інфраструктурою виробничого підприємства ливарного профілю. У звіті з практики наведено, що підприємство використовує файловий сервер, сервер домену Active Directory, сервер резервного копіювання, сервер бухгалтерської системи, сервер виробничої бази даних, а також мережеву інфраструктуру з міжмережевим екраном, Wi-Fi і VPN-доступом. До ключових активів віднесено базу даних замовлень, фінансову базу даних, технологічну документацію, облікові записи доменної структури, конфігурації мережевого обладнання та журнали подій систем безпеки. Під час практики було виявлено 17 ключових інформаційних активів, із яких 6 мають високий рівень критичності, а також використано розрахунки SLE і ALE для оцінювання очікуваних втрат [2].

Отже, актуальність теми визначається трьома взаємопов’язаними чинниками: зростанням залежності підприємств від інформаційних систем, фрагментарністю прийняття рішень щодо захисту активів і потребою в економічному обґрунтуванні контрзаходів. Узагальнення цих чинників наведено на рис. 1.1.

Рис.1.1 – Чинники актуальності теми

Таким чином, постановка проблеми полягає в необхідності розроблення підходу, який дозволяє не лише описати інформаційні активи підприємства, а й оцінити їхню цінність, пов’язати її зі сценаріями загроз, визначити очікувані втрати та обґрунтувати вибір контрзаходів. Саме ця логіка покладена в основу подальших розділів роботи: спочатку аналізується предметна область і наявні підходи, далі розглядаються недоліки існуючої реалізації, після чого пропонується гібридний метод і програмний модуль підтримки оцінювання.

Місце інформаційних активів у діяльності сучасного підприємства

Інформаційний актив у роботі розглядається як ресурс, що має цінність для організації, використовується у процесах створення продукту або послуги й потребує цілеспрямованого захисту. На відміну від традиційного уявлення, за яким активом вважаються лише дані або документи, сучасний підхід включає також програмне забезпечення, системні конфігурації, облікові записи, журнали подій, резервні копії, сервіси віддаленого доступу, інформацію про контрагентів, технологічні параметри виробництва та навіть організаційні знання, закріплені в

цифрових середовищах. Така широка інтерпретація необхідна, оскільки порушення будь-якого з перелічених елементів здатне спричинити збій у роботі всієї інформаційної системи.

У промисловому середовищі інформаційні активи мають подвійну природу. З одного боку, вони виконують класичні офісні функції: підтримують бухгалтерію, документообіг, роботу з персоналом і взаємодію із замовниками. З іншого боку, вони інтегровані з технологічними процесами, тобто безпосередньо впливають на ритмічність виробництва, коректність виробничих завдань, дотримання норм витрати матеріалів, контроль якості та логістику. Саме тому цінність активу в таких умовах не може визначатися лише його ринковою ціною або вартістю програмного продукту. Вона формується як сукупний ефект від його ролі в бізнес-процесах, ступеня залежності підприємства від безперервної роботи активу та масштабів наслідків у разі його компрометації.

У межах аналізу предметної області активи класифікуються за функціональним призначенням, рівнем критичності та типом наслідків у разі порушення їхніх властивостей. Практичний матеріал підприємства, отриманий під час переддипломної практики, підтверджує правильність такого поділу, оскільки в межах однієї організації одночасно співіснують активи з різним горизонтом впливу: від локальних службових файлів до центральної виробничої бази даних, від конфігурації комутатора до доменної інфраструктури, яка визначає доступ співробітників до ресурсів [2].

Особливої уваги заслуговують активи, що поєднують високу інформаційну цінність і високу операційну значущість. Наприклад, технологічна документація є критичною не тільки через конфіденційність, а й через вимогу збереження цілісності: навіть незначне спотворення параметрів плавки, креслень або маршрутних карт може призвести до браку, збільшення витрати матеріалів чи порушення техніки безпеки. Аналогічно облікові записи доменної структури мають високу цінність не як самостійний набір записів, а як інструмент контролю доступу до всієї корпоративної інфраструктури. З огляду на це, оцінювання інформаційних активів має спиратися на системне бачення організації. Кожен актив повинен

аналізуватися не ізольовано, а у зв’язку з бізнес-процесами, користувачами, технічними залежностями, каналами передачі даних та сценаріями інцидентів. Такий підхід створює передумови для формування реєстру активів як основи подальшого ризик-аналізу й дає змогу перейти від переліку ресурсів до усвідомленої моделі управління безпекою (табл. 1.1).

Таблиця 1.1 – Узагальнена класифікація інформаційних активів виробничого підприємства

Група активів	Приклади	Основне значення для підприємства	Типові наслідки порушення
Дані	Бази замовлень, фінансова БД, технологічні карти	Підтримка обліку, планування й виробництва	Втрата даних, спотворення розрахунків, зупинка процесів
Системні сервіси	AD, файлові служби, резервне копіювання, VPN	Доступ користувачів і безперервність роботи IT-середовища	Втрата доступу, збої автентифікації, простої
Конфігурації та журнали	Налаштування мережі, логи безпеки, політики доступу	Керованість і контроль подій безпеки	Ускладнення розслідування, помилкові налаштування, приховані інциденти
Програмні комплекси	ERP, бухгалтерська система, документообіг, моніторинг	Автоматизація бізнес- і виробничих процесів	Порушення роботи підрозділів, затримка рішень
Облікові дані	Доменно-користувацькі записи, адміністраторські облікові дані	Розмежування прав і контроль доступу	Ескалація привілеїв, несанкціонований доступ

Понятійний апарат дослідження: цінність активу, загроза, вразливість, ризик і очікувані втрати

Для коректної постановки задачі необхідно чітко розмежувати ключові поняття, що використовуються в роботі. Передусім слід відрізняти цінність активу від його вартості у вузькому фінансовому сенсі. У контексті інформаційної безпеки цінність активу відображає не лише його прямий грошовий еквівалент, а й сукупний вплив на виконання функцій підприємства. Тому один і той самий актив може мати порівняно невелику балансову вартість, але дуже високу операційну критичність. Наприклад, конфігураційний файл маршрутизатора або резервний доменний контролер зазвичай не мають великої ринкової ціни, проте їхній вихід із ладу може призвести до непропорційно великих наслідків.

У теорії інформаційної безпеки загроза розглядається як потенційна подія або дія, здатна спричинити шкоду активу через використання наявної вразливості. Вразливість, своєю чергою, є слабким місцем в архітектурі, конфігурації, організації процесів або поведінці персоналу, що створює умови для реалізації загрози. Важливо підкреслити, що сама по собі вразливість ще не означає настання збитків. Негативні наслідки виникають тоді, коли існує реальне джерело загрози та достатні умови для експлуатації слабкості.

Ризик у цій дипломній роботі трактується як поєднання ймовірності реалізації певного сценарію загрози та величини втрат, яких може зазнати підприємство. Таке трактування дає змогу перейти від абстрактного опису небезпеки до числової або принаймні впорядкованої пріоритезації. Коли ймовірність висока, а потенційні втрати значні, розглядається ризик як пріоритетний. Якщо ж один із компонентів є незначним, потреба у дорогих заходах захисту може бути переглянута.

Категорія очікуваних втрат є ключовою для управлінського рівня. Вона дає змогу перевести проблему безпеки у фінансово зрозумілий вимір. До очікуваних

втрат можуть входити прямі збитки від відновлення даних і систем, втрати від простою виробництва, порушення зобов’язань перед клієнтами, витрати на реагування та розслідування інциденту, а також непрямі наслідки: падіння довіри партнерів, погіршення репутації, штрафи та збільшення операційного навантаження на персонал.

З позиції оцінювання активів найбільш поширеним є підхід, за якого цінність визначається через вплив порушення конфіденційності, цілісності та доступності. Такий підхід добре узгоджується з класичною моделлю CIA та забезпечує зручну основу для побудови реєстру активів. Водночас для практичного використання в управлінні ризиками цієї трійки недостатньо. Необхідно також враховувати роль активу в ключових процесах, швидкість відновлення, залежність від нього інших сервісів і можливість заміни або дублювання. Саме тому в роботі доцільно розглядати цінність активу як інтегральну характеристику, а не як один показник, відірваний від реального середовища.

Для початкової інтегральної оцінки критичності активу може застосовуватися така узагальнена залежність:

Для недопущення заниження критичності використовується правило максимального впливу: якщо хоча б одна з властивостей C, I або A має критичне значення, підсумкова первинна оцінка не може бути нижчою за це значення.

$$KCIA = \max(C, I, A) \qquad (1.1)$$

де K_CIA – первинна критичність активу за правилом максимального впливу;

C, I, A – оцінки впливу порушення конфіденційності, цілісності та доступності відповідно;

У подальшій методиці це правило поєднується зі зваженою багатокритеріальною моделлю, що враховує ваги критеріїв і якість доказової бази.

Для виробничих підприємств вагові коефіцієнти зазвичай не є однаковими. Якщо актив прямо впливає на керування технологічним процесом, підвищеної ваги набувають цілісність і доступність. Якщо ж актив містить комерційно чутливі дані, креслення, фінансові розрахунки або персональні дані, суттєво зростає роль

конфіденційності. Саме настройка ваг робить модель придатною до адаптації в різних організаціях.

Аналіз існуючих підходів до оцінювання цінності інформаційних активів

У науковій і прикладній літературі можна виділити кілька великих груп підходів до оцінювання цінності інформаційних активів. Перша група - якісні методи. Вони спираються на експертне судження, інтерв'ювання відповідальних осіб, шкали типу «низький – середній – високий» або бальні оцінки. Перевага цього підходу полягає у швидкому запуску, невисоких вимогах до вихідних даних і можливості застосування в умовах обмеженої статистики. Недоліком є суб'єктивність, залежність від складу експертів і складність подальшого економічного обґрунтування рішень.

Друга група - кількісні підходи, орієнтовані на визначення активу у грошовому або умовно-грошовому вимірі. Тут можуть використовуватися оцінка вартості простою, вартості відновлення, вартості володіння, розміру можливих штрафів, упущеної вигоди та інших економічних показників. Кількісний підхід є більш переконливим для менеджменту, однак вимагає значно кращої якості вхідних даних, зокрема інформації про інциденти, тривалість простою, залежності між процесами та історичні показники збоїв.

Третя група - комбіновані або гібридні методики. Вони поєднують експертні шкали для первинної класифікації з подальшим переведенням результатів у фінансові показники для найбільш критичних активів. Саме гібридний підхід у більшості випадків виявляється найбільш життєздатним для реальних підприємств, оскільки дозволяє не перевантажувати оцінювання там, де це економічно недоцільно, і водночас забезпечує достатню точність для пріоритетних об'єктів захисту.

Окреме місце посідають стандартизовані підходи, пов'язані з міжнародними системами управління інформаційною безпекою. Так, ISO/IEC 27001:2022 визначає

вимоги до системи менеджменту інформаційної безпеки та орієнтує організації на ризик-орієнтоване планування заходів захисту. ISO/IEC 27005:2022 надає докладні рекомендації щодо управління ризиками інформаційної безпеки і фактично задає рамку для ідентифікації активів, джерел загроз, вразливостей, наслідків та варіантів оброблення ризику. NIST SP 800-30 Rev.1 концентрується на проведенні ризик-оцінювання та підкреслює необхідність врахування загроз, вразливостей, імовірності та впливу. NIST Cybersecurity Framework 2.0 доповнює цю логіку набором функцій Govern, Identify, Protect, Detect, Respond і Recover, що дозволяє інтегрувати аналіз активів у ширшу систему управління кіберризиком [3–6].

Критичний аналіз показує, що жоден із зазначених підходів не є універсальним у чистому вигляді. Якісні методи занадто грубі для фінансового порівняння альтернатив; кількісні методи часто страждають від дефіциту даних; стандарти задають рамку, але не гарантують конкретної адаптації до предметної області. Саме тому при розробленні запропонованої методики доцільно поєднати стандартний процес ідентифікації та оцінювання з набором показників, доступних у конкретній організації, а також із обліком властивостей активів виробничого підприємства.

Узагальнені результати для цього етапу наведено в табл. 1.2.

Таблиця 1.2 – Порівняння підходів до оцінювання цінності інформаційних активів

Підхід	Сутність	Переваги	Обмеження	Доцільність використання
Якісний	Експертні шкали, ранжування, CIA-оцінювання	Швидкість, простота, малі вимоги до даних	Суб’єктивність, важко перевести у гроші	Початковий аудит і класифікація
Кількісний	Грошова оцінка втрат, вартості відновлення, простою	Добре сприймається менеджментом,	Потребує статистики й достовірних вихідних даних	Критичні активи та інвестиційні рішення

Підхід	Сутність	Переваги	Обмеження	Доцільність використання
		дає основу для ROI		
Стандартно-орієнтований	Оцінювання в рамках ISO/NIST-процесів	Системність, сумісність з ISMS, повторюваність	Потребує адаптації до конкретного підприємства	Формалізація процесу управління ризиками
FAIR/квазикількісний	Аналіз частоти та масштабу ймовірних втрат	Фінансова мова ризику, зв'язок із рішеннями бізнесу	Високі вимоги до моделювання й даних	Поглиблений аналіз окремих сценаріїв
Гібридний	Поєднання експертної та кількісної оцінки	Баланс практичності та точності	Потрібно налаштовувати критерії й ваги	Найбільш придатний для дипломної методики

Матеріали переддипломної практики підтверджують ефективність гібридного підходу. На підприємстві спочатку виконувалося експертне оцінювання критичності активів за критеріями конфіденційності, цілісності та доступності, а для окремих ключових активів застосовувався розрахунок вартості простою та очікуваних річних втрат. Така послідовність є логічною, оскільки дозволяє сконцентрувати кількісний аналіз на тих ресурсах, які мають найбільший вплив на діяльність організації [2].

1.5 Аналіз підходів до оцінювання очікуваних втрат і ризику

Після визначення цінності активів логічним кроком є оцінювання можливих втрат у разі реалізації загроз. Саме на цьому етапі проблема інформаційної безпеки перетворюється на задачу управління ризиком. У найпростішому вигляді ризик розглядається як добуток імовірності події та величини її наслідків. Проте для практичних розрахунків такий вираз потребує деталізації: необхідно визначити, що

саме вважається подією, як оцінюється її частота, які компоненти включаються до втрат і яким є часовий горизонт аналізу.

Одним з найпоширеніших прикладних підходів є використання показників SLE (Single Loss Expectancy) та ALE (Annual Loss Expectancy). Показник SLE відображає очікувану величину разових збитків від реалізації конкретного сценарію, а ALE - очікувані річні втрати з урахуванням частоти повторення такого сценарію протягом року. Перевага цієї моделі полягає у простоті інтерпретації та можливості напряму оцінити економічний ефект від зниження ймовірності інциденту або зменшення його впливу.

Водночас при застосуванні SLE та ALE слід уникати механічного підходу. Насамперед потрібно коректно визначити цінність активу та коефіцієнт впливу сценарію. Не кожна подія призводить до повної втрати активу; часто мова йде про часткову деградацію, тимчасову недоступність, втрату цілісності окремої функції або компрометацію даних із наступним відновленням. Крім того, частота події може бути оцінена за історичними журналами, галузевою статистикою, аналітикою CERT-UA або експертним шляхом - і в кожному випадку рівень невизначеності буде різним.

Альтернативою класичним формулам є сценарний аналіз. У його межах розглядаються конкретні ланцюги подій: наприклад, компрометація облікового запису адміністратора, поширення шкідливого коду на файлові ресурси, шифрування виробничої бази даних, зупинка планування випуску продукції, простій цеху й подальше відновлення з резервної копії. Перевага такого підходу полягає в тому, що він дає змогу врахувати міжсистемні залежності та опосередковані наслідки, які не завжди видно з окремого розрахунку по активу.

Для більш зрілого рівня аналізу використовуються моделі, орієнтовані на кількісне вимірювання частоти та масштабу ймовірних втрат, наприклад Open FAIR. Їх сильна сторона - орієнтація на фінансовий вимір ризику та зв’язок із управлінськими рішеннями. Водночас такі моделі потребують якісної статистичної бази й достатньої аналітичної зрілості підприємства, що не завжди досяжно в межах бакалаврської роботи. Тому для предметної області даного дослідження

більш виправданим є поєднання класичних показників SLE/ALE зі сценарним уточненням найбільш критичних загроз.

У розрахунковій частині для окремих сценаріїв використовуються такі співвідношення:

$$SLE = AV \cdot EF; \quad ALE = SLE \cdot ARO. \qquad (1.2)$$

де AV – вартість (цінність) активу;

EF – коефіцієнт впливу загрози на актив;

ARO – очікувана частота реалізації події протягом року.

За звітом з переддипломної практики для сервера виробничої бази даних було прийнято вартість простою 45 000 грн за годину та середній час відновлення 6 годин, що дало SLE = 270 000 грн. Для сценарію ransomware з річною частотою 0,3 отримано ALE = 81 000 грн. Після запропонованого впровадження багатофакторної автентифікації значення ARO зменшувалося до 0,1, а очікувані річні втрати - до 27 000 грн, що показало потенційний економічний ефект 54 000 грн на рік [2]. Наведений приклад демонструє, як кількісне оцінювання дозволяє перейти від декларацій про небезпеку до обґрунтованих управлінських рішень.

Узагальнені результати для цього етапу наведено в табл. 1.3.

Таблиця 1.3 – Порівняння підходів до оцінювання очікуваних втрат

Метод	Інформаційна база	Що отримуємо	Переваги	Обмеження
Матриця ризиків	Експертні оцінки ймовірності та впливу	Пріоритети загроз	Наочність і простота	Низька точність у грошовому вимірі
SLE/ALE	Вартість активу, частота події, коефіцієнт впливу	Очікувані разові та річні втрати	Прямий зв’язок із фінансами	Чутливість до якості даних
Сценарний аналіз	Опис ланцюга інциденту, залежності між сервісами	Деталізовані наслідки конкретного сценарію	Враховує каскадні ефекти	Більш трудомісткий

Метод	Інформаційна база	Що отримуємо	Переваги	Обмеження
FAIR-підхід	Дані про частоту подій і масштаб втрат	Ризик як імовірна частота та величина майбутніх втрат	Добре підходить для бізнес-комунікації	Потребує розвиненої культури збору даних

1.6 Специфіка загроз для інформаційних активів виробничого підприємства

Перелік загроз для інформаційних активів формується як на основі загальновідомих кіберризиків, так і з урахуванням предметної області конкретного підприємства. Для виробничого середовища характерною є комбінація класичних офісних ризиків та ризиків, пов’язаних із безперервністю технологічних процесів. Це означає, що навіть інциденти, які на перший погляд мають локальний IT-характер, можуть швидко масштабуватися у виробничу, логістичну або фінансову проблему.

За матеріалами переддипломної практики до найбільш значущих загроз були віднесені ransomware, відмова серверного обладнання, несанкціонований доступ, помилки персоналу та DDoS-атаки на VPN-шлюз [2]. Такий перелік видається обґрунтованим, оскільки кожна із зазначених загроз відображає різні механізми негативного впливу. Програми-шифрувальники порушують доступність і часто цілісність даних; апаратні збої або відмова накопичувачів ведуть до недоступності сервісів; несанкціонований доступ створює ризики для всіх трьох властивостей інформації; помилки персоналу можуть призводити як до випадкового видалення даних, так і до хибних конфігурацій; атаки на канали віддаленого доступу блокують критично важливі адміністративні та виробничі дії.

Особливістю виробничого підприємства є висока роль часу відновлення. Якщо у багатьох офісних середовищах інцидент призводить переважно до затримки окремих процедур, то у виробництві навіть кілька годин недоступності

бази даних замовлень, ERP-системи або мережевого сегмента можуть зупинити погодження маршрутних карт, випуск супровідної документації, контроль залишків сировини та формування змінних завдань. Саме тому в оцінюванні загроз важливо враховувати не лише факт збитку, а й часову динаміку його накопичення.

Не менш важливим є людський фактор. Практика інформаційної безпеки доводить, що вразливості часто виникають не лише через технічні помилки, а й через недостатнє навчання персоналу, повторне використання паролів, нехтування правилами резервного копіювання, несвоєчасне встановлення оновлень або надмірно широкі права доступу. Для виробничих підприємств проблема ускладнюється тим, що персонал має різний рівень цифрової грамотності, а пріоритет оперативного виконання виробничих завдань інколи витісняє дотримання кібергігієни.

Отже, модель загроз у межах цієї дипломної роботи повинна бути багаторівневою. Вона має враховувати технічні загрози, пов’язані з мережевою інфраструктурою й серверами; програмні загрози, пов’язані зі шкідливим кодом та експлуатацією вразливостей; організаційні загрози, пов’язані з доступом і процесами; а також зовнішні деструктивні впливи на віддалений доступ і канали обміну даними. Лише за такого підходу оцінка втрат буде наближеною до реальних умов експлуатації активів.

Узагальнені результати для цього етапу наведено в табл. 1.4.

Таблиця 1.4 – Узагальнення основних загроз та їх впливу на активи підприємства

Загроза	Найбільш уразливі активи	Основний тип наслідків	Коментар щодо оцінювання
Ransomware	Файлові ресурси, БД замовлень, виробнича БД, резервні каталоги	Втрата доступності, часткова втрата цілісності, простій	Доцільно рахувати SLE/ALE і час відновлення

Загроза	Найбільш уразливі активи	Основний тип наслідків	Коментар щодо оцінювання
Відмова обладнання	Сервери, мережеве обладнання, системи зберігання	Переривання сервісів, втрата операційного часу	Важливі MTTR, наявність резервування й бекапів
Несанкціонований доступ	Доменно-облікові записи, ERP, документообіг, журнали	Компрометація конфіденційності й цілісності	Необхідно враховувати права доступу і сценарії ескалації
Помилка персоналу	Конфігурації, довідники, резервні копії, службові дані	Неправильні налаштування, випадкове видалення	Добре оцінюється сценарно та через процедури контролю
DDoS / відмова VPN	VPN-шлюз, канали віддаленого адміністрування	Недоступність віддалених сервісів і затримка реагування	Доцільно враховувати критичність віддаленого доступу для підтримки

1.7 Аналіз недоліків існуючих рішень та обґрунтування напряму дослідження

Проведений огляд дозволяє зробити висновок, що проблема оцінювання цінності інформаційних активів і очікуваних втрат має не лише технічний, а й методичний характер. У більшості організацій інформація про активи накопичується в різних реєстрах або навіть зберігається неформально: частина відомостей належить IT-відділу, частина - бухгалтерії, частина - виробничим підрозділам. Через це одна й та сама система оцінюється різними працівниками по-різному, а результати не складаються в єдину картину для прийняття рішень.

Слабким місцем типових якісних підходів є те, що вони добре відповідають на питання «що є важливим», але гірше відповідають на питання «наскільки виправданими є витрати на захист». З іншого боку, типові кількісні підходи часто

вимагають такого обсягу статистики, якого на реальному підприємстві немає. Звідси виникає потреба у методиці, яка не перевантажує організацію зайвими даними, але водночас дає можливість обґрунтовано оцінити найбільш критичні сценарії.

Важливо також враховувати, що окремі стандарти описують процеси на високому рівні узагальнення. Вони визначають логіку ідентифікації, аналізу, оцінювання й оброблення ризиків, але не встановлюють конкретних формул або шкал для кожної предметної області. Це не є недоліком стандартів як таким; навпаки, така гнучкість дозволяє адаптувати їх до організації. Однак у межах дипломної роботи це означає потребу у побудові прикладної моделі, яка наповнює стандартну рамку конкретними показниками, критеріями та правилами інтерпретації.

Проведений під час практики аналіз підприємства показав, що найбільшу практичну цінність має саме поєднання якісного та кількісного оцінювання. Спочатку формується реєстр активів і виконується їх ранжування за критеріями конфіденційності, цілісності та доступності, а потім для активів із високою критичністю визначаються типові сценарії загроз, розраховуються разові та річні очікувані втрати, а також обґрунтовуються заходи зниження ризику. Така схема забезпечує і системність, і прийнятну трудомісткість, і зрозумілість результатів для керівництва.

Отже, у подальшому дослідженні розробляється адаптована методика, що поєднує: а) інвентаризацію та класифікацію активів; б) інтегральну оцінку їх критичності; в) побудову сценаріїв основних загроз; г) кількісне визначення очікуваних втрат для пріоритетних сценаріїв; ґ) формування рекомендацій щодо зниження ризиків та оцінку їхнього економічного ефекту. Такий підхід є найбільш доречним для дипломної роботи прикладного спрямування за спеціальністю «Кібербезпека та захист інформації».

1.8 Об’єкт, предмет, мета та завдання дослідження

З урахуванням теми дипломної роботи, вимог методичних рекомендацій кафедри та результатів аналізу предметної області **об’єктом дослідження** визначено процес оцінювання цінності інформаційних активів та очікуваних втрат від реалізації загроз в інформаційній інфраструктурі підприємства. Таке формулювання відображає саме процес і явище, що породжують проблемну ситуацію, та відповідає академічним вимогам до визначення об’єкта дослідження [1].

Предметом дослідження виступають методи, моделі, критерії та засоби оцінювання критичності інформаційних активів, імовірності реалізації загроз та величини очікуваних втрат, адаптовані до умов виробничого підприємства. Предмет концентрує увагу не на всій інфраструктурі як такій, а на тих властивостях і механізмах, які дозволяють побудувати практичну методику оцінювання.

Метою дипломної роботи є підвищення обґрунтованості прийняття рішень у сфері захисту інформаційних активів шляхом розроблення та апробації підходу до комплексного оцінювання їхньої цінності й очікуваних втрат при реалізації загроз. У цьому формулюванні важливо, що робота спрямована не на абстрактне дослідження ризиків, а на створення інструменту підтримки управлінського рішення.

Для досягнення поставленої мети необхідно вирішити такі основні завдання: проаналізувати предметну область і структуру інформаційних активів підприємства; узагальнити підходи до оцінювання критичності активів; дослідити методи визначення очікуваних втрат і ризику; сформувати перелік типових загроз для обраного середовища; розробити інтегровану модель оцінювання; виконати апробацію моделі на матеріалах практики; визначити рекомендації щодо зменшення ризику та оцінити економічний ефект від запропонованих заходів.

Практична цінність такого підходу полягає в тому, що результати оцінювання можуть бути використані для пріоритезації активів, обґрунтування витрат на захист, вибору порядку впровадження організаційних і технічних заходів,

а також підготовки матеріалів для керівництва підприємства. Іншими словами, дослідження спрямоване на перехід від фрагментарного реагування на інциденти до планового управління ризиками.

Узагальнені результати для цього етапу наведено в табл. 1.5.

Таблиця 1.5 – Формалізація елементів постановки дослідження

Елемент	Зміст
Об’єкт дослідження	Процес оцінювання цінності інформаційних активів та очікуваних втрат від реалізації загроз у корпоративній інформаційній інфраструктурі підприємства
Предмет дослідження	Методи, моделі, критерії та засоби якісного й кількісного оцінювання критичності активів і можливих втрат
Мета	Розроблення підходу до комплексної оцінки цінності активів і очікуваних втрат для підтримки рішень щодо захисту
Ключовий результат	Методика або модель, придатна до використання в умовах виробничого підприємства

1.9 Постановка задачі дослідження та вимоги до майбутньої методики

З урахуванням проведеного аналізу в цій дипломній роботі поставлено таку задачу: розробити методику оцінювання цінності інформаційних активів та очікуваних втрат від реалізації загроз, яка забезпечує можливість ранжування активів за критичністю, визначення пріоритетних сценаріїв ризику та обґрунтування доцільності впровадження захисних заходів у середовищі виробничого підприємства. У постановці задачі акцент зроблено на прикладному результаті: методика має бути придатною до практичного використання, а не лише до теоретичного опису.

Перша група вимог до майбутньої методики - змістові вимоги. Методика повинна враховувати всі основні види інформаційних активів підприємства,

охоплювати критерії конфіденційності, цілісності та доступності, враховувати роль активів у бізнес-процесах і допускати аналіз не лише окремих ресурсів, а й їх взаємозалежностей. Для виробничого середовища це особливо важливо, оскільки наслідки інцидентів часто мають каскадний характер.

Друга група - вимоги до даних і процедур. Методика має використовувати реалістично доступні джерела інформації: результати інвентаризації, журнали подій, відомості про простої, опитування відповідальних осіб, статистику внутрішніх інцидентів і галузеві експертні оцінки. Надмірно складні моделі, що потребують великих масивів історичних даних, не будуть достатньо практичними для більшості підприємств середнього масштабу.

Третя група - вимоги до результатів. Отримані оцінки повинні бути придатними до інтерпретації на двох рівнях: технічному та управлінському. Для IT- та безпекових фахівців важлива деталізація загроз, вразливостей і джерел втрат. Для керівництва критично важливо бачити ранжування активів, прогноз очікуваних втрат і оцінку ефекту від контрзаходів. Таким чином, вихідними даними методики мають бути не лише бали або категорії, а й зрозумілі узагальнення для прийняття рішень.

Четверта група - вимоги до адаптивності. Методика повинна дозволяти змінювати вагові коефіцієнти, набір сценаріїв і критерії оцінювання залежно від особливостей організації. Це дає можливість використовувати її не тільки для підприємства, що стало базою практики, а й для інших організацій зі схожою структурою IT-інфраструктури.

Узагальнюючи викладене, за основу прийнято гібридну методику, де перший етап присвячений інвентаризації та визначенню критичності активів, другий - побудові моделі загроз і сценаріїв, третій - кількісній оцінці очікуваних втрат для найбільш критичних сценаріїв, а четвертий - формуванню обґрунтованих рекомендацій щодо зниження ризику. Саме така логіка використовується далі в роботі.

Узагальнені результати для цього етапу наведено в табл. 1.6.

Таблиця 1.6 – Основні вимоги до методики оцінювання

Група вимог	Зміст вимог
Повнота	Охоплення основних класів активів, властивостей CIA, типових загроз і сценаріїв втрат
Практичність	Використання доступних на підприємстві джерел даних і простих процедур збору інформації
Інтерпретованість	Можливість отримати як технічні, так і фінансово зрозумілі результати
Адаптивність	Налаштування ваг, шкал, сценаріїв та критеріїв під особливості організації
Придатність до обґрунтування рішень	Порівняння ризиків і оцінка ефекту від запропонованих захисних заходів

Висновки до розділу 1

У першому розділі виконано аналіз задачі оцінювання цінності інформаційних активів і очікуваних втрат при реалізації загроз у середовищі виробничого підприємства. Показано, що актуальність теми зумовлена високою залежністю бізнес-процесів від інформаційних систем, потребою в економічно обґрунтованих рішеннях щодо захисту та недостатністю фрагментарних підходів до пріоритезації активів.

На підставі аналізу предметної області встановлено, що інформаційні активи підприємства мають різну природу та різний вплив на операційну діяльність. Особливу роль відіграють виробничі бази даних, технологічна документація, доменні облікові записи, конфігурації мережевого обладнання та журнали подій. Це обумовлює потребу у багатокритеріальному оцінюванні активів із урахуванням конфіденційності, цілісності, доступності та ролі в бізнес-процесах.

Проведений аналіз існуючих підходів засвідчив, що найбільш придатним для умов дипломної роботи є гібридний підхід, який поєднує експертне ранжування активів і кількісне оцінювання очікуваних втрат для найбільш критичних сценаріїв.

Такий підхід спирається на загальні рамки міжнародних стандартів та дозволяє врахувати реальні дані, отримані під час переддипломної практики.

У результаті сформульовано об’єкт, предмет, мету та завдання дослідження, а також постановку задачі розроблення методики оцінювання, що має бути практичною, адаптивною, інтерпретованою й придатною до обґрунтування рішень щодо захисту активів. На цій основі здійснюється перехід до побудови моделі предметної області, деталізації критеріїв оцінювання та апробації розробленого підходу на матеріалах підприємства.

РОЗДІЛ 2

АНАЛІЗ ІСНУЮЧОЇ РЕАЛІЗАЦІЇ ОЦІНЮВАННЯ ЦІННОСТІ ІНФОРМАЦІЙНИХ АКТИВІВ ТА НАПРЯМИ ЇЇ ОПТИМІЗАЦІЇ

2.1 Загальна характеристика існуючої реалізації оцінювання

Матеріали переддипломної практики дають змогу відновити поточну логіку оцінювання, яка використовується на підприємстві як робочий, але спрощений механізм прийняття рішень. Вона починається з інвентаризації активів і попереднього ранжування за критеріями конфіденційності, цілісності та доступності, далі переходить до виділення типових загроз, після чого для частини сценаріїв виконуються розрахунки SLE та ALE. Фактично йдеться про гібридну, але дуже компактну процедуру, орієнтовану не на формальну зрілість процесу, а на швидке отримання приблизних оцінок для IT-відділу й керівництва.

Сильним боком такої реалізації є її практична застосовність. Підприємство не потребує дорогого програмного комплексу, значних масивів історичних даних або окремого підрозділу з управління ризиками. Уже на початковому етапі можна скласти реєстр активів, побачити критичні точки інфраструктури, оцінити вплив найбільш небезпечних інцидентів та підготувати стислий перелік контрзаходів. Саме тому для середовища зі зрілістю процесів нижче середньої подібний підхід виглядає привабливим: він швидко запускається і зрозумілий учасникам без тривалого навчання.

Разом із тим простота на практиці трансформується у суттєве спрощення предметної області. У звіті фігурують 17 ключових активів, з яких 6 мають високий рівень критичності; оцінювання здійснюється за шкалою 1-5 за трьома класичними критеріями, а для сервера виробничої бази даних наведено приклад SLE = 270 000 грн та ALE = 81 000 грн. Після впровадження MFA очікуване річне значення втрат у прикладі зменшується до 27 000 грн, а економічний ефект інтерпретується як 54

000 грн на рік. Ці результати добре ілюструють логіку процедури, але одночасно показують її надто високу залежність від припущень, які не завжди формалізовані.

Проблема полягає не в тому, що використані показники є неправильними самі по собі. Навпаки, CIA-модель, SLE, ARO та ALE є поширеними й методично виправданими інструментами первинного ризик-аналізу. Недолік полягає в тому, що вони застосовуються без достатньої деталізації об’єктів оцінювання, без моделі залежностей між активами та без механізму контролю якості вхідних даних. У такій конфігурації навіть формально коректна формула здатна породжувати управлінськи неточний результат.

Отже, існуюча реалізація розглядається як корисний стартовий рівень, але не як завершену методику, придатну для масштабування, автоматизації або використання як доказову основу для інвестицій у безпеку. Далі увага зосереджується на трьох питаннях: які саме складові реалізації є найбільш вразливими, чому вони обмежують достовірність результату і які напрями оптимізації дозволять підвищити практичну цінність системи оцінювання.

Узагальнені результати для цього етапу наведено в табл. 2.1.

Таблиця 2.1 – Узагальнення етапів існуючої реалізації на підприємстві

Етап	Поточний зміст	Практичний результат	Ключове обмеження
Інвентаризація	Перелік серверів, БД, облікових записів, конфігурацій, журналів подій	Виявлено 17 активів, 6 з високою критичністю	Відсутня ієрархія, власники та залежності активів
Якісна оцінка	Експертна шкала 1-5 за C, I, A	Швидке ранжування ресурсів	Однакова вага критеріїв і висока суб’єктивність
Модель загроз	Перелік типових загроз: ransomware, відмова обладнання, помилка персоналу, DDoS	Визначено пріоритетні сценарії	Сценарії неповні та слабко прив’язані до вразливостей

Етап	Поточний зміст	Практичний результат	Ключове обмеження
Кількісний аналіз	Розрахунок SLE і ALE для ключових активів	Є фінансова інтерпретація ризику	Не деталізовано склад збитків і спосіб оцінки частоти
Рекомендації	MFA, сегментація, SIEM, резервне копіювання, навчання	Підготовлено перелік заходів	Немає формального механізму порівняння альтернатив

2.2 Аналіз інвентаризації активів та побудови моделі предметної області

Початковою точкою будь-якого ризик-орієнтованого процесу є не формула, а правильне визначення того, що саме оцінюється. У поточній реалізації реєстр активів сформовано переважно як перелік технічних об’єктів і ключових даних: сервери, бази даних, облікові записи, конфігурації мережевого обладнання, журнали подій. Для швидкого старту цього достатньо, але для системного аналізу така модель є занадто плоскою. Вона не відображає життєвий цикл активу, не фіксує його бізнес-власника, не описує залежності між ресурсами і не розмежовує первинні та похідні активи.

Наприклад, виробнича база даних не існує сама по собі. Її цінність і ризик пов’язані з прикладною системою, серверною платформою, доменною інфраструктурою, каналами резервного копіювання, політиками доступу, робочими місцями технологів і навіть із графіком виробництва. Якщо оцінювати лише саму БД як ізольований об’єкт, залишається непоміченим каскадний ефект: інцидент у суміжному компоненті може призвести до тих самих наслідків, що й пряме ураження БД. Через це реєстр активів повинен відображати не просто список, а мережу логічних та операційних зв’язків.

Суттєвим недоліком є відсутність формального розподілу ролей і відповідальності. У реальній організації актив має щонайменше технічного власника, бізнес-власника та користувачів, інтереси яких можуть відрізнятися. IT-

відділ оцінює доступність, бухгалтерія підкреслює конфіденційність і цілісність фінансових даних, виробничий підрозділ акцентує на безперервності технологічного процесу. Коли ці позиції не розмежовані, фінальна оцінка перетворюється на усереднений компроміс, а не на прозорий і відтворюваний результат.

Ще одна проблема полягає у змішуванні різних класів активів в одній шкалі без чітких правил нормалізації. Дані, програмні сервіси, мережеві конфігурації, облікові записи та журнали подій мають різну природу. Для частини з них ключовою є конфіденційність, для інших - відновлюваність, для третіх - керованість доступу або діагностична цінність. Коли всі вони потрапляють у єдину бальну таблицю, порівнянність оцінок стає умовною. Оцінка 4 бали для доменного облікового запису і 4 бали для технологічної документації не означає однаковий тип шкоди й не дає однакового управлінського сигналу.

Недостатньо опрацьованим залишається питання меж активу. У практиці часто оцінюється цілий сервер, хоча насправді найбільшу цінність мають не апаратні ресурси, а дані та сервіси, які на ньому розміщені. У такому разі відновлення «заліза» може коштувати порівняно недорого, тоді як відновлення прикладного середовища, історичних даних, інтеграцій і довіри до інформації є значно дорожчим. Отже, неправильне визначення межі активу веде до спотворення й вартості, і сценаріїв загроз.

Для оптимізації цього етапу необхідно перейти від простого реєстру до структурованої моделі активів. Доцільно виокремити бізнес-активи, інформаційні активи, програмно-технічні компоненти та підтримувальні сервіси; для кожного зафіксувати власника, місце використання, критичні залежності, допустимий час простою, допустиму втрату даних і джерела доказів щодо цінності. Така деталізація не є бюрократією заради форми. Вона забезпечує підставу для того, щоб наступні розрахунки втрат і ризику спиралися на реальну операційну картину, а не на набір інтуїтивних оцінок.

2.3 Аналіз критеріїв цінності активів і процедури їх шкалювання

У наявній реалізації критичність активу визначається як середнє значення оцінок конфіденційності, цілісності та доступності. Такий підхід зрозумілий, традиційний і технічно простий, однак саме в простоті міститься його методичне обмеження. Усереднення трьох показників приховує ситуації, коли один критерій має критичне значення, а два інші є помірними. Для частини промислових активів цього вже достатньо, щоб ризик вважався дуже високим, але середня арифметична може «згладити» картину і опустити актив нижче в пріоритетному списку.

Особливо проблематичною є гіпотеза про рівність ваг C, I та A. Для виробничого підприємства це припущення рідко виконується. Наприклад, для технологічних параметрів плавки і виробничих рецептів порушення цілісності часто небезпечніше, ніж тимчасове розголошення. Для серверів і мережевих шлюзів критичною є доступність. Для фінансової й кадрової інформації першочерговою стає конфіденційність. Таким чином, універсальне усереднення суперечить реальному пріоритету бізнес-процесів і штучно вирівнює те, що за своєю природою є нерівнозначним.

Додатковий недолік пов’язаний із низькою роздільною здатністю шкали 1-5. У невеликих командах така шкала зручна, але при різних інтерпретаціях критеріїв вона швидко втрачає точність. Один експерт вважає 5 балів ознакою повної зупинки виробництва, інший - будь-якою фінансовою втратою вище певного порога, третій - порушенням законодавчих вимог. Якщо рубежі шкали не формалізовані, самі бали перестають бути стандартизованими. У результаті зміна складу експертів або навіть зміна контексту обговорення може помітно змінити значення критичності без фактичної зміни стану активу.

Поточний підхід майже не враховує фактор невизначеності. Експерт змушений поставити одне число, навіть якщо не має достатньої впевненості або має лише часткові дані. Це стимулює псевдоточність: оцінка виглядає чіткою, хоча насправді за нею стоїть широкий діапазон можливих інтерпретацій. У системах управління ризиком така ілюзія точності є небезпечнішою за чесне визнання

інтервалу, бо керівництво схильне сприймати єдине число як факт, а не як наближення.

Крім того, модель CIA не охоплює всіх критеріїв, що визначають цінність активу саме для дипломної теми. В економічному плані важливими є відновлюваність, залежність від активу інших сервісів, регуляторні наслідки, вплив на репутацію, наявність дублювання, складність розслідування інциденту, чутливість до помилки персоналу, а також швидкість виявлення компрометації. Якщо ці чинники не винесені в окремі параметри, вони або губляться, або неформально змішуються з C, I та A, що знову ж таки погіршує відтворюваність оцінювання.

Оптимізація цього етапу полягає у переході до багатокритеріальної зваженої моделі. До базових складових слід додати бізнесову важливість, відновлюваність та регуляторно-договірні наслідки, а також зафіксувати словесні описи кожного рівня шкали. Тоді оцінка стане не лише точнішою, а й пояснюваною. Важливо, щоб користувач системи міг побачити, чому актив отримав саме такий рівень критичності, які критерії дали основний внесок і які з них мають найвищу вагу для конкретної організації.

Для оптимізованого варіанта доцільно використовувати інтегральний показник, у якому поєднуються правило максимального впливу, ваги критеріїв, коефіцієнти достовірності оцінки та грошова значущість активу. Остаточна формалізація цієї моделі перенесена до підрозділу 3.2, де наведено формули (3.1)–(3.4), шкалу 0–3 та правило переходу від грошової оцінки до бальної.

Узагальнені результати для цього етапу наведено в табл. 2.2.

Таблиця 2.2 – Порівняння поточної та оптимізованої моделі оцінювання цінності активів

Компонент	Поточна реалізація	Оптимізований підхід	Очікуваний ефект
Критерії	Лише C, I, A	C, I, A + бізнесова значущість,	Повніше відображення реальної цінності активу

Компонент	Поточна реалізація	Оптимізований підхід	Очікуваний ефект
Ваги	Неявно рівні	Налаштовувані залежно від предметної області	Усунення штучного вирівнювання критеріїв
Шкала	1-5 без повної формалізації рубежів	Шкала з текстовими дескрипторами і прикладами	Підвищення повторюваності оцінки
Невизначеність	Не враховується	Можливість фіксувати довірчий рівень або інтервал	Чесніше представлення якості даних
Пояснюваність	Результат як одне число	Декомпозиція внеску кожного критерію	Придатність до захисту перед керівництвом

2.4 Аналіз моделі загроз, вразливостей і сценаріїв реалізації інцидентів

У звіті з практики наведено перелік базових загроз: ransomware, відмова обладнання, несанкціонований доступ, помилка персоналу, DDoS-атака на VPN. Для первинного аналізу це доречний набір, але він радше виконує роль загального переліку небезпек, ніж повноцінної сценарної моделі. Між загрозою, вразливістю, активом і наслідком існує ланцюг причинно-наслідкових зв’язків, який у поточній реалізації описаний не повністю. Саме через це оцінювання іноді зводиться до загального судження «загроза небезпечна», а не до формалізованого сценарію «джерело загрози експлуатує конкретну слабкість певного активу і породжує визначений тип збитків».

Найпомітнішою проблемою є змішування різних рівнів абстракції. Наприклад, ransomware - це клас загрозливої події, відмова обладнання - тип технічного інциденту, помилка персоналу - організаційний фактор, а DDoS на VPN - уже майже готовий конкретний сценарій. Така неоднорідність ускладнює порівняння оцінок. В одному випадку аналізується цілий клас атак, в іншому -

одиничний вектор впливу, в третьому - першопричина, що може породити безліч різних інцидентів.

Ще одне обмеження полягає у недостатньому врахуванні передумов реалізації загроз. Частота й наслідки атаки залежать не лише від самого джерела загрози, а й від наявності відкритих сервісів, якості сегментації мережі, стану резервного копіювання, рівня привілейованого доступу, практики адміністрування, журналювання та моніторингу. Якщо ці передумови не внесені до моделі, неможливо пояснити, чому для одного й того самого активу одна загроза вважається високою, а для іншого - помірною.

Для виробничих систем важливим є також часовий і каскадний вимір сценарію. Наприклад, компрометація доменного облікового запису адміністратора може спочатку не спричинити жодних видимих втрат, але через певний час призвести до шифрування виробничої БД, відключення сервісів резервного копіювання і блокування віддаленого доступу. Поточна реалізація переважно оцінює інциденти як одноетапні, тоді як у реальних атаках наслідок формується через послідовність взаємопов’язаних кроків.

Модель загроз також потребує прив’язки до джерел доказів. Внутрішні журнали подій, статистика CERT-UA, результати аудиту конфігурацій, перелік типових вразливостей, історія відмов обладнання, дані про резервні копії та дисципліну оновлень повинні працювати не як загальний фон, а як елементи підтвердження конкретних сценаріїв. Інакше сценарії залишаються декларативними, а кількісні оцінки - слабко верифікованими.

Оптимізована реалізація має перейти від списку загроз до бібліотеки сценаріїв. Для кожного критичного активу необхідно фіксувати джерело загрози, вразливість або передумову, спосіб реалізації, найбільш ймовірні наслідки, засоби виявлення, існуючі контрзаходи та типи втрат. Такий підхід не лише підвищує точність оцінки, а й створює пряму основу для проектування запропонованої методики або програмного модуля у наступному розділі.

2.5 Визначення частоти подій та показника ARO

Показник ARO у поточній реалізації визначається на основі аналізу журналів за два роки, використання статистики CERT-UA та експертної оцінки адміністратора. На перший погляд це збалансоване поєднання внутрішніх та зовнішніх джерел, однак проблема полягає в їхній неоднорідності. Внутрішні журнали відображають локальний досвід підприємства, CERT-UA показує загальнонаціональний або галузевий фон, а експертна оцінка - суб'єктивне бачення конкретного фахівця. Поєднання таких джерел без формальних правил калібрування створює ризик методичного довільного вибору значень.

Дворічний горизонт спостереження є надто коротким для низькочастотних, але високонебезпечних подій. Якщо за два роки на підприємстві не було інциденту шифрування БД, це не означає, що річна частота близька до нуля; це лише означає, що внутрішня історія не містить достатніх спостережень. Навпаки, для часто повторюваних технічних збоїв дворічна статистика може бути корисною, але тоді постає питання репрезентативності: чи однаково журналювалися події протягом усього періоду, чи не змінювалась конфігурація середовища, чи не було пропусків у фіксації інцидентів.

Використання зовнішньої статистики теж вимагає обережності. Дані CERT-UA або інших центрів реагування показують загальний рівень загроз, але не враховують специфіку конкретного підприємства: його архітектуру, розмір, профіль атакуваної поверхні, рівень сегментації, дисципліну резервного копіювання, частоту оновлень, людський фактор. Без адаптації до локального контексту зовнішня частота або переоцінює ризик, або, навпаки, створює хибне відчуття безпеки, якщо підприємство має слабкіші захисні механізми, ніж середнє по вибірці.

Експертна оцінка адміністратора часто є необхідною, але вона страждає від когнітивних упереджень. Людина схильна сильніше запам'ятовувати нещодавні події, перебільшувати знайомі проблеми і недооцінювати рідкісні, але руйнівні сценарії. Крім того, один експерт не може однаково добре оцінити і поведінкові, і

виробничі, і фінансові аспекти ризику. Це означає, що ARO, встановлений одноосібно, не повинен вважатися остаточним без процедури верифікації або хоча б колективного погодження.

Поточна реалізація також не враховує можливу зміну частоти в часі. Після впровадження MFA, сегментації або SIEM ARO дійсно може зменшитися, але не завжди лінійно і не для всіх типів сценаріїв. Частота інцидентів залежить від взаємодії кількох захисних шарів, зрілості реагування та швидкості виявлення. Тому проста заміна значення 0.3 на 0.1 без опису механізму такого зниження виглядає методично слабкою.

Для оптимізації ARO використовується не точкове, а інтервальне або сценарне представлення частоти. Мінімальне, базове і песимістичне значення дають значно чеснішу картину, ніж одне число. Додатково фіксую джерела даних, ступінь упевненості в оцінці та фактори, які можуть змінити частоту після впровадження контролів. Такий підхід підвищує прозорість моделі і дозволяє краще пояснювати результати управлінцям.

2.6 Підхід до розрахунків разових та річних втрат

Приклад із сервером виробничої бази даних демонструє сильний бік поточної методики: вона дозволяє швидко отримати грошову оцінку інциденту. Вартість простою у 45 000 грн за годину при середньому часі відновлення 6 годин дає SLE = 270 000 грн, а при ARO = 0.3 - ALE = 81 000 грн. Ці значення легко інтерпретувати та використовувати у службовій аргументації. Проте саме їхня наочність може приховувати складну структуру втрат, яка в поточному підході спрощена до одного домінантного компоненту - простою.

Реальні наслідки інциденту рідко обмежуються тільки зупинкою виробництва. До прямих витрат додаються витрати на відновлення середовища, перевірку цілісності даних, роботу зовнішніх підрядників, форензичний аналіз, відновлення резервних копій, понаднормову працю персоналу, комунікацію з

контрагентами, повторне введення даних, відтермінування поставок і коригування облікових документів. Якщо ці складові не включені до SLE, результат є корисним лише як груба нижня межа, але не як повний економічний еквівалент інциденту.

Другою проблемою є припущення про лінійну залежність між тривалістю простою та збитком. Для виробничого підприємства втрати часто мають пороговий або каскадний характер: перша година простою може мати обмежений вплив, але зрив зміни, печі, поставки або контрактного дедлайну різко збільшує розмір наслідків. Аналогічно відновлення роботи не завжди означає повне відновлення бізнес-процесу: після запуску сервісу може залишатися відкладений виробничий борг, накопичення незавершених операцій і потреба в повторній синхронізації даних.

Поточна реалізація майже не диференціює типи втрат залежно від виду загрози. Для ransomware, саботажу, помилки персоналу та відмови обладнання структура збитків різна. У випадку криптолокера велике значення має цілісність резервних копій та час ухвалення рішення про відновлення. Для компрометації облікових записів на перший план виходять непомітна модифікація даних, необхідність перевірки журналів та перегляд політик доступу. Для DDoS або відмови VPN збиток може бути пов’язаний не з даними, а з недоступністю сервісу для віддалених працівників і затримкою управлінських дій.

Методично слабким є і те, що ALE обчислюється як єдиний добуток SLE та ARO, хоча обидва показники самі по собі є наближенням. Коли два неточні параметри перемножуються, похибка зростає, але в поточній моделі цей ефект ніяк не відображається. У підсумку управлінське рішення спирається на число, яке виглядає точним до гривні, хоча фактично може відхилятися у значно ширших межах.

Оптимізація кількісного блоку повинна передбачати декомпозицію втрат на компоненти і перехід до сценарного аналізу. Разову втрату доцільно розбити щонайменше на прямі технологічні втрати, витрати на відновлення, контрактно-правові наслідки та вторинні організаційні витрати. Річну втрату варто оцінювати як інтервал або як набір сценаріїв з різною ймовірністю. Тоді модель зберігає

простоту сприйняття, але позбавляється найбільш небезпечних ілюзій надмірної точності.

Для більш повного розрахунку разової втрати використовується розкладення за компонентами:

$$SLE\_ext = L\_dir + L\_down + L\_rec + L\_for + L\_contr + L\_rep. \quad (2.1)$$

де SLE_ext – розширена разова втрата від інциденту;

L_dir – прямі технічні та виробничі втрати;

L_down – втрати від простою;

L_rec – витрати на відновлення систем, даних і сервісів;

L_for – витрати на аналіз інциденту та перевірку цілісності;

L_contr – договірні, штрафні або регуляторні наслідки;

L_rep – репутаційні та непрямі організаційні втрати.

Узагальнені результати для цього етапу наведено в табл. 2.3.

Таблиця 2.3 – недоліки поточного кількісного блоку оцінювання втрат

Проблема	Як проявляється	Наслідок для рішення	Напрям оптимізації
Неповний склад збитків	Ураховується переважно простій	Заниження вартості інциденту	Декомпозиція SLE на компоненти
Лінійність моделі	Втрати пропорційні годинам простою	Ігноруються пороги та каскадні ефекти	Сценарне моделювання з рівнями наслідків
Точкові значення	Одне число для SLE і ARO	Прихована невизначеність	Інтервали або мінімум-база-максимум
Однаковий підхід до різних загроз	Структура збитку не залежить від типу інциденту	Слабка адекватність моделі	Окремі шаблони збитків за класами сценаріїв
Немає сліду джерел даних	Незрозуміло, як отримано окремі компоненти	Низька доказовість перед керівництвом	Паспорт оцінки з посиланням на джерела

2.7 Оцінювання ефективності контрзаходів і економічного обґрунтування захисту

У поточній реалізації після впровадження MFA для вибраного сценарію ARO зменшується з 0.3 до 0.1, а ALE - з 81 000 грн до 27 000 грн. Звідси робиться висновок про економічний ефект у розмірі 54 000 грн на рік. Така логіка демонструє правильний напрям думки: захисний захід повинен оцінюватися не як технічна прикраса, а як інструмент зменшення очікуваних втрат. Однак для повноцінного управлінського висновку цього недостатньо.

По-перше, оцінювання зосереджене лише на одному параметрі - зниженні частоти. Насправді контрзахід може впливати не тільки на ARO, а й на розмір разової втрати. Наприклад, ізоляція сегментів мережі не лише зменшує ймовірність горизонтального поширення атаки, а й обмежує масштаб збитків. Регулярне тестування резервних копій скорочує тривалість відновлення, тобто безпосередньо впливає на SLE. SIEM може не запобігти події, але скоротити час виявлення і таким чином зменшити втрати. Отже, редукція ефекту контролю лише до ARO спрощує картину.

По-друге, поточний розрахунок не враховує повну вартість самого контрзаходу. Впровадження MFA, сегментації, SIEM або навчання персоналу має капітальні та операційні витрати: ліцензії, інтеграцію, налаштування, адміністрування, підтримку, аудит, витрати часу співробітників, можливе зниження продуктивності, навчання і супровід змін. Якщо розглядати лише різницю ALE, можна помилково визнати вигідним захід, який фактично не окупається або окупається лише в довгому горизонті.

По-третє, нинішній підхід слабо враховує взаємодію контролів між собою. У реальному середовищі безпека формується сукупністю шарів. MFA без ревізії привілейованих облікових записів і журналювання дає менший ефект; сегментація без якісного управління правилами доступу теж не вирішує проблему; резервні

копії без перевірки відновлення можуть створювати хибне відчуття захищеності. Економічне обґрунтування повинно оцінювати не поодинокий захід у вакуумі, а портфель взаємопов'язаних рішень.

Ще одна слабкість полягає у відсутності поняття залишкового ризику. Навіть після впровадження контролю ризик не зникає повністю; він змінює профіль. Частина сценаріїв стає менш імовірною, частина - легше виявляється, деякі наслідки зменшуються, але певний залишок загрози зберігається. Якщо цей залишковий ризик не оцінюється окремо, керівництво отримує надто оптимістичну картину і може припинити подальші вдосконалення зарано.

Оптимізувати блок економічного обґрунтування можна через порівняння чистого річного ефекту, строку окупності та зниження залишкового ризику. Для кожного заходу або пакета заходів слід оцінювати зміну SLE, зміну ARO, сукупну вартість володіння, організаційну складність впровадження і залежність від інших контролів. Така модель складніша за поточну, зате вона набагато краще відповідає вимозі дипломної теми: показати не просто факт існування ризику, а економічно обґрунтований спосіб його зменшення.

Чистий річний ефект від контрзаходу визначається не як просту різницю між двома ALE, а як різницю з урахуванням витрат на захист:

$$E_{net} = (ALE_{before} - ALE_{after}) - TCO_{ctrl}. \quad (2.2)$$

де E_{net} – чистий річний ефект;

ALE_{before}, ALE_{after} – очікувані річні втрати до та після впровадження контролю;

TCO_{ctrl} – повна річна вартість володіння та підтримки контролю.

2.8 Підхід організаційної реалізації процесу оцінювання

Навіть добре підібрані показники не працюють належним чином, якщо організаційний процес оцінювання побудований епізодично. За матеріалами практики видно, що аналіз проводився IT-відділом спільно з окремими

представниками бухгалтерії та виробничого підрозділу, причому значна частина дій мала консультативний або аналітичний характер. Для переддипломної практики це природно, однак для постійного функціонування системи ризик-аналізу така форма є недостатньо формалізованою. Потрібні сталі ролі, регламент перегляду оцінок і процедура погодження результатів.

Слабким місцем є відсутність чітко закріпленого власника методики. Якщо реєстр активів веде ІТ-відділ, а фінансові параметри оцінює бухгалтерія, без формального координатора з'являється ризик розриву між технічним і бізнесовим баченням. З часом це призводить до того, що оцінки оновлюються неритмічно, частина активів випадає з поля зору, а контрзаходи впроваджуються без повернення до вихідної моделі ризику. Таким чином, сама процедура перетворюється на разову акцію, а не на цикл постійного вдосконалення.

Важливою організаційною прогалиною є невизначеність тригерів для перегляду оцінки. У реальній інфраструктурі ризик змінюється після модернізації мережі, заміни серверів, появи нового каналу віддаленого доступу, запуску нової ERP-функції, переходу на інший режим резервного копіювання або після суттєвого інциденту. Якщо переоцінка виконується лише епізодично, система швидко втрачає актуальність. Отже, потрібно запровадити календарний і подієвий режими перегляду: періодичний плановий перегляд та позапланову переоцінку після змін у середовищі.

Ще одна проблема - слабкий зв'язок між результатами оцінювання і процедурою прийняття рішень. Якщо керівництво не бачить формалізованого переліку ризиків, рівня їх прийнятності, відповідальних осіб та дедлайнів оброблення, навіть якісно проведений аналіз не переходить у практичні дії. Тому організаційна оптимізація повинна включати не лише поліпшення методики, а й ув'язку її результатів із бюджетуванням, планом захисту, внутрішнім аудитом і контролем виконання рішень.

Для підвищення зрілості процесу встановлюються щонайменше такі ролі: власник активу, власник ризику, технічний експерт, координатор методики та особа, що погоджує бізнес-пріоритет. Також пропонується впровадити короткий

паспорт оцінки для кожного критичного активу: дата перегляду, джерела даних, учасники оцінювання, поточні контролі, залишковий ризик, рішення та термін наступної перевірки. Це знижує залежність системи від окремих працівників і перетворює її на керований процес.

2.9 Критика технічної реалізації та використання інструментів оцінювання

З практичного погляду існуюча реалізація, ймовірно, спирається на табличний редактор, локальні журнали подій, ручне узагальнення даних та експертні обговорення. На ранніх етапах це цілком виправдано, але з ростом кількості активів, сценаріїв і контрзаходів ручна форма ведення ризик-моделі стає джерелом помилок. З’являються дублікати записів, різні версії таблиць, втрати контексту при оновленні, неузгоджені поля і неможливість простежити, хто саме змінив показники.

Технічна слабкість ручного обліку особливо помітна у питаннях простежуваності та історичності. Для якісного аналізу важливо бачити не лише поточну оцінку, а й те, як вона змінювалася у часі: чому актив піднявся в пріоритеті, який контроль вплинув на зменшення ARO, коли було змінено власника, які припущення лежали в основі попередніх розрахунків. У звичайній таблиці така історія часто або втрачається, або фіксується неструктуровано в коментарях, які швидко стають непридатними для аудиту.

Недостатньою є і ступінь інтеграції з реальними джерелами даних. Якщо реєстр активів не пов’язаний із доменною структурою, систерезервного копіювання, моніторингом, інвентаризацією обладнання та журналами інцидентів, то його потрібно постійно оновлювати вручну. Це дорого, повільно і майже завжди призводить до застарівання даних. Для критичних активів така затримка означає, що рішення можуть ухвалюватися на основі стану інфраструктури, якого вже не існує.

Окремо слід відзначити проблему відсутності вбудованого контролю якості даних. У ручних моделях ніхто не заважає ввести нелогічні значення, забути оновити час відновлення, залишити ARO від старої конфігурації або невірно перенести суму витрат. Якщо система не перевіряє повноту полів, допустимі межі, взаємозв'язок показників і наявність обов'язкових доказів, ризик-аналітика стає вразливою до технічних помилок майже так само, як інфраструктура - до кіберзагроз.

Технічна оптимізація не обов'язково означає негайне впровадження складної GRC-платформи. Уже на дипломному рівні пропонується модульна реалізація: структурований реєстр активів, довідник загроз і сценаріїв, блок розрахунку показників, журнал змін, форму погодження оцінок і засоби формування звітів для керівництва. Навіть простий прототип у вигляді програми або веб-модуля вирішує низку системних проблем, які ручні таблиці залишають невирішеними.

2.10 Напрями оптимізації існуючої реалізації

Критика поточного підходу має практичну цінність лише тоді, коли вона переходить у конструктивні пропозиції. Першим напрямом оптимізації є уточнення об'єкта оцінювання: замість плоского списку слід сформувати багаторівневий реєстр активів з відображенням бізнесового контексту, технічних залежностей і допустимих параметрів відновлення. Це створює основу, на якій можна зіставляти технічні інциденти з реальними наслідками для підприємства, а не лише з умовними балами.

Другий напрям перехід від однорідної CIA-оцінки до багатокритеріальної моделі з налаштовуваними вагами. Для промислового середовища ваги мають встановлюватися окремо для класів активів: дані, сервіси, конфігурації, облікові записи, журнали, канали доступу. Це не лише підвищує точність, а й дозволяє будувати правила автоматизованого ранжування, коли однаковий бал означає однаковий рівень управлінської уваги.

Третій напрям оптимізації пов’язаний зі сценарним підходом. Для кожного критичного активу створюється обмежений, але чітко описаний набір сценаріїв: порушення доступності, компрометація облікового запису, шифрування даних, спотворення технологічної інформації, втрата резервної копії, збій мережевого обладнання, інсайдерська помилка. Саме сценарії, а не абстрактні загрози, використовую як одиницю розрахунку очікуваних втрат і ефекту контрзаходів.

Четвертий напрям - нормалізація розрахунку втрат. SLE слід формувати з компонентів, ALE - представляти як базовий або інтервальний річний прогноз, а результати - показувати у формі, придатній для двох аудиторій: технічної та управлінської. Для IT-фахівця важливо бачити, які саме чинники дали найбільший внесок; для керівництва - які активи і сценарії формують найбільші очікувані витрати та які заходи дають найкращий співвідношення ефекту до вартості.

П’ятий напрям - організаційне та технічне закріплення процесу. Необхідні регламент перегляду, паспорт оцінки, журнал змін, правила погодження та мінімальна автоматизація. Навіть якщо підприємство ще не готове до повноцінної системи GRC, воно може отримати суттєвий виграш від централізованого інструмента з контрольованими довідниками, шаблонами сценаріїв і вбудованими перевірками коректності.

У сукупності ці напрями оптимізації формують логічний перехід до розробки. Вона має не просто повторити існуючі формули в іншому інтерфейсі, а вирішити конкретні проблеми: підвищити відтворюваність оцінки, зменшити суб’єктивність, зробити моделі пояснюваними, дати змогу порівнювати контрзаходи і забезпечити регулярне оновлення даних. Саме така постановка забезпечує наукову і практичну новизну подальшої частини дипломної роботи.

Узагальнені результати для цього етапу наведено в табл. 2.4.

Таблиця 2.4 – Основні напрями оптимізації існуючої реалізації

Напрям	Що саме змінюється	Яку проблему усуває	Практичний результат
Структурований реєстр активів	Активи групуються за рівнями і залежностями	Плоский список без контексту	Краща точність вибору сценаріїв
Багатокритеріальна оцінка	Ваги і критерії налаштовуються	Грубе усереднення C, I, A	Адекватніше ранжування активів
Сценарний аналіз	Оцінюються конкретні інцидентні ланцюги	Абстрактний перелік загроз	Прив’язка ризику до реальних подій
Розширений SLE/ALE	Ураховується структура втрат і невизначеність	Заниження збитків та псевдоточність	Більш переконливе економічне обґрунтування
Процес і автоматизація	Регламент, журнал змін, перевірки полів, звітність	Разовий ручний характер оцінювання	Стійкість і відтворюваність системи

2.11 Вимоги до удосконаленої реалізації та перехід до розробки

Після аналізу недоліків формулюються вимоги до удосконаленої реалізації, яка може стати предметом розробки. Передусім вона має бути практичною для підприємства середнього масштабу: не вимагати надмірної кількості ручних операцій, не залежати від унікальної експертизи однієї особи та не спиратися на дані, яких організація фактично не здатна зібрати. Це принципово, оскільки надмірно складна модель часто програє простішій лише тому, що не приживається у реальному середовищі.

Друга вимога - пояснюваність. Кожне підсумкове значення повинно розкладатися на зрозумілі компоненти: які критерії сформували цінність активу,

які сценарії дали найбільший внесок у річний ризик, які припущення були використані для частоти, які втрати враховано і як саме контрзахід змінює модель. Без такого розкладання система буде видавати цифри, але не створюватиме довіри з боку керівництва і не стане інструментом прийняття рішень.

Третя вимога - адаптивність. Удосконалена реалізація повинна дозволяти змінювати ваги критеріїв, довідники активів, сценарії, шаблони збитків і правила агрегації залежно від типу підприємства. Для ливарного виробництва один профіль важливості, для медичної установи або торговельної компанії - інший. Якщо модель не допускає адаптації, вона швидко перетворюється на жорсткий шаблон, придатний лише для одного кейсу.

Четверта вимога - підтримка оцінювання заходів захисту. Система повинна не тільки показувати «де болить», а й дозволяти моделювати «що зміниться, якщо впровадити конкретний захід». Саме цей функціонал є найбільш цінним для дипломної теми, оскільки переводить оцінку з режиму констатації у режим проєктування рішень. Керівник або фахівець з безпеки має бачити, які контрзаходи знижують ризик найбільш відчутно, які є залежності між ними і яким є чистий економічний результат.

П’ята вимога - фіксація невизначеності й джерел даних. Удосконалений інструмент повинен зберігати не лише числові значення, а й дату оцінки, походження параметрів, рівень довіри та відповідального експерта. Це важливо для повторного перегляду, внутрішнього аудиту та поступового накопичення організаційної пам’яті. Саме завдяки такій пам’яті модель з часом стає кращою, а не просто перезапускається щоразу «з чистого аркуша».

Отже, сформульовані у другому розділі вимоги задають основу для власного методу та програмної реалізації, які усувають ключові недоліки існуючого підходу. орієнтуюся на інструмент, що поєднує багатокритеріальну оцінку активів, сценарний аналіз загроз, розрахунок очікуваних втрат, оцінювання ефективності контрзаходів і базову автоматизацію процедур оновлення та звітності.

Узагальнені результати для цього етапу наведено в табл. 2.5.

Таблиця 2.5 – Вимоги до удосконаленої реалізації оцінювання

Група вимог	Зміст вимоги	Чому це важливо
Функціональні	Реєстр активів, сценарії загроз, розрахунок втрат, аналіз контрзаходів	Покриває повний цикл від оцінки до рішення
Методичні	Налаштовувані критерії, ваги, шаблони збитків, фіксація невизначеності	Підвищує коректність і адаптивність
Організаційні	Ролі, погодження, періодичний перегляд, журнал змін	Перетворює оцінювання на сталий процес
Технічні	Централізоване зберігання, валідація даних, звіти, історичність	Зменшує помилки ручного ведення
Управлінські	Пояснюваність, ранжування, ROI/ефект від контролів	Дозволяє обґрунтовувати інвестиції у захист

Висновки до розділу 2

У другому розділі здійснено критичний аналіз існуючої реалізації оцінювання цінності інформаційних активів та очікуваних втрат, яка застосовувалася на базовому підприємстві під час переддипломної практики. Показано, що її сильними сторонами є простота, швидкий запуск, зрозумілість для користувачів та наявність базової фінансової інтерпретації ризику через показники SLE і ALE.

Разом із тим установлено низку суттєвих обмежень. До них належать плоска модель активів без повного врахування залежностей і власників, надмірна залежність від експертного судження при оцінці критичності, неповна сценаризація загроз, спрощене визначення ARO, неповний склад збитків при розрахунку SLE та відсутність формального підходу до оцінювання ефективності контрзаходів і залишкового ризику.

Окремо виявлено організаційні та технічні недоліки: епізодичний характер процедури, недостатню формалізацію ролей, відсутність журналу змін, слабку інтеграцію з джерелами даних і високу ймовірність помилок ручного ведення. Це обмежує можливість масштабування існуючого підходу та знижує його доказову силу при обґрунтуванні витрат на безпеку.

На підставі проведеної критики сформульовано основні напрями оптимізації: перехід до структурованого реєстру активів, використання багатокритеріальної зваженої моделі оцінювання, сценарний аналіз загроз, розширений розрахунок очікуваних втрат, формалізацію процесу та мінімальну автоматизацію. Далі здійснюється перехід до запропонованої методики та програмної реалізації оцінювання.

РОЗДІЛ 3

РОЗРОБКА ГІБРИДНОГО МЕТОДУ ТА ПРОГРАМНОГО МОДУЛЯ ОЦІНЮВАННЯ ЦІННОСТІ ІНФОРМАЦІЙНИХ АКТИВІВ І ОЧІКУВАНИХ ВТРАТ ПРИ РЕАЛІЗАЦІЇ ЗАГРОЗ

У межах розробки формується гібридний підхід до розв’язання задачі оцінювання цінності інформаційних активів і очікуваних втрат при реалізації загроз. Отже, здійснюється перехід від аналізу та критики наявної практики до практичного рішення, яке охоплює методичну, організаційну й програмну складові. Для прийняття управлінських рішень у сфері інформаційної безпеки, недостатньо навести набір формул; потрібно створити зрозумілий, відтворюваний і придатний до автоматизації процес.

Базова ідея розробки полягає у поєднанні трьох підходів, які в попередніх розділах були розглянуті окремо. Перший підхід - багатокритеріальне оцінювання цінності активу, що дозволяє врахувати не тільки конфіденційність, цілісність і доступність, а й бізнесову значущість, складність відновлення та можливі регуляторні наслідки. Другий підхід - сценарне оцінювання загроз і втрат, яке переводить абстрактну категорію ризику у конкретні події з конкретними наслідками. Третій підхід - програмна підтримка процесу, що забезпечує накопичення даних, прозорість розрахунків, історичність оцінок і можливість оперативного перегляду результатів.

Запропонований підхід орієнтований на умови виробничого підприємства, однак не обмежується лише цим середовищем. Його можна масштабувати для організацій, у яких існують залежності між сервісами, бізнес-процесами, виробничими даними, мережевою інфраструктурою та обліковими системами. Саме така ситуація спостерігалась на базовому підприємстві під час переддипломної практики: найбільшу складність створювали не окремі активи як ізольовані об’єкти, а їхня взаємозалежність, нерівномірна критичність і різний

характер потенційних втрат. Отже, розробка повинна враховувати не лише стан активу, а і його місце в загальній системі функціонування підприємства.

3.1 Концепція гібридного методу оцінювання та вимоги до нього

Потреба у власній розробці виникає безпосередньо з результатів другого розділу. Критичний аналіз наявної реалізації показав, що на підприємстві фактично використовується корисний, але спрощений інструментарій: експертне визначення важливості активів, обмежений перелік загроз, приблизна оцінка частоти інцидентів і розрахунок SLE/ALE для окремих сценаріїв. Така реалізація дозволяє швидко зорієнтуватися у проблемному полі, однак не забезпечує необхідної точності, пояснюваності та стійкості результатів у момент, коли керівництво має вирішувати питання пріоритетності захисту, бюджету та допустимого рівня ризику.

Отже, розробка повинна розв’язати одночасно кілька задач. По-перше, вона має усунути розрив між якісним описом активів і кількісною оцінкою збитків. По-друге, вона повинна формалізувати той досвід, який у поточній практиці існує лише у вигляді експертних суджень окремих працівників. По-третє, розроблений підхід має бути придатним до програмної реалізації, щоб результати оцінювання не залежали від випадкової структури таблиці чи особистого стилю ведення документації окремим аналітиком.

У роботі пропонується гібридний багатокритеріальний сценарний метод оцінювання цінності інформаційних активів та очікуваних втрат. Його гібридність означає поєднання експертних оцінок, нормалізованих шкал, фінансових показників, сценарного опису інцидентів і факторів невизначеності. Багатокритеріальність означає, що цінність активу більше не зводиться лише до CIA-тріади, а оцінюється за ширшим набором ознак. Сценарність означає, що розрахунок втрат виконується не для абстрактного «ризику загалом», а для конкретного ланцюга подій із заданими умовами реалізації, передумовами та наслідками.

На відміну від традиційного підходу, де актив часто оцінюється як ізольований елемент реєстру, розроблений метод трактує актив як об’єкт у мережі залежностей. Це означає, що оцінка цінності активу має враховувати його вплив на пов’язані сервіси, бізнес-процеси та інші активи. Так, сервер виробничої бази даних є цінним не лише через власну апаратну вартість, а тому, що від нього залежить планування змін, облік виконання операцій, взаємодія з ERP-модулем, подальша аналітика та своєчасне виконання договірних зобов’язань.

Ключовою рисою розробленого рішення є включення коефіцієнта достовірності оцінки. У традиційних табличних моделях однакову вагу можуть мати оцінки, отримані з різною якістю підтверджень: одна оцінка базується на логах і фінансових документах, інша - на суб’єктивному припущенні експерта. Запропонований метод дає змогу фіксувати джерела даних і через коефіцієнт достовірності коригувати інтегральний результат. Таким чином, підсумкова оцінка стає не лише числом, а числом із поясненням, на чому воно побудоване.

Ще одна відмінність полягає у двоконтурній природі методу. Перший контур - аналітичний - призначений для визначення поточної цінності активу, сценарних збитків і річних очікуваних втрат. Другий контур - управлінський - використовується для оцінки доцільності контрзаходів, розрахунку залишкового ризику та пріоритезації проєктів захисту. Така двоконтурність важлива, оскільки в реальній практиці організація цікавиться не тільки тим, «який ризик існує», а й тим, «що саме потрібно зробити насамперед і який ефект це дасть».

Отже, розроблений підхід виступає центральним практичним результатом дослідження. У ньому результати аналізу, критики та формалізації переходять у рішення, придатне для впровадження на підприємстві. Саме тому далі послідовно описуються принципи методу, математичну модель, алгоритм функціонування, структуру програмного модуля та приклад апробації у виробничому середовищі.

3.2 Формальна модель, система показників і вхідні дані

Проєктування методу починається з формулювання принципів, які мають бути покладені в його основу. Без цього розробка ризикує повторити недоліки існуючої реалізації, лише у більш складній формі. Першим принципом є принцип предметної адекватності. Він означає, що всі критерії, шкали та формули повинні відображати саме ті втрати і залежності, які дійсно характерні для базового підприємства. Для виробничого середовища це насамперед вплив на безперервність процесів, час відновлення, коректність технологічних даних і можливість каскадного поширення наслідків на суміжні ділянки IT-інфраструктури.

Другим принципом є принцип пояснюваності. Будь-яке підсумкове значення, яке формує система, має розкладатися на зрозумілі компоненти: які критерії були використані, яку вагу вони мали, які джерела підтверджують оцінку, який сценарій втрати було обрано і які параметри вплинули на частоту події. Для дипломної роботи цей принцип особливо важливий, оскільки він дає змогу захистити запропоноване рішення не лише як «працюючий розрахунок», а як методично обґрунтовану систему прийняття рішень.

Третім принципом є адаптивність. Розроблений метод не повинен бути жорстко прив’язаним до одного-єдиного набору ваг або одного набору загроз. На практиці підприємства відрізняються за моделлю процесів, галузевими вимогами та рівнем цифрової залежності. Отже, метод має дозволяти змінювати вагові коефіцієнти критеріїв, оновлювати бібліотеку загроз, обирати різні типи втрат і коригувати коефіцієнти ефективності контрзаходів без повного перепроєктування всієї системи.

Четвертий принцип - це простежуваність оцінки в часі. Ризики та цінність активів є динамічними; вони змінюються разом із модернізацією інфраструктури, появою нових сервісів, зміною складу даних і впровадженням контролів. Тому розроблений підхід повинен зберігати версійність розрахунків: коли виконано оцінку, хто її погодив, які параметри застосовано, які документи або логи були

джерелом чисел. Саме наявність історії дає змогу згодом порівнювати стани «до» і «після» впровадження захисних заходів.

П’ятим принципом є економічна інтерпретованість результатів. Для технічного спеціаліста важливо бачити вплив конкретної вразливості на систему, а для керівництва - отримувати відповідь у зрозумілому вигляді: які можливі втрати, який контроль доцільно впровадити першим, скільки це коштуватиме і коли окупиться. Тому розроблений метод повинен підтримувати як відносні показники критичності, так і грошовий вимір базової цінності активу, разової втрати, річної очікуваної втрати та економічного ефекту від контрзаходів.

Шостим принципом є врахування невизначеності. У галузі інформаційної безпеки неможливо побудувати абсолютно точну модель: частина параметрів базується на статистиці, частина - на експертних оцінках, а частина - на аналітичних припущеннях. Ігнорування цього факту створює оману точності, коли користувач сприймає результат як незаперечне число. У межах розробки пропонується враховувати невизначеність через коефіцієнт достовірності даних, базовий, оптимістичний та песимістичний сценарії, а також окрему фіксацію джерела кожної оцінки.

Нарешті, сьомим принципом виступає автоматизовуваність. Метод створюється не як суто теоретична конструкція, а як основа для програмного модуля підтримки рішень. Це означає, що кожен його етап має бути алгоритмізований: від заповнення паспорта активу до формування рейтингу ризиків і побудови звіту. Завдяки цьому користувач отримає не розрізнені розрахунки в електронній таблиці, а керований процес, який може бути масштабований на десятки активів і сценаріїв.

Узагальнені результати для цього етапу наведено в табл. 3.1.

Таблиця 3.1 – Принципи побудови розробленого методу

Принцип	Сутність	Практичне значення
Предметна адекватність	Критерії і сценарії відображають реальні процеси підприємства	Зменшує розрив між розрахунком і реальною експлуатацією
Пояснюваність	Кожен підсумок розкладається на компоненти та джерела даних	Полегшує захист результатів і внутрішній аудит
Адаптивність	Ваги, сценарії та контролі можна змінювати без переробки моделі	Дозволяє масштабувати підхід на різні активи
Простежуваність	Зберігається історія оцінок та їх версій	Підтримує аналіз динаміки ризику
Економічна інтерпретованість	Результати подаються у вигляді втрат і ефекту заходів	Дає підстави для бюджетних рішень
Урахування невизначеності	Фіксується достовірність джерел і варіативність результату	Зменшує оману псевдоточної оцінки
Автоматизовуваність	Усі кроки можуть бути реалізовані програмно	Сприяє стандартизації процесу

Візуалізацію відповідного елемента подано на рис. 3.1.

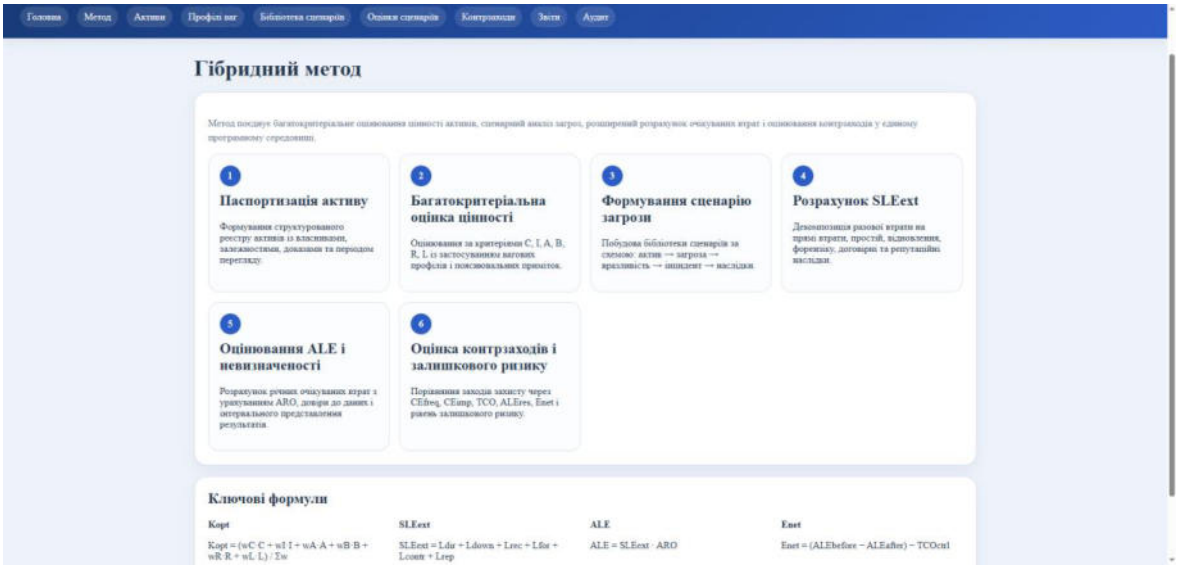

Рис 3.1 - Інтерфейс сторінки "Гібридний метод" у програмному модулі.

3.2.1 Формальна модель паспорта інформаційного активу та система вхідних даних

Практична придатність методу безпосередньо залежить від того, наскільки добре організовані вхідні дані. Саме тому центральним поняттям розробленого рішення є паспорт інформаційного активу. Паспорт розглядається не як короткий опис об’єкта, а як стандартизована картка, у якій фіксуються ідентифікаційні, технічні, процесні, фінансові та доказові характеристики активу. Такий підхід дозволяє подолати один із ключових недоліків існуючої реалізації, де активи були представлені в плоскому реєстрі без повноцінного зв’язку з бізнес-процесами та власниками.

У межах паспорта виокремлено декілька блоків. Перший блок - ідентифікаційний: унікальний код активу, назва, тип, місце розташування, належність до підрозділу, власник активу та відповідальний технічний адміністратор. Другий блок - функціональний: бізнес-процеси, які використовують актив, пов’язані інформаційні ресурси, залежні сервіси та допустимий час простою. Третій блок - фінансово-ризиковий: базова вартість активу, джерела розрахунку втрат, критичні сценарії, типові контрзаходи та параметри достовірності вихідних даних.

Окремий блок паспорта присвячений фінансовим та відновлювальним характеристикам. Сюди належать орієнтовна вартість заміни, оцінка витрат на відновлення, оцінка вартості повторного створення або реконструкції даних, втрати від простою за годину або за зміну, можливі штрафні чи договірні наслідки. Фіксація цих параметрів є критично важливою для подальшого переходу від інтегральної критичності до грошової моделі. Інакше кількісне оцінювання неминуче буде ґрунтуватися на довільних припущеннях.

Ще одним важливим елементом паспорта є блок залежностей. У ньому описуються upstream- та downstream-залежності: які сервіси чи пристрої потрібні для роботи активу і які інші елементи інфраструктури залежать від нього. Для сервера виробничої бази даних це можуть бути контролер домену, система резервного копіювання, дискова підсистема, мережевий комутатор, ERP-модуль та робочі місця диспетчерів. Наявність такого блоку дозволяє враховувати каскадність наслідків, що особливо актуально для виробничих інформаційних систем.

Паспорт активу повинен містити й доказовий блок. Для кожної числової або експертної оцінки необхідно фіксувати джерело: лог-файли, інвентаризаційні документи, договори, бухгалтерські оцінки, акти інцидентів, результати аудиту, інтерв’ю з власником активу. На підставі цього формується коефіцієнт достовірності вхідних даних. Якщо актив оцінюється переважно за документованими джерелами, достовірність є високою; якщо ж значна частина параметрів базується на експертних припущеннях, коефіцієнт має бути знижений.

Формалізація паспорта активу дає змогу перейти від неструктурованих знань до єдиного шаблону оцінювання. Це не лише підвищує якість даних, а й спрощує подальшу автоматизацію. Програмний модуль може контролювати обов’язковість заповнення полів, перевіряти логічні суперечності, підказувати допустимі діапазони та не дозволяти виконувати розрахунок без мінімального набору даних. У результаті якість вхідної інформації стає частиною самої методики, а не зовнішнім неконтрольованим фактором.

Таким чином, запропонований паспорт активу виконує подвійну функцію. По-перше, він стандартизує збір даних для методу оцінювання. По-друге, він є основою для інформаційної моделі програмної реалізації. Саме через паспорт забезпечується зв’язок між описом активу, його критичністю, сценаріями загроз, збитками, контрзаходами та історією змін.

Узагальнені результати для цього етапу наведено в табл. 3.2.

Таблиця 3.2 – Структура паспорта інформаційного активу

Блок	Ключові поля	Джерела даних	Призначення
Ідентифікаційний	Код, назва, тип, власник, адміністратор	CMDB, інвентаризація, накази	Однозначна ідентифікація активу
Функціональний	Процеси, допустимий простій, пов’язані сервіси	Інтерв’ю, регламенти, карти процесів	Зв’язок з бізнесом
Технічний	Платформа, ПЗ, сегмент, резервування, логування	Системні журнали, схеми, налаштування	Оцінка експонування і відновлюваності
Фінансовий	Вартість заміни, відновлення, простою, штрафів	Бухгалтерія, договори, розрахунки	Формування AV_base
Залежності	Upstream/downstream сервіси та їх критичність	Архітектурні схеми, експертні оцінки	Облік каскадного впливу
Доказовий	Посилання на логи, акти, документи, інтерв’ю	Документи та журнали	Підтримка коефіцієнта достовірності

Узагальнені результати для цього етапу наведено в табл. 3.2а.

Таблиця 3.2а – Приклад заповненого паспорта інформаційного активу

Поле паспорта	Приклад заповнення для сервера виробничої БД
Код активу	A-DB-PRD-01
Назва активу	Сервер виробничої бази даних
Власник активу	Начальник виробничого підрозділу / IT-відділ
Технічний адміністратор	Системний адміністратор доменної інфраструктури
Бізнес-процеси	Планування змін, облік операцій, формування маршрутних карт, контроль виконання замовлень
Ключові залежності	Active Directory, ERP-модуль, система резервного копіювання, мережевий сегмент виробництва
Допустимий простій	до 2 годин без суттєвого порушення зміни; понад 6 годин - критичний вплив
RTO / RPO	RTO = 6 год; RPO = 1 год
Оцінки C/I/A/B/R/L	C=2; I=3; A=3; B=3; R=2; L=2
Грошова база AV_base	1 180 000 грн
Основний сценарій ризику	RANS-DB-01: ransomware із шифруванням виробничої БД та зупинкою планування
Джерела доказів	Інвентаризаційний список, журнали подій, оцінка вартості простою, інтерв’ю з власником процесу
Поточні контрзаходи	Резервне копіювання, доменна автентифікація, обмеження прав доступу, журналювання подій

У табл. 3.2а показано приклад не абстрактного, а заповненого паспорта активу, який далі використовується як джерело для розрахунку критичності, грошової бази, сценарних втрат і залишкового ризику.

3.2.2 Інтегральна модель цінності інформаційного активу

$$K\_val = \max(\max(C, I, A), K\_w, S\_money). \quad (3.1)$$

У формулі (3.1) реалізовано вимогу оцінювання за максимальним значенням: якщо хоча б один із базових критеріїв CIA або грошова складова S_money має рівень 3, підсумкова критичність активу не може бути занижена середнім значенням інших показників. Тут S_money - бальна грошова оцінка активу, отримана після перетворення AV_base за табл. 3.3а.

Для всіх критеріїв застосовується єдина чотирирівнева шкала 0–3: 0 - вплив відсутній або несуттєвий; 1 - помірний вплив; 2 - високий вплив; 3 - критичний вплив на діяльність підприємства.

Таблиця 3.2б – Універсальна шкала оцінювання критеріїв 0–3

Бал	**Рівень впливу**	**Універсальний опис для критеріїв C/I/A/B/R/L**
0	Відсутній або несуттєвий	Порушення не впливає на ключові процеси, не потребує окремих витрат і не створює помітних наслідків для підприємства.
1	Помірний	Вплив локальний, обмежений одним підрозділом або коротким проміжком часу; відновлення можливе штатними засобами без значних витрат.
2	Високий	Порушення впливає на важливий бізнес-процес, потребує залучення IT/безпекових фахівців, може спричинити фінансові, договірні або репутаційні наслідки.
3	Критичний	Порушення зупиняє або суттєво спотворює ключовий процес, має каскадний вплив на залежні системи та створює значні фінансові або регуляторні втрати.

Ваги критеріїв визначаються експертною групою відповідно до типу активу: для технологічних систем вищу вагу отримують доступність, цілісність і бізнесова значущість; для фінансових та персональних даних - конфіденційність і регуляторні наслідки; для складних сервісів - відновлюваність.

Після формалізації вхідних даних наступним кроком є побудова інтегральної моделі цінності активу. Запропонована модель відходить від спрощеного усереднення критеріїв конфіденційності, цілісності та доступності й використовує розширену багатокритеріальну модель. Вона включає шість основних критеріїв: конфіденційність C, цілісність I, доступність A, бізнесову значущість B, складність відновлення R та регуляторно-репутаційні наслідки L. Кожен критерій оцінюється за шкалою 0–3, де 0 означає відсутність значущого впливу, а 3 - критичний вплив на підприємство.

На відміну від існуючого підходу, у розробленій моделі кожен критерій має не лише вагу, а й коефіцієнт достовірності. Ідея полягає в тому, що дві однакові за величиною оцінки не повинні автоматично вважатися рівнозначними, якщо одна з них підтверджена документами, а інша спирається лише на експертне припущення.

Інтегральна оцінка цінності активу визначається за формулою зваженого середнього з поправкою на достовірність:

$$K_w = (\Sigma(w_i \cdot s_i \cdot q_i)) / (\Sigma w_i). \qquad (3.2)$$

де K_w - зважена складова інтегральної оцінки; s_i - оцінка і-го критерію за шкалою 0–3; w_i - вага критерію; q_i - коефіцієнт достовірності оцінки. У межах запропонованого методу сума ваг нормується до 1, однак модель може працювати і при довільній сумі ваг, якщо ділити на суму всіх w_i.

Вибір ваг залежить від специфіки підприємства. Для виробничого середовища посилено вагу доступності, цілісності та бізнесової значущості, оскільки саме вони безпосередньо впливають на випуск продукції, коректність маршрутів, технологічні карти, планування замовлень і зупинки виробничого циклу.

Окремим завданням є перехід від інтегральної критичності до монетарної бази активу. Для цього вводиться показник базової грошової цінності AV_base,

який формується не через абстрактне множення критичності на умовний коефіцієнт, а через суму ключових компонентів вартості. У межах розробленого рішення пропонується враховувати п’ять компонентів: вартість заміни активу C_rep, вартість відновлення або реконфігурації C_res, вартість відновлення чи повторного створення даних C_data, втрати від допустимого простою C_proc та можливі регуляторно-договірні наслідки C_leg.

Базова грошова цінність активу визначається за такою залежністю:

AV_base = C_rep + C_res + C_data + C_proc + C_leg. (3.3)

де AV_base - базова грошова цінність активу. На практиці цей показник виконує роль верхньої контрольної межі для подальших сценарних розрахунків. Якщо певний сценарій не призводить до повної втрати функціональності чи даних, то для нього застосовується лише частка AV_base через коефіцієнт впливу EF. Якщо ж сценарій пов’язаний із повним руйнуванням або втратою активу, то EF може наближатися до 1.

Для демонстрації роботи моделі розглядається сервер виробничої бази даних. За результатами інвентаризації й експертного аналізу прийнято: C = 2, I = 3, A = 3, B = 3, R = 2, L = 2. При коефіцієнтах достовірності q = [0.9; 0.95; 0.95; 0.9; 0.8; 0.75] та базових вагах зважена складова K_w становить приблизно 2.40, а за правилом максимального значення K_val = 3.00. Це підтверджує критичність активу для підприємства.

Монетарна база для цього активу може бути сформована так: C_rep = 280 000 грн, C_res = 120 000 грн, C_data = 160 000 грн, C_proc = 540 000 грн, C_leg = 80 000 грн. Тоді AV_base = 1 180 000 грн. На відміну від вузького підходу, де вартість активу часто ототожнюється лише з апаратним забезпеченням або втратою простою за декілька годин, така модель краще відображає реальну економічну значущість активу для підприємства.

Після визначення грошової бази активу AV_base результат переводиться у бальну шкалу 0–3. Це потрібно для того, щоб фінансовий вимір можна було порівнювати з експертними критеріями C, I, A, B, R та L у межах єдиного рейтингу активів.

Формалізовано переведення грошової бази у бальну шкалу задається залежністю:

S_money = 0, якщо AV_base < 50 000; 1, якщо 50 000 ≤ AV_base < 250 000; 2, якщо 250 000 ≤ AV_base < 750 000; 3, якщо AV_base ≥ 750 000. (3.4)

Узагальнені результати для цього етапу наведено в табл. 3.3а.

Таблиця 3.3а – Переведення грошової оцінки активу у бальну шкалу

Бал S_money	Діапазон AV_base, грн	Інтерпретація
0	до 50 000	Несуттєва фінансова значущість; локальний вплив
1	50 000 - 249 999	Помірна значущість; втрати обмежені окремим підрозділом
2	250 000 - 749 999	Висока значущість; можливий вплив на ключовий процес
3	750 000 і більше	Критична значущість; очікувані втрати впливають на виробничу або фінансову стабільність

Для сервера виробничої бази даних AV_base = 1 180 000 грн, тому за табл. 3.3а грошова складова отримує S_money = 3. Надалі це значення використовується як додатковий контрольний показник під час формування підсумкової критичності активу.

Отже, запропонована інтегральна модель вирішує два завдання: формує узагальнений показник цінності для ранжування активів і створює монетарну основу для подальшого розрахунку збитків. Саме поєднання цих двох рівнів - відносного й грошового - становить одну з основних переваг розробленого рішення.

Узагальнені результати для цього етапу наведено в табл. 3.3.

Таблиця 3.3 – Критерії оцінювання цінності активу

Критерій	Зміст критерію	Рекомендована вага	Типова інтерпретація високого значення
C	Конфіденційність	0.15	Розкриття даних завдає значної шкоди
I	Цілісність	0.20	Спотворення даних призводить до помилкових рішень
A	Доступність	0.25	Зупинка активу зриває виробничі або офісні процеси
B	Бізнесова значущість	0.20	Актив критичний для ключових процесів
R	Складність відновлення	0.10	Відновлення потребує значного часу й ресурсів
L	Регуляторно-репутаційні наслідки	0.10	Існують штрафні, договірні або іміджеві втрати

Візуалізацію відповідного елемента подано на рис. 3.2.

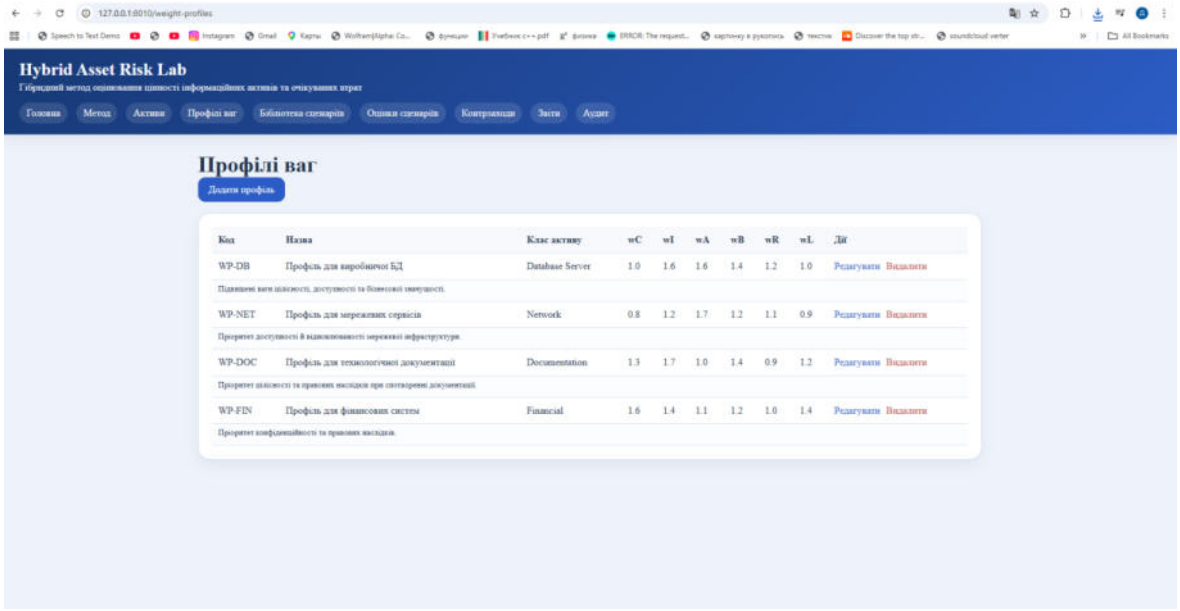

Рис 3.2 - Сторінка профілів ваг для різних класів активів.

3.2.3 Сценарна модель загроз, вразливостей і коефіцієнта впливу

Після оцінювання базової цінності активу необхідно формалізувати спосіб, у який загрози впливають на нього. У межах розробленого рішення пропонується перейти від простого списку загроз до бібліотеки сценаріїв. Сценарій розглядається як опис послідовності подій, що включає джерело загрози, вразливість або передумову, актив-ціль, можливі точки виявлення, типи порушення та перелік наслідків. Така побудова є істотно точнішою за фіксацію лише назви загрози, оскільки одна і та сама загроза може реалізуватися в різних формах і з різними наслідками.

Кожен сценарій у бібліотеці повинен містити щонайменше такі атрибути: код сценарію, назву, категорію джерела загрози, опис передумов реалізації, базовий тип впливу, набір задіяних активів, можливі каскадні наслідки, типи втрат, а також параметри для оцінювання частоти й масштабу впливу. Наприклад, сценарій «RANS-DB-01» може означати зараження робочої станції оператора, ескалацію прав, шифрування файлового шару та бази даних, блокування операційного планування і подальший простій виробничої ділянки.

Щоб забезпечити кількісне оцінювання наслідків, у роботі вводиться коефіцієнт сценарного впливу EF_s. Він характеризує частку базової грошової цінності активу, яка фактично втрачається внаслідок конкретного сценарію. На відміну від грубого експертного коефіцієнта, EF_s формується як зважена комбінація чотирьох складових: порушення конфіденційності D_conf, порушення цілісності D_int, порушення доступності D_avail та каскадного/процесного впливу D_chain.

Коефіцієнт EF_s пропонується визначати за такою формулою:

$$EF\_s = \lambda1 \cdot D\_conf + \lambda2 \cdot D\_int + \lambda3 \cdot D\_avail + \lambda4 \cdot D\_chain. \quad (3.5)$$

де λ1…λ4 - ваги складових впливу сценарію, сума яких дорівнює 1. Для виробничого підприємства раціонально підвищити вагу доступності й цілісності, оскільки втрата актуального стану виробничих даних або зупинка облікових і

диспетчерських функцій безпосередньо впливають на хід виробництва. Типовий набір ваг для таких умов: $\lambda1 = 0.15$, $\lambda2 = 0.35$, $\lambda3 = 0.35$, $\lambda4 = 0.15$.

Складова D_chain є принципово новою для розглянутого класу задач. Вона відображає не прямий вплив на актив, а той додатковий збиток, який виникає через залежні системи. Якщо відмова сервера бази даних паралізує планування, друк маршрутних карт, логістику між ділянками та подальшу передачу даних у бухгалтерський контур, то загальна тяжкість сценарію зростає навіть тоді, коли апаратне забезпечення саме по собі не зазнало фізичного знищення.

Для сценарію ransomware на сервері виробничої бази даних можна задати D_conf = 0.40, D_int = 0.80, D_avail = 0.95, D_chain = 0.60. За наведених ваг EF_s становить 0.72. Це означає, що пряме ураження активу плюс каскадний процесний вплив призводять до втрати приблизно 72 % його базової грошової цінності. Подальші прямі витрати, наприклад витрати на форензіку або комунікацію з підрядниками, додаються окремо на етапі розрахунку SLE.

Завдяки бібліотеці сценаріїв метод стає структурованим і таким, що легко автоматизується. Аналітик не формулює загрозу щоразу з нуля, а обирає типовий сценарій, адаптує його параметри до конкретного активу та при потребі створює нову версію. У програмному модулі це дає змогу повторно використовувати напрацьовані шаблони, зменшує варіативність оцінок між різними користувачами і підвищує порівнюваність результатів.

Узагальнені результати для цього етапу наведено в табл. 3.4.

Таблиця 3.4 – Фрагмент бібліотеки сценаріїв загроз

Код	Сценарій	Ключові передумови	Типові наслідки
RANS-DB-01	Шифрування виробничої БД	Компрометація облікового запису, слабка сегментація, уразливі резервні копії	Простій, втрата даних, витрати на відновлення

HW-DB-02	Відмова дискової підсистеми	Зношення носіїв, відсутність резервування, помилки моніторингу	Простій, вартість відновлення, деградація сервісу
ADM-PRIV-03	Несанкціонований привілейований доступ	Слабкий контроль адміністративних облікових записів	Зміна конфігурації, витік або спотворення даних
UPD-ERR-04	Помилка під час оновлення	Відсутність тестового контуру, слабкий регламент змін	Зупинка сервісу, відкат, витрати на відновлення
PWR-LOSS-05	Втрата живлення або збій інженерної інфраструктури	Неналежне резервування електроживлення	Аварійне завершення роботи, пошкодження даних

3.3 Алгоритм розрахунку очікуваних втрат, залишкового ризику та оцінювання контрзаходів

Критичним етапом розрахунків є оцінювання частоти реалізації сценарію. У класичному варіанті для цього використовується ARO, але в практиці підприємств саме цей показник часто стає найбільш суперечливим, оскільки реальних інцидентів мало, а доступна статистика є неповною. У межах розробленого рішення пропонується визначати ARO не як одноразову експертну константу, а як агрегований показник, що поєднує три джерела інформації: історичні дані підприємства, зовнішню галузеву статистику та структуровану експертну оцінку.

Базовий показник частоти визначається як зважена сума цих трьох джерел: історичної частоти f_hist, зовнішньої частоти f_ext та експертної частоти f_exp. До цієї суми застосовуються два коригувальні множники: M_exposure, який відображає реальний рівень експонування активу (наприклад, наявність публічних сервісів, віддалених доступів, слабкої сегментації), і M_control, який відображає поточний рівень захищеності до впровадження нових заходів.

З урахуванням зазначеного пропонується така формула:

$$ARO_{base} = (\mu1 \cdot f_{hist} + \mu2 \cdot f_{ext} + \mu3 \cdot f_{exp}) \cdot M_{exposure} \cdot M_{control}. \quad (3.6)$$

де μ1, μ2, μ3 - ваги джерел частоти, сума яких дорівнює 1; $M_{exposure} \geq 1$ при підвищеній поверхні атаки або підвищеній операційній вразливості; $M_{control} \leq 1$, якщо в системі вже діють ефективні механізми зниження ризику. Якщо ж наявні контролі формальні або не покривають сценарій, $M_{control}$ може дорівнювати 1.

Разова втрата у межах розробленого рішення обчислюється як розширений показник SLE_ext. На відміну від вузької моделі, де SLE дорівнює AV · EF, у пропонованому методі береться до уваги не лише частка втрати базової цінності активу, а й набір додаткових компонентів, що виникають у конкретному інциденті. Серед таких компонентів: витрати на реагування L_{resp}, витрати на форензичний аналіз L_{for}, витрати на відновлення із зовнішнім залученням L_{rec}, штрафні або договірні наслідки L_{contr}, репутаційні втрати L_{rep}.

Розширений показник разової втрати пропонується визначати за формулою:

$$SLE_{ext} = AV_{base} \cdot EF_s + L_{resp} + L_{for} + L_{rec} + L_{contr} + L_{rep}. \quad (3.7)$$

де SLE_{ext} - разова очікувана втрата за конкретним сценарієм. Такий підхід дозволяє поєднати логіку asset-centric оцінювання з incident-centric моделлю. Базова цінність активу відображає загальний економічний масштаб об’єкта, коефіцієнт EF_s - частку ураження в конкретному сценарії, а додаткові складові - зовнішні витрати реагування, які у багатьох реальних інцидентах становлять істотну частину збитків.

Річні очікувані втрати визначаються за класичною логікою добутку разової втрати на частоту події, однак у роботі рекомендується використовувати три значення: ALE_low, ALE_base та ALE_high. Їх формування ґрунтується на варіації коефіцієнтів EF_s і ARO залежно від рівня невизначеності. Це дозволяє керівництву бачити не псевдоточну цифру, а інтервал, у межах якого можуть знаходитися реальні втрати.

Для сервера виробничої бази даних візьмемо прикладні значення: $f_{hist} = 0.25$, $f_{ext} = 0.35$, $f_{exp} = 0.30$; ваги $\mu1 = 0.40$, $\mu2 = 0.35$, $\mu3 = 0.25$; $M_{exposure} = 1.10$; $M_{control} = 0.85$. Тоді $ARO_{base} \approx 0.278$. За AV_{base} = 1 180 000 грн, EF_s =

0.72, L_resp + L_for + L_rec + L_contr + L_rep = 120 000 грн отримаємо SLE_ext = 969 600 грн. Відповідно ALE_base ≈ 269 549 грн на рік.

Отримане значення є істотно вищим за той результат, який могла б дати спрощена методика з другого розділу. Це не означає, що попередня оцінка була «неправильною»; радше вона була неповною і не враховувала частину реально значущих витрат. Саме таким чином розроблене рішення демонструє свою практичну цінність: воно дозволяє побачити приховані компоненти збитку і уникнути систематичного недооцінювання ризику.

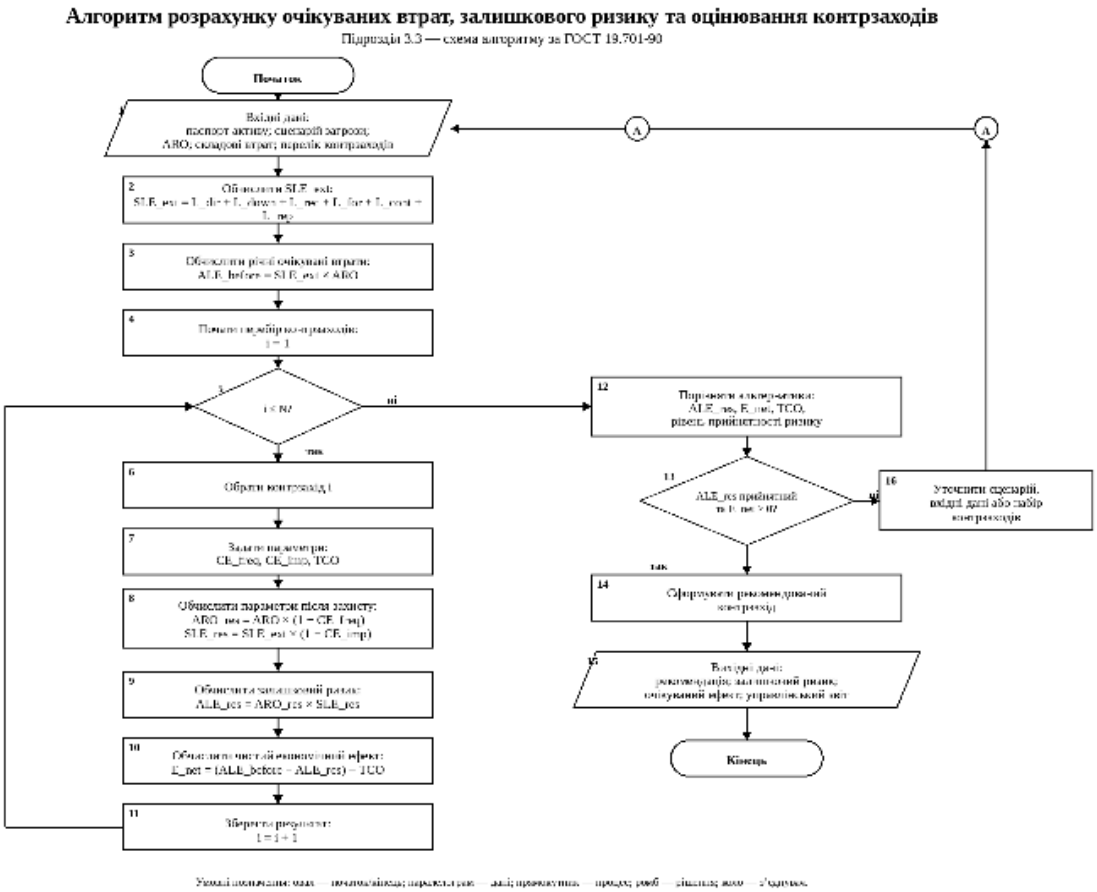

Рис 3.3 - Алгоритм розрахунку очікуваних втрат, залишкового ризику та оцінювання контрзаходів

3.3.1 Оцінювання залишкового ризику та економічної доцільності контрзаходів

Будь-яка методика оцінювання ризику має практичний сенс лише тоді, коли дозволяє обґрунтовувати рішення щодо захисту. Тому в межах розробленого

рішення окремим етапом передбачено оцінювання залишкового ризику після впровадження контрзаходів. На відміну від спрощеної моделі, де захисний захід впливає лише на ARO, у запропонованому підході контроль може змінювати як частоту реалізації сценарію, так і величину разової втрати. Наприклад, багатофакторна автентифікація здебільшого зменшує частоту компрометації, а резервне копіювання та сегментація мережі здатні істотно знизити масштаб наслідків.

Для кожного контрзаходу вводяться два показники ефективності: CE_freq - частка зменшення частоти сценарію, і CE_imp - частка зменшення його наслідків. У загальному випадку вони можуть визначатися за експертною шкалою, на основі тестових сценаріїв, за результатами аудиту або за статистикою інцидентів після впровадження. Якщо впроваджується набір контролів, їхня сукупна дія не повинна визначатися простим додаванням відсотків, оскільки це може призвести до завищених результатів. Доцільніше використовувати послідовне застосування коефіцієнтів або логіку неповного перекриття.

Залишкові значення частоти та разової втрати пропонується визначати так:

$$ARO_{res} = ARO_{base} \cdot (1 - CE_{freq}); \quad SLE_{res} = SLE_{ext} \cdot (1 - CE_{imp}). \quad (3.8)$$

де ARO_res і SLE_res - залишкові значення після впровадження контрзаходу або їх набору. Різниця між ALE_before та ALE_res показує річний обсяг зниження очікуваних втрат. Однак для управлінського рішення цього недостатньо, оскільки сам контрзахід також має вартість.

Залишкові річні очікувані втрати обчислюються за формулою:

$$ALE_{res} = ARO_{res} \cdot SLE_{res}. \quad (3.9)$$

Тому в розробленому методі використовується показник чистого річного ефекту E_net. Він визначається як різниця між зниженням очікуваних річних втрат і повною річною вартістю володіння контролем TCO_ctrl. Під повною вартістю слід розуміти не лише ліцензійні платежі, а й витрати на впровадження, супровід, навчання персоналу, адміністрування та можливий вплив на продуктивність.

Формально чистий ефект визначається так:

$$E_{net} = (ALE_{before} - ALE_{res}) - TCO_{ctrl}. \quad (3.10)$$

де $E_{net} > 0$ свідчить про економічно виправданий контроль у межах річного горизонту. Якщо $E_{net} < 0$, це не означає автоматичну відмову від заходу, оскільки для окремих критичних активів або регуляторно обумовлених сервісів контроль може бути необхідним незалежно від безпосередньої фінансової окупності. Однак навіть у такому разі показник E_{net} дозволяє коректно порівнювати альтернативні варіанти реалізації захисту.

Для прикладу розглянемо комбінацію контрзаходів для сервера виробничої бази даних: MFA для адміністраторів, сегментацію мережі, контроль привілейованих облікових записів і незмінні резервні копії. Нехай сукупно вони забезпечують $CE_{freq} = 0.45$ та $CE_{imp} = 0.40$. Тоді $ARO_{res} \approx 0.153$, $SLE_{res} = 581\,760$ грн, $ALE_{res} \approx 88\,409$ грн. Якщо повна річна вартість володіння комплексом контролів становить 92 000 грн, то чистий річний ефект E_{net} дорівнює приблизно 89 140 грн. Крім того, підприємство отримує не лише фінансовий ефект, а й зменшення операційної невизначеності.

Отже, розроблена модель залишкового ризику дозволяє об’єднати технічну та економічну логіку. Вона показує не лише те, який ризик існує, а й те, як саме він змінюється під дією конкретних заходів, у скільки ці заходи обходяться і який ефект можна очікувати у вимірі річних втрат. Саме ця властивість робить метод придатним для підтримки бюджетних та пріоритетних рішень.

Узагальнені результати для цього етапу наведено в табл. 3.5.

Таблиця 3.5 – Параметри оцінювання контрзаходів

Показник	Зміст	Діапазон	Управлінський сенс
CE_{freq}	Частка зниження частоти сценарію	0..1	Показує, наскільки контроль зменшує ймовірність події
CE_{imp}	Частка зниження масштабу наслідків	0..1	Показує, наскільки контроль пом’якшує збиток

TCO_ctrl	Повна річна вартість володіння контролем	грн/рік	Дає реалістичну вартість захисту
ALE_res	Залишкові річні очікувані втрати	грн/рік	Показує ризик після впровадження
E_net	Чистий річний ефект	грн/рік	Підтримує вибір економічно доцільного заходу

Щоб запропонований підхід можна було використовувати повторно і без двозначностей, його необхідно подати у вигляді чіткого алгоритму. Алгоритм є містком між методичною та програмною частиною дипломної роботи. З одного боку, він визначає послідовність дій аналітика, а з іншого - задає логіку функціонування програмного модуля. У межах роботи пропонується алгоритм із десяти послідовних кроків, які охоплюють повний цикл від інвентаризації активу до вибору оптимального контрзаходу.

Крок 1 полягає у створенні або актуалізації паспорта активу. На цьому етапі збираються ідентифікаційні дані, функціональні характеристики, залежності, фінансові параметри та джерела доказів. Крок 2 - верифікація повноти й якості даних. Якщо обов’язкові поля не заповнені або окремі значення суперечать одне одному, розрахунок не запускається. Крок 3 - призначення критеріїв і ваг, з урахуванням профілю підприємства та типу активу.

Крок 4 полягає у визначенні оцінок за критеріями C, I, A, B, R, L і коефіцієнтів достовірності q_i. На підставі цих даних обчислюється інтегральна цінність K_val та формується початковий рейтинг активу. Крок 5 - розрахунок базової грошової цінності AV_base за компонентною моделлю. Крок 6 - вибір одного або кількох релевантних сценаріїв із бібліотеки загроз та адаптація їх параметрів до конкретного активу.

Крок 7 передбачає оцінювання частоти сценарію. Для цього збираються історичні, зовнішні та експертні дані, після чого визначається ARO_base. Крок 8 - розрахунок коефіцієнта сценарного впливу EF_s, додаткових витрат реагування та

підсумкового показника SLE_ext. Далі, на кроці 9, обчислюється ALE_base і, за потреби, інтервал невизначеності у вигляді оптимістичного, базового та песимістичного значень.

Крок 10 полягає у моделюванні контрзаходів. Для кожного можливого заходу або їх набору визначаються CE_freq, CE_imp, TCO_ctrl, після чого розраховуються ARO_res, SLE_res, ALE_res, E_net та строк окупності. Якщо розглядається кілька альтернатив, вони ранжуються за рівнем зниження ризику, вартістю, складністю впровадження та регуляторною необхідністю. Підсумковий звіт містить як детальні числові показники, так і рекомендацію щодо пріоритетів реалізації.

Алгоритм можна подати і в більш формалізованому вигляді. Нехай A - множина активів, S - бібліотека сценаріїв, Ctr - множина контрзаходів. Для кожного $a \in A$ формується паспорт P(a), на підставі якого обчислюються K_val(a) та AV_base(a). Для кожного релевантного $s \in S$ визначаються ARO(a,s), EF(a,s), SLE(a,s), ALE(a,s). Для кожного $ctr \in Ctr$ додатково визначаються ALE_res(a,s,ctr) та E_net(a,s,ctr). Далі формується підсумкова множина рішень R(a), упорядкована за критерієм мінімізації залишкового ризику та максимізації економічного ефекту.

Перевагою такого алгоритму є те, що він не вимагає від користувача тримати всю логіку оцінювання в пам’яті. Навпаки, процедура стандартизується і стає відтворюваною. Це знижує залежність від окремого експерта, полегшує аудит результатів і дає змогу використовувати метод як внутрішній корпоративний регламент. Для дипломної роботи це також важливо, оскільки алгоритмізована форма підтверджує завершеність розробки й можливість її переходу до програмної реалізації.

Отже, розроблений алгоритм не лише описує черговість кроків, а й фіксує управлінську логіку методу. Спочатку організація описує актив і його значущість, потім переходить до сценарію та втрат, а далі - до моделювання рішень. Саме така послідовність відповідає здоровій практиці ризик-орієнтованого управління безпекою і усуває характерну помилку, коли захисні заходи обираються до того, як зрозуміло, що саме і від чого потрібно захищати.

3.4 Програмний модуль підтримки оцінювання

Оскільки розробка орієнтована на практичне застосування, її подано не тільки як метод, а й як концепцію програмного модуля. Такий модуль розглядається як інформаційно-аналітичний інструмент підтримки прийняття рішень з оцінювання цінності активів, розрахунку очікуваних втрат і вибору контрзаходів.

Архітектурно модуль побудовано за трирівневою схемою. Перший рівень - рівень представлення, на якому працює користувач: форми введення паспорта активу, вибір сценаріїв, налаштування ваг, перегляд аналітичних панелей і завантаження звітів. Другий рівень - рівень прикладної логіки, де розміщено розрахункове ядро, правила обробки сценаріїв, механізм порівняння контрзаходів і підсистему перевірки повноти даних. Третій рівень - рівень зберігання, у якому підтримуються реєстр активів, бібліотека сценаріїв, журнали змін і довідники.

Для реалізації фактичного прототипу в межах дипломної роботи використовується стек Python + FastAPI + SQLite з клієнтською частиною на базі HTML/CSS. Такий вибір дав змогу поєднати простоту розгортання, прозорість серверної логіки та достатню швидкодію для локального аналітичного інструмента.

Програмний модуль повинен підтримувати рольову модель доступу. Мінімально необхідними ролями є адміністратор системи, аналітик ризиків, власник активу, технічний експерт та керівник, що переглядає агреговані звіти. Розмежування ролей дозволяє не лише захищати дані, а й підвищує якість оцінок, оскільки кожен учасник відповідає за свій сегмент інформації. Власник активу підтверджує бізнесову значущість і допустимий простій, технічний експерт - стан резервування й уразливості, аналітик - коректність сценарної та фінансової моделі.

Функціонально модуль поділено на кілька підсистем. Перша підсистема - «Реєстр активів», яка відповідає за паспорт активу, залежності та історію змін. Друга - «Бібліотека сценаріїв», де зберігаються шаблони загроз і параметри їхнього впливу. Третя - «Розрахункове ядро», яке виконує обчислення K_val, SLE_ext, ALE, залишкового ризику та чистого ефекту від контрзаходів. Четверта - «Звітність і

візуалізація», де формуються аналітичні картки, зведені таблиці та рекомендації для керівництва.

Особливо важливою є підсистема журналювання та аудиту. Вона повинна зберігати інформацію про те, хто й коли змінив ваги, додав новий сценарій, оновив вартість простою чи переглянув оцінку ефективності контролю. Наявність такого журналу робить систему придатною до внутрішнього аудиту і дозволяє пояснити причини зміни підсумкових чисел. Для задачі дипломної роботи це є суттєвим аргументом на користь програмної реалізації, оскільки ручні таблиці майже ніколи не забезпечують належної історичності й простежуваності.

Програмний модуль також повинен підтримувати декілька режимів аналізу. Перший режим - базовий, коли оцінюється окремий актив за одним сценарієм. Другий режим - пакетний, коли проводиться оцінювання групи активів за типовим набором сценаріїв. Третій режим - сценарій оптимізації, коли система порівнює кілька альтернативних наборів контрзаходів і ранжує їх за ефектом. Саме третій режим робить систему корисною для прийняття рішень керівництвом, оскільки дозволяє не лише бачити проблему, а й вибирати найкращий варіант реагування.

Отже, проєктування програмного модуля є природним продовженням розробленого методу. Якщо метод задає правила, показники та формули, то модуль перетворює їх на керований процес. Саме поєднання методу й програмного засобу створює завершене рішення, придатне для використання на підприємстві та достатньо змістовне для дипломного дослідження.

Узагальнені результати для цього етапу наведено в табл. 3.6.

Таблиця 3.6 – Основні підсистеми програмного модуля

Підсистема	Основні функції	Результат роботи
Реєстр активів	Паспорти, власники, залежності, історія змін	Актуальний опис активів
Бібліотека сценаріїв	Шаблони загроз, передумови, параметри впливу	Стандартизовані сценарії оцінки

Розрахункове ядро	K_val, AV_base, EF_s, SLE_ext, ALE, залишковий ризик	Кількісні результати оцінювання
Каталог контролів	CE_freq, CE_imp, TCO, сумісність зі сценаріями	База для вибору заходів
Звітність	Аналітичні картки, рейтинги, управлінські звіти	Підтримка прийняття рішень
Журнал аудиту	Фіксація змін та дій користувачів	Простежуваність і контроль якості

Візуалізацію відповідного елемента подано на рис. 3.4.

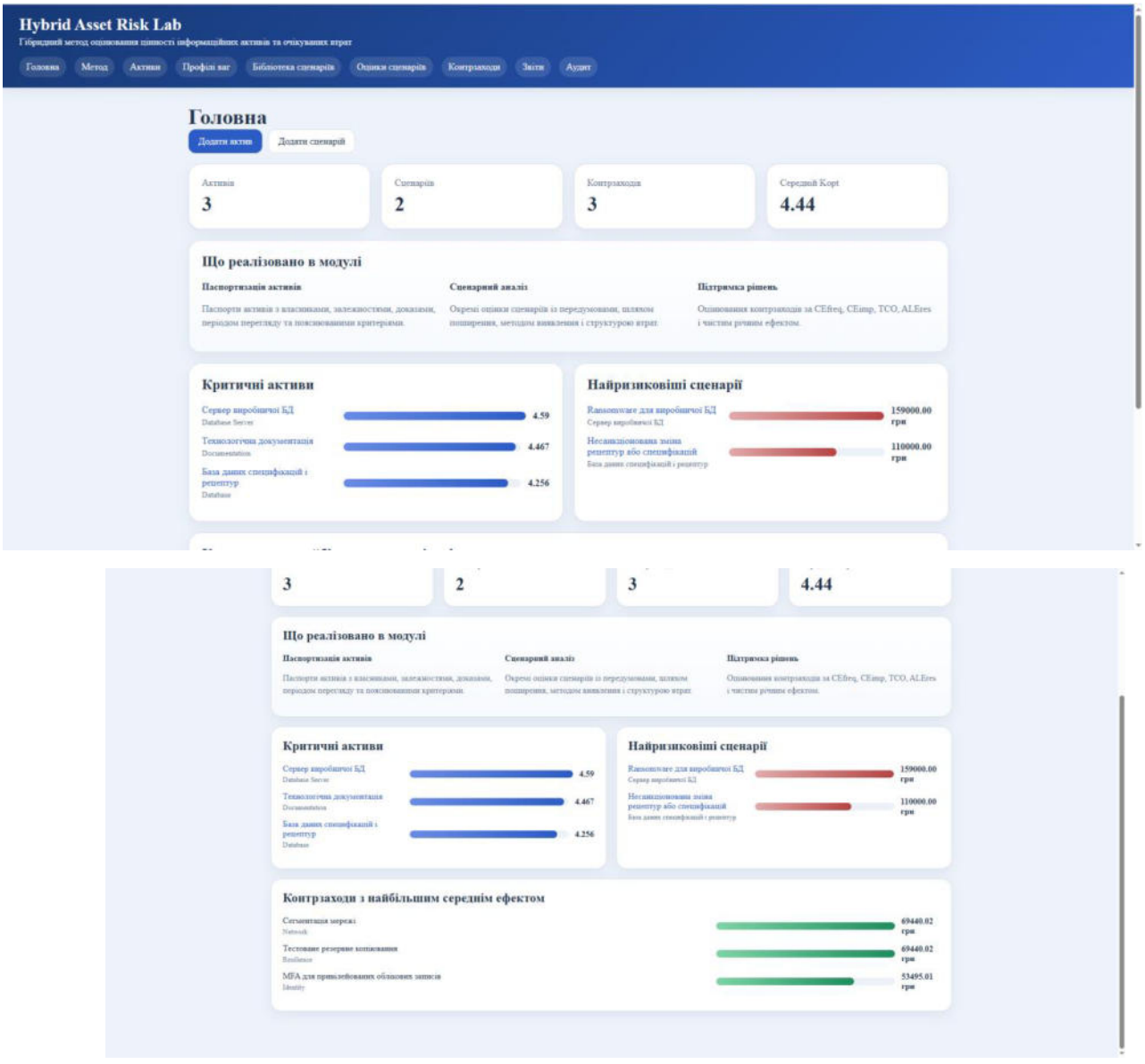

Рис 3.4 - Головна аналітична панель програмного модуля.

Візуалізацію відповідного елемента подано на рис. 3.5.

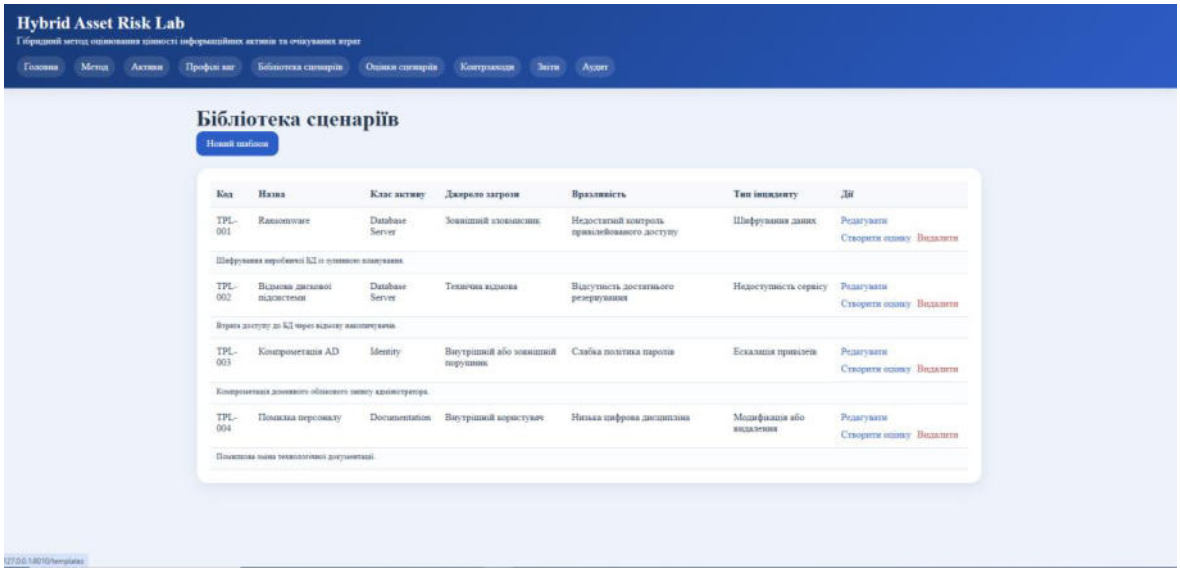

Рис 3.5 - Бібліотека сценаріїв загроз у реалізованому модулі.

3.4.1 Інформаційна модель даних і структура зберігання результатів

Щоб програмний модуль був реалізованим не лише концептуально, а й структурно, необхідно описати інформаційну модель даних. У межах дипломної роботи пропонується реляційна модель із виокремленням сутностей «Актив», «Паспорт активу», «Залежність», «Сценарій», «Оцінка сценарію», «Контрзахід», «Оцінка контролю», «Джерело доказу» та «Журнал змін». Така модель дозволяє уникнути дублювання даних і забезпечує нормалізоване зберігання інформації для подальших аналітичних обчислень.

Сутність «Актив» містить базові ідентифікаційні відомості: унікальний ідентифікатор, назву, клас активу, місце використання, статус життєвого циклу, власника та відповідального адміністратора. Сутність «Паспорт активу» містить розширені параметри оцінювання: бізнес-процеси, допустимий простій, показники C, I, A, B, R, L, ваги критеріїв, коефіцієнти достовірності, а також компонентні складові грошової цінності. Це розділення доцільне, оскільки один і той самий актив у часі може мати кілька версій паспорта.

Сутність «Залежність» описує зв’язок між активами і містить тип зв’язку, його критичність та напрям. Завдяки їй можна реалізувати функцію каскадного аналізу, коли при оцінці сценарію система враховує не тільки основний актив, а й вплив на пов’язані елементи. Сутність «Сценарій» зберігає код сценарію, опис загрози, передумови, коефіцієнти D_conf, D_int, D_avail, D_chain, а також типові додаткові витрати. Сутність «Оцінка сценарію» пов’язує конкретний сценарій із конкретним активом і фіксує параметри ARO, EF_s, SLE_ext, ALE та інтервал невизначеності.

Окремого опису потребує сутність «Контрзахід». Вона повинна містити назву заходу, його тип, сферу дії, рекомендований рівень застосування, орієнтовний TCO, CE_freq, CE_imp та набір сумісних сценаріїв. Сутність «Оцінка контролю» реалізує зв’язок між активом, сценарієм та конкретним заходом або їх набором. Саме тут зберігаються показники ARO_res, SLE_res, ALE_res, E_net, строк окупності, статус погодження та коментарі експертів.

У моделі даних важливе місце займає сутність «Джерело доказу». Для кожної оцінки має зберігатися посилання на документ, лог, акт інциденту, інтерв’ю або інше джерело. Це дозволяє не втрачати контекст походження числа і підтримує коефіцієнт достовірності q_i. Сутність «Журнал змін» зберігає дату, автора, тип дії, поле, старе значення, нове значення та підставу змін. У поєднанні ці сутності формують повну картину життєвого циклу оцінки.

З технічної точки зору така інформаційна модель добре узгоджується з реляційною базою даних і підтримує побудову SQL-запитів для формування звітів. Наприклад, можна отримати перелік активів з найбільшим ALE, список сценаріїв із найвищим коефіцієнтом EF_s, ранжування контрзаходів за чистим ефектом або історію змін оцінки окремого сервера. Крім того, модель дозволяє під’єднати зовнішні джерела даних у майбутньому, наприклад CMDB, систему резервного копіювання або SIEM.

Отже, інформаційна модель у межах дипломної роботи виконує не другорядну, а системоутворюючу функцію. Вона перетворює набір формул на структуру, придатну для зберігання, перевірки, повторного використання та

розвитку. Саме через неї розроблена методика переходить із рівня текстового опису на рівень цілісної керованої системи.

Узагальнені результати для цього етапу наведено в табл. 3.7.

Таблиця 3.7 – Основні сутності інформаційної моделі

Сутність	Ключові поля	Зв’язки	Призначення
Актив	ID, назва, тип, власник, статус	1:M з паспортами, залежностями	Ідентифікація об’єкта
Паспорт активу	Критерії, ваги, AV_base, допустимий простій	M:1 з активом	Оцінювальний профіль активу
Залежність	Актив-джерело, актив-приймач, тип, критичність	M:1 до активів	Облік каскадного впливу
Сценарій	Код, загроза, передумови, EF-параметри	1:M з оцінками сценарію	Типовий шаблон події
Оцінка сценарію	ARO, SLE_ext, ALE, інтервали	M:1 до активу та сценарію	Кількісні результати
Контрзахід	Назва, тип, CE_freq, CE_imp, TCO	1:M з оцінками контролю	Моделювання рішень
Джерело доказу	Тип, посилання, дата, опис	M:1 до паспорта або оцінки	Підтвердження даних
Журнал змін	Користувач, дата, дія, старе/нове значення	M:1 до будь-якої сутності	Аудит і простежуваність

Зовнішній вигляд відповідної форми програмного модуля подано на рис. 3.6.

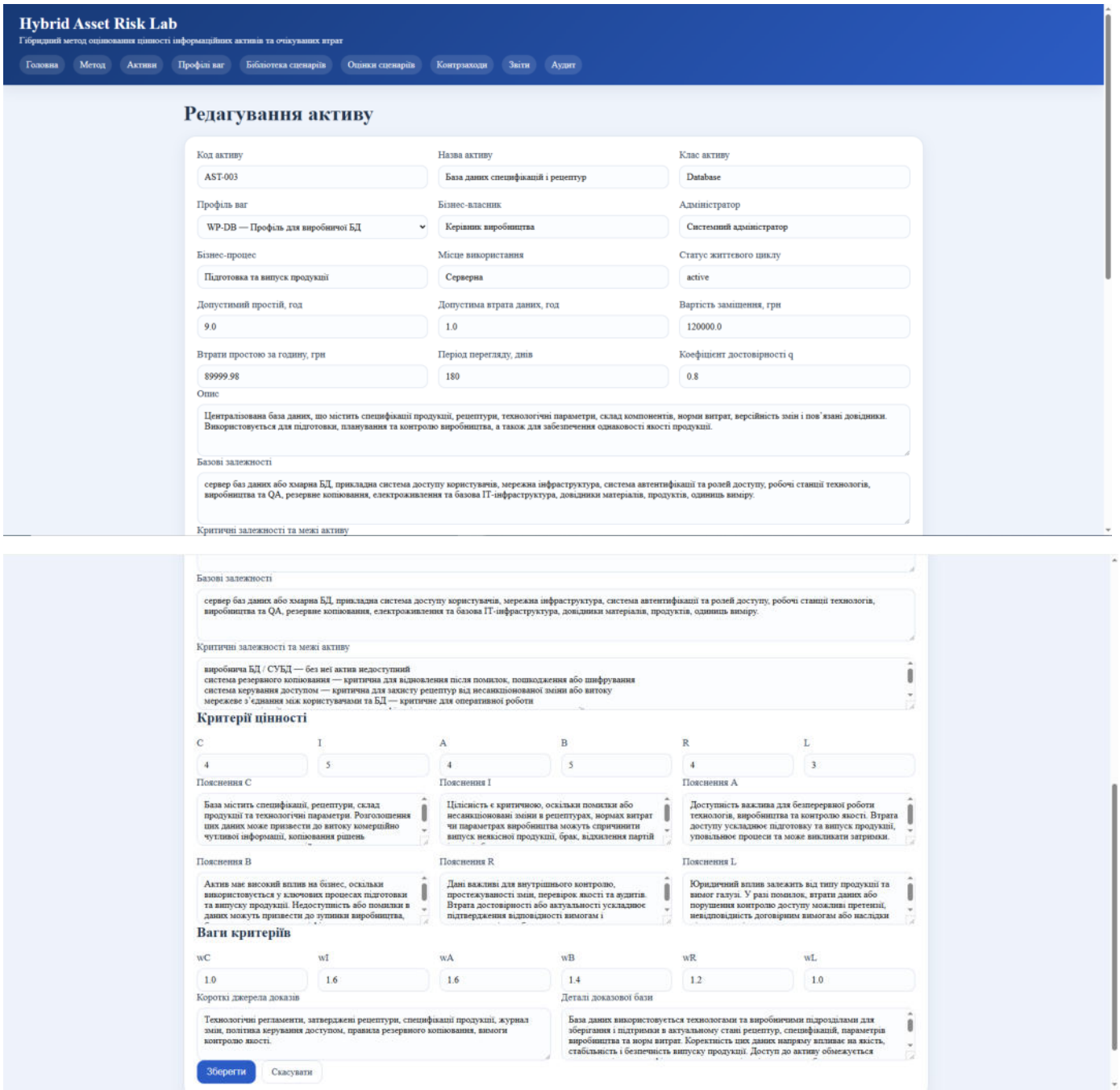

Рис 3.6 - Форма редагування паспорта активу: критерії цінності, ваги та доказова база.

Візуалізацію відповідного елемента подано на рис. 3.7.

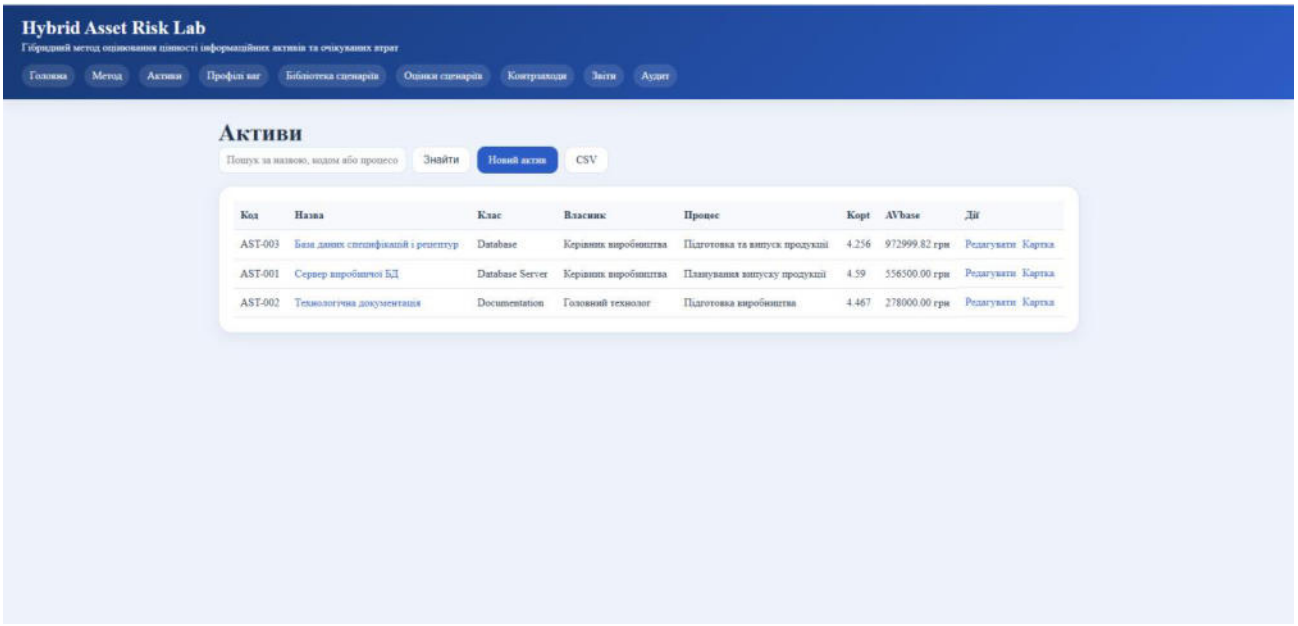

Рис 3.7 - Реєстр активів у програмному модулі.

3.4.2 Логіка роботи користувача, інтерфейсні форми та звітність

Зручність використання є однією з умов реального впровадження будь-якої аналітичної системи. Тому в межах розробки описується не лише математичні обчислення, а й логіку взаємодії користувача з програмним модулем. Пропонується сценарій роботи, у якому користувач проходить послідовність дій від створення паспорта активу до отримання аналітичного звіту й вибору контрзаходів.

На стартовій формі користувач бачить перелік активів із можливістю фільтрації за типом, підрозділом, рівнем критичності та статусом актуальності оцінки. Для кожного активу відображаються базові атрибути, дата останнього перегляду, поточний рівень критичності та максимальний показник ALE серед пов’язаних сценаріїв. Така панель виконує роль оперативного реєстру і дозволяє швидко визначити, які об’єкти потребують перегляду насамперед.

Форма паспорта активу в реалізованому модулі поділена на логічні блоки: загальні відомості, власники та ролі, операційні параметри, залежності, критерії C, I, A, B, R, L, вагові коефіцієнти та доказову базу. Такий поділ зменшує

навантаження на користувача і робить заповнення форми послідовним та пояснюваним.

Після заповнення паспорта користувач переходить до бібліотеки сценаріїв. Система дозволяє обирати типовий шаблон загрози для конкретного класу активу, після чого сформувати індивідуальну оцінку сценарію з урахуванням ARO, SLE_ext, залишкового ризику та очікуваного економічного ефекту від контрзаходів.

Результати розрахунку подаються у декількох формах. Перша форма - реєстр активів і картка окремого активу, де містяться паспортні параметри, критерії цінності та доказова база. Друга - бібліотека сценаріїв і таблиця оцінок сценаріїв із SLE_ext, ALE, ALE_res та E_net. Третя - аналітичний звіт, у якому активи, сценарії та контрзаходи ранжуються за критичністю, небезпечністю та середнім ефектом.

Модуль підтримує експорт табличних звітів у формат CSV, формує аналітичну панель для технічного та управлінського рівнів і веде журнал аудиту всіх суттєвих змін. Це дає змогу використовувати результати не лише в межах системи, а й у внутрішній документації підприємства та під час аналізу впровадження контрзаходів.

Отже, продумана логіка користувацької взаємодії є важливим елементом розробки. Вона забезпечує застосовність методу без надмірного ускладнення, зменшує кількість помилок введення, підвищує якість інтерпретації результатів і підсилює управлінську цінність системи. Іншими словами, програмний модуль не просто «рахує», а супроводжує користувача через стандартизований цикл оцінювання.

3.5 Апробація розробленого рішення, порівняльна оцінка та умови впровадження

Для перевірки практичної придатності розробленого методу в дипломній роботі виконано його апробацію на матеріалах базового підприємства. Оскільки у

звіті з практики вже було виділено сімнадцять інформаційних активів і шість критичних, апробацію сфокусовано на найбільш значущому з них - сервері виробничої бази даних.

На першому етапі апробації у модулі сформовано три демонстраційні активи: сервер виробничої БД, технологічну документацію та базу даних специфікацій і рецептур. Для кожного активу було заповнено паспорт із власниками, залежностями, критеріями C, I, A, B, R, L та доказовими примітками.

На другому етапі модуль виконав автоматичний розрахунок інтегральної цінності активів і монетарної бази AV_base. Для сервера виробничої БД отримано K_val = 3.00 та AV_base = 1 180 000 грн, для технологічної документації - K_val = 2.67 та AV_base = 540 000 грн, а для бази даних специфікацій і рецептур - K_val = 3.00 та AV_base = 972 999,82 грн.

На третьому етапі сформовано два сценарії оцінювання: ransomware для сервера виробничої БД та несанкціоновану зміну рецептур або специфікацій для бази даних специфікацій і рецептур. Модуль автоматично обчислив SLE_ext, ALE, ALE_res та E_net для кожного сценарію.

Для сценарію ransomware модуль визначив SLE_ext = 969 600 грн, ALE = 269 549 грн, ALE_res = 88 409 грн та чистий річний ефект E_net ≈ 89 140 грн. Для сценарію несанкціонованої зміни рецептур або специфікацій отримано SLE_ext = 550 000 грн, ALE = 110 000 грн, ALE_res = 54 450 грн та E_net = 37 550 грн.

На наступному етапі уведено у модуль типові контрзаходи: MFA для привілейованих облікових записів, сегментацію мережі, тестоване резервне копіювання та SIEM із журналюванням. Для кожного заходу було задано CE_freq, CE_imp, TCO, відповідальну роль і орієнтовний термін реалізації.

Порівняння з первинною реалізацією є показовим. На відміну від спрощеної моделі, новий модуль відображає не лише базові втрати, а й залишковий ризик, аудиторський слід змін і ефективність альтернативних контрзаходів, що робить результати придатними до управлінського обґрунтування.

Узагальнюючи результати апробації, встановлено, що розроблений метод і програмний модуль забезпечують відтворюване ранжування активів, предметне

оцінювання сценаріїв, порівняння захисних заходів та фіксацію історії змін у журналі аудиту. Саме це підтверджує практичну придатність розробленого рішення.

Узагальнені результати для цього етапу наведено в табл. 3.8.

Таблиця 3.8 – Приклад розрахунку для сервера виробничої бази даних

Етап	Показник	Значення	Коментар
Оцінка цінності	K_val	3.00 бала	Актив належить до критичних за шкалою 0–3
Грошова база	AV_base	1 180 000 грн	Сумарна базова цінність активу
Сценарний вплив	EF_s	0.72	Ransomware з високим впливом на доступність і цілісність
Разова втрата	SLE_ext	969 600 грн	З урахуванням додаткових витрат реагування
Річна частота	ARO_base	0.278	Агрегована оцінка з трьох джерел
Річні втрати	ALE_base	269 549 грн	Базовий стан до впровадження заходів
Після контролів	ALE_res	88 409 грн	Залишковий ризик після пакета заходів
Економічний ефект	E_net	≈ 89 140 грн/рік	Чистий річний ефект після врахування ТСО

Візуалізацію відповідного елемента подано на рис. 3.8.

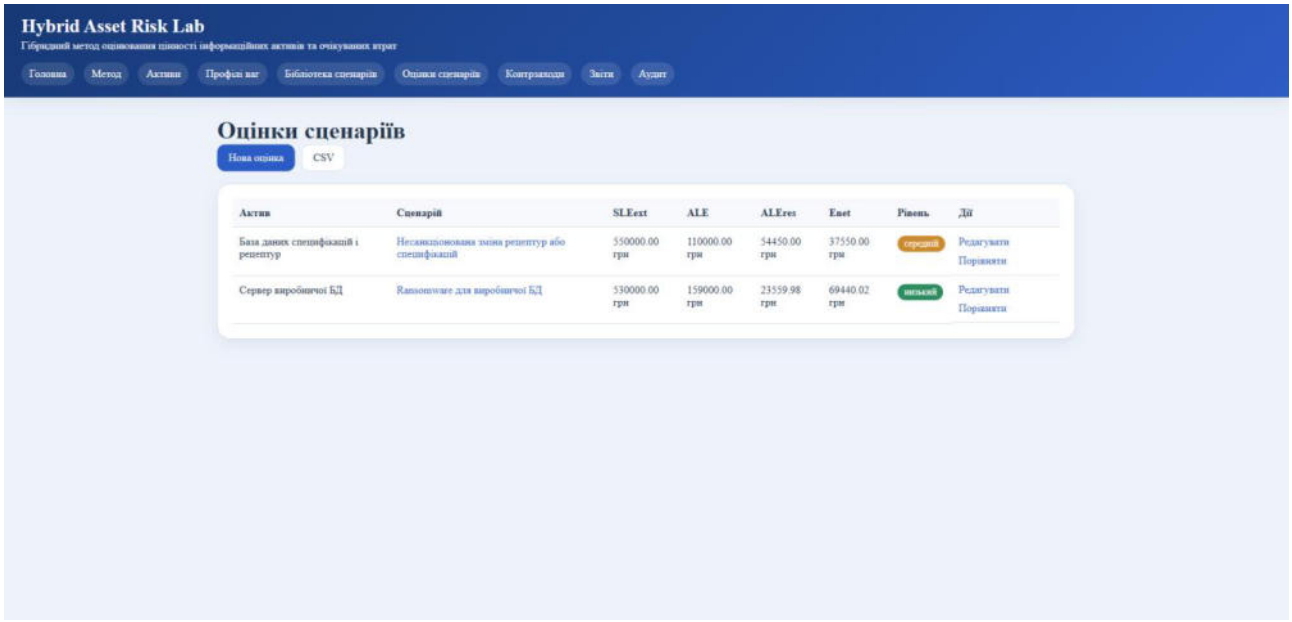

Рис 3.8 - Таблиця оцінок сценаріїв із показниками SLEext, ALE, ALEres та Enet.

Візуалізацію відповідного елемента подано на рис. 3.9.

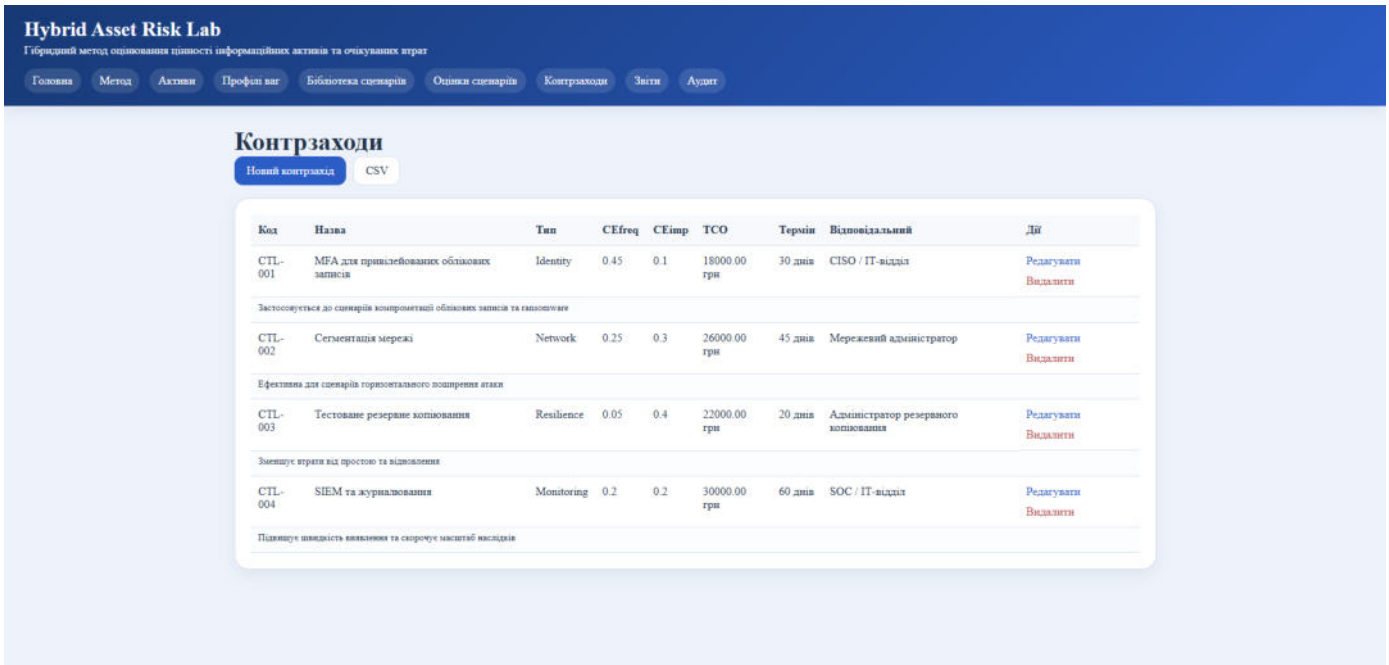

Рис 3.9 - Каталог контрзаходів із параметрами CEfreq, CEimp і TCO.

Візуалізацію відповідного елемента подано на рис. 3.10.

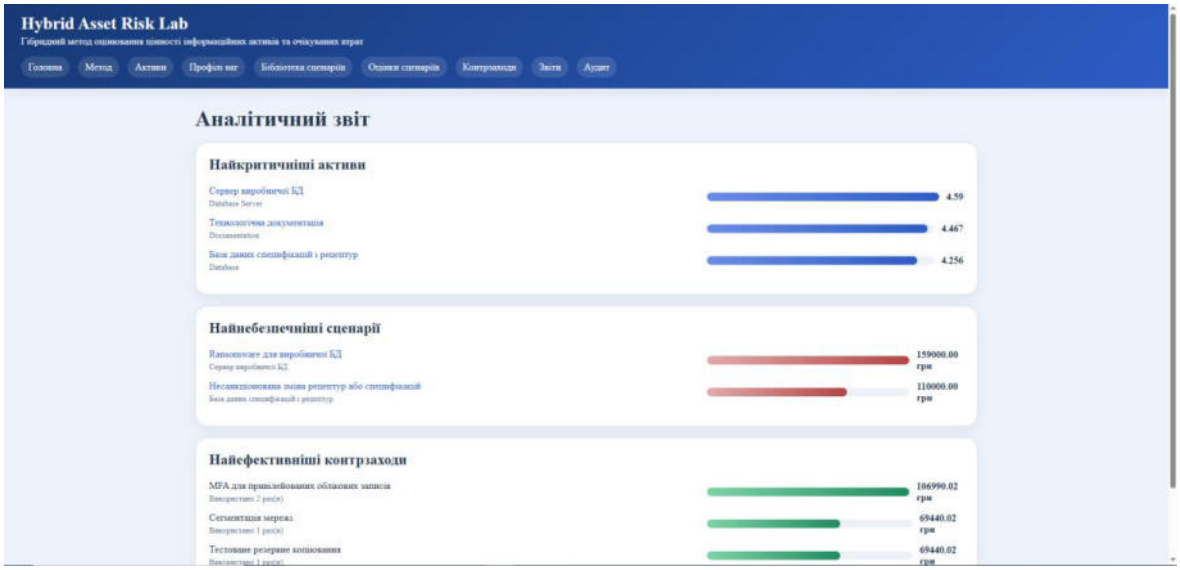

Рис 3.10 - Аналітичний звіт: ранжування активів, сценаріїв і контрзаходів.

3.5.1 Порівняльна оцінка розробленого рішення та умови його впровадження

Після апробації виконується порівняльна оцінка розробленого рішення відносно існуючої реалізації, яку розглянуто у другому розділі. Таке порівняння дозволяє не лише продемонструвати новизну рішення, а й показати, які саме проблеми воно усуває. За критерієм моделі активу рішення переходить від плоского переліку до структурованого паспорта з залежностями, відповідальними особами та доказовими джерелами. За критерієм оцінки цінності активу воно переходить від рівновагового CIA-середнього до багатокритеріальної моделі з вагами й коефіцієнтами достовірності.

За критерієм моделі загроз розроблене рішення замінює перелік загроз бібліотекою сценаріїв, що має істотне значення для пояснюваності та автоматизації. За критерієм кількісного оцінювання збитків воно переходить від вузького SLE/ALE до розширеного розрахунку, у якому враховуються базова цінність активу, додаткові витрати реагування і залишковий ризик.

Важливо підкреслити, що переваги розробленого рішення не є безумовними поза контекстом організації. Метод потребує більшої дисципліни збору даних,

чіткого визначення ролей і початкового наповнення бібліотеки сценаріїв. Це означає, що впровадження повинно здійснюватися поетапно. На першому етапі пропонується обмежитися критичними активами, на другому - розширити перелік сценаріїв, а на третьому - інтегрувати модуль із системами інвентаризації, журналювання та резервного копіювання.

Умовою успішного впровадження є також організаційна підтримка керівництва. Якщо результати оцінювання не використовуються під час планування бюджету, пріоритезації проєктів чи перевірки обґрунтованості витрат на безпеку, навіть найкраща методика швидко перетворюється на формальність. Тому у межах впровадження слід визначити власника процесу, періодичність перегляду, правила затвердження ваг, перелік обов’язкових доказів і формат управлінських звітів.

Окремо варто зазначити, що розроблене рішення має потенціал подальшого розвитку: підтримку ролей доступу, розширення бібліотеки сценаріїв, додавання нових профілів ваг і впровадження автоматизованого експорту аналітичних карток активів у формати DOCX та PDF.

Таким чином, порівняльна оцінка підтверджує, що розроблене рішення усуває головні методичні, організаційні та технічні недоліки, виявлені в другому розділі. Воно робить оцінювання більш предметним, прозорим, економічно інтерпретованим і придатним до автоматизації. Саме ці характеристики визначають його практичну цінність для підприємства та науково-прикладну цінність для дипломної роботи.

Узагальнені результати для цього етапу наведено в табл. 3.9

Таблиця 3.9 – Порівняння існуючої реалізації та розробленого рішення

Критерій	Існуюча реалізація	Розроблене рішення
Модель активу	Плоский перелік активів	Паспорт активу із залежностями та доказами
Цінність активу	Середнє CIA	Багатокритеріальна модель C, I, A, B, R, L
Достовірність даних	Не фіксується окремо	Коефіцієнти q_i і джерела доказів
Модель загроз	Список загроз	Бібліотека сценаріїв
Розрахунок втрат	Базовий SLE/ALE	Розширений SLE_ext і інтервали ALE
Оцінка контролів	Здебільшого через ARO	CE_freq, CE_imp, TCO, E_net, ALE_res
Інструментальна база	Табличний облік	Програмний модуль з журналом змін
Пояснюваність	Часткова	Повна декомпозиція результатів

Візуалізацію відповідного елемента подано на рис. 3.11.

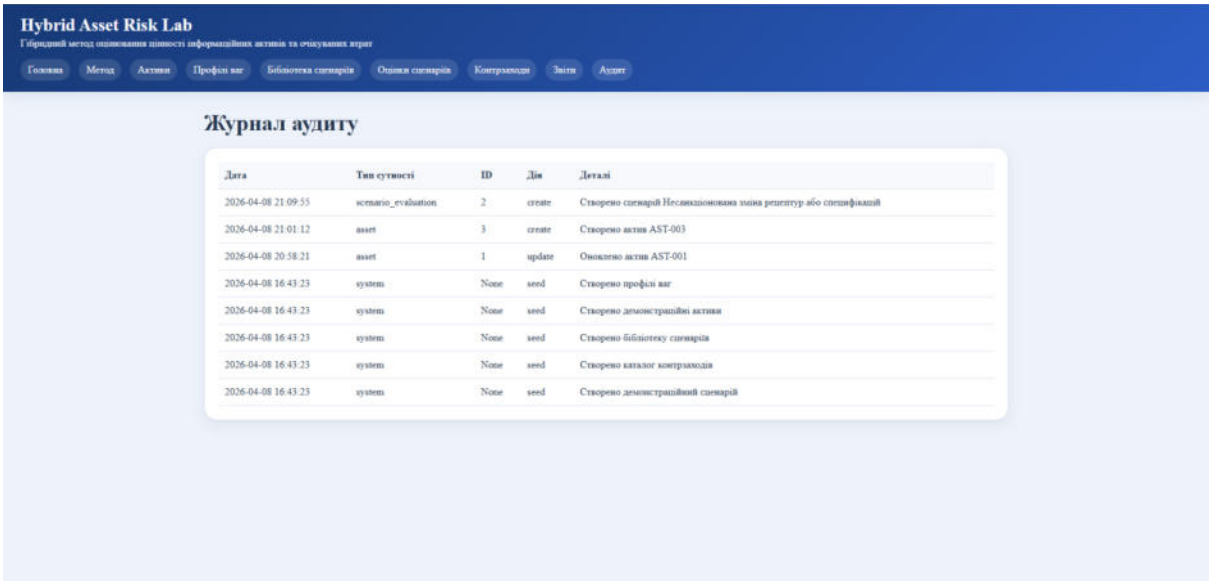

Рис 3.11 - Журнал аудиту змін і дій користувача.

3.6 Додаткові діаграми розробленого рішення

Для повнішого подання практичної частини роботи додано три діаграми: алгоритм оцінювання, перехід від грошової оцінки до бальної шкали та Діаграму класів програмного модуля. Вони узагальнюють логіку, описану у підрозділах 3.2–3.4, і наведені на рис. 3.12–3.14.

Опис: Наведено схему оцінювання активу, очікуваних втрат і контрзаходів. Алгоритм починається з формування вхідних даних: паспорта активу, критеріїв C, I, A, B, R, L, вагових коефіцієнтів, фінансових параметрів, бібліотеки сценаріїв загроз і переліку контрзаходів. Після цього створюється або актуалізується паспорт активу та перевіряється повнота внесених даних. Якщо дані є неповними або суперечливими, вони уточнюються.

Далі виконується оцінювання цінності активу, розраховується інтегральний показник K_val і базова грошова цінність AV_base. Після вибору релевантного сценарію загрози визначаються частота його реалізації, очікувані втрати та рівень ризику. На завершальному етапі для кожного контрзаходу розраховується залишковий ризик, чистий економічний ефект і строк окупності. За результатами порівняння альтернатив формується підсумкова рекомендація щодо пріоритетного контрзаходу та звіт для прийняття управлінського рішення.

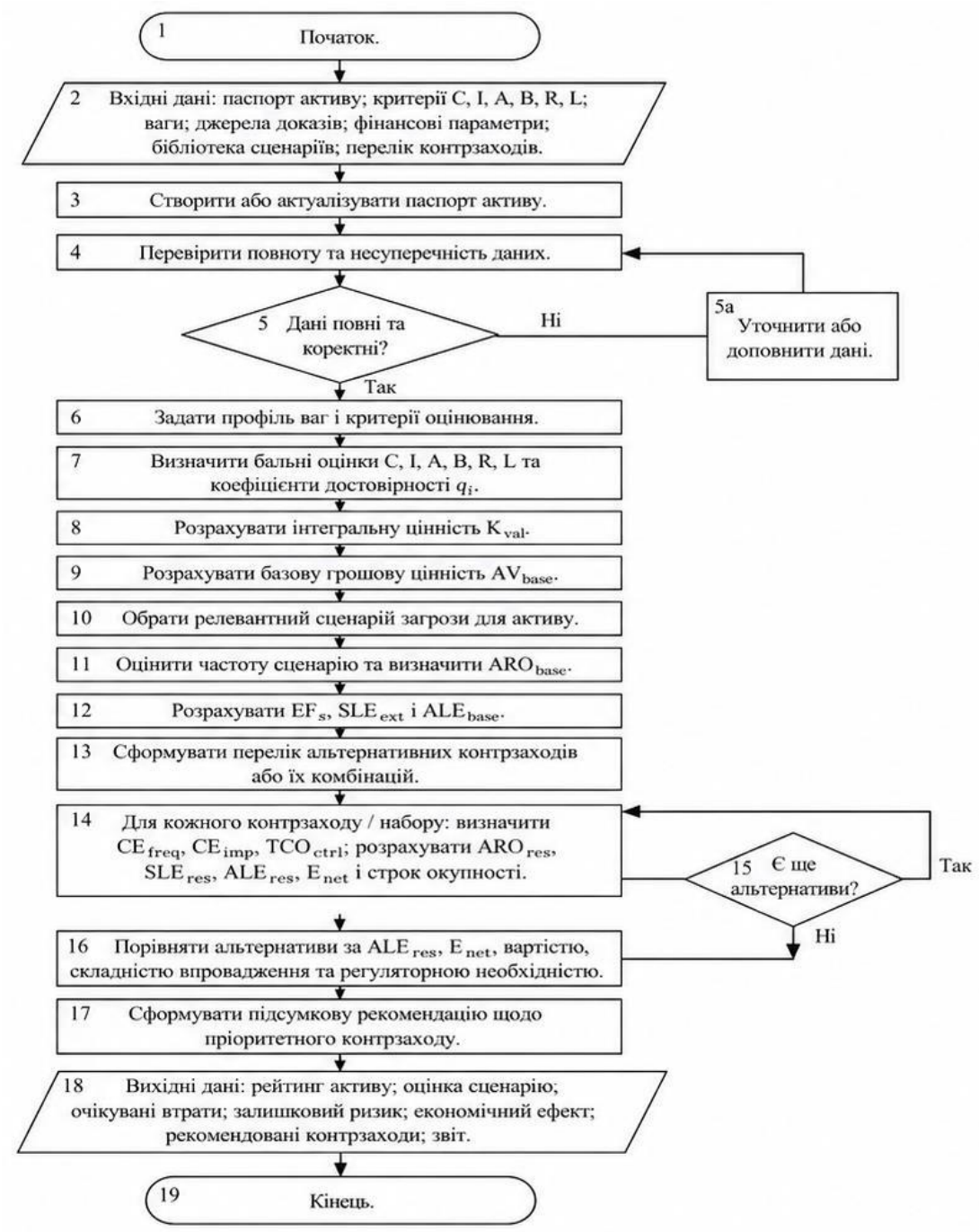

Рис 3.12 – Схема алгоритму оцінювання активу, втрат і контрзаходів.

Опис: Для забезпечення узгодженості між грошовою та бальною складовими оцінювання в роботі використовується алгоритм переходу від базової грошової оцінки активу до бальної шкали. Необхідність такого переходу пояснюється тим, що фінансовий показник AV_base сам по собі є зручним для економічного обґрунтування, однак його складно безпосередньо поєднувати з експертними

критеріями C, I, A, B, R, L, які оцінюються у балах. Тому грошова оцінка додатково переводиться у шкалу 0–3, де 0 відповідає незначній фінансовій цінності, а 3 — критичній фінансовій значущості активу.

Алгоритм, наведений на рис. 3.13, починається з отримання вхідних даних: значення AV_base, шкали порогових значень T1, T2, T3 та правил підприємства щодо інтервалів оцінювання. На першому етапі грошова оцінка активу нормується для подальшого порівняння з установленими порогами. Далі виконується послідовна перевірка значення AV_base. Якщо AV_base менше за перший поріг T1, активу присвоюється 0 балів, що відповідає незначній фінансовій цінності. Якщо значення перевищує T1, але є меншим за T2, актив отримує 1 бал і належить до групи помірної фінансової значущості. Якщо AV_base перебуває між T2 і T3, активу присвоюється 2 бали, що свідчить про високу фінансову цінність. У випадку, коли AV_base дорівнює або перевищує T3, актив отримує 3 бали та класифікується як критично значущий.

Після визначення відповідного рівня отримана бальна оцінка S_money фіксується у паспорті активу. Надалі вона передається до інтегрального розрахунку цінності активу та використовується разом з іншими критеріями оцінювання. Такий підхід дозволяє поєднати економічний вимір ризику з багатокритеріальною експертною моделлю, а також уникнути ситуації, коли актив із високою реальною вартістю недооцінюється через недостатню деталізацію якісних показників.

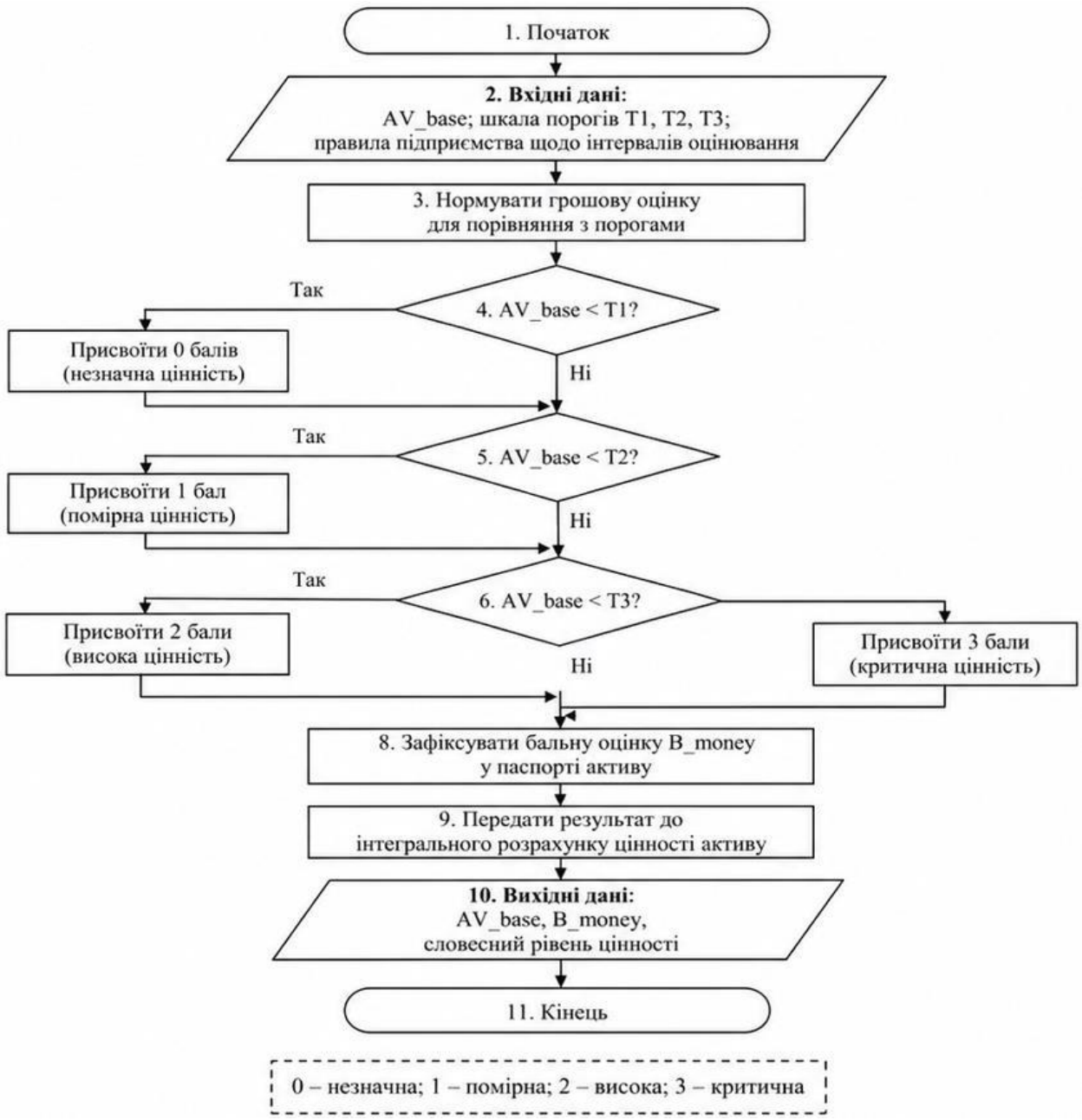

Рис 3.13 – Діаграма переходу від грошової оцінки активу до бальної шкали

Рисунок 3.14 – Діаграма класів програмного модуля підтримки оцінювання

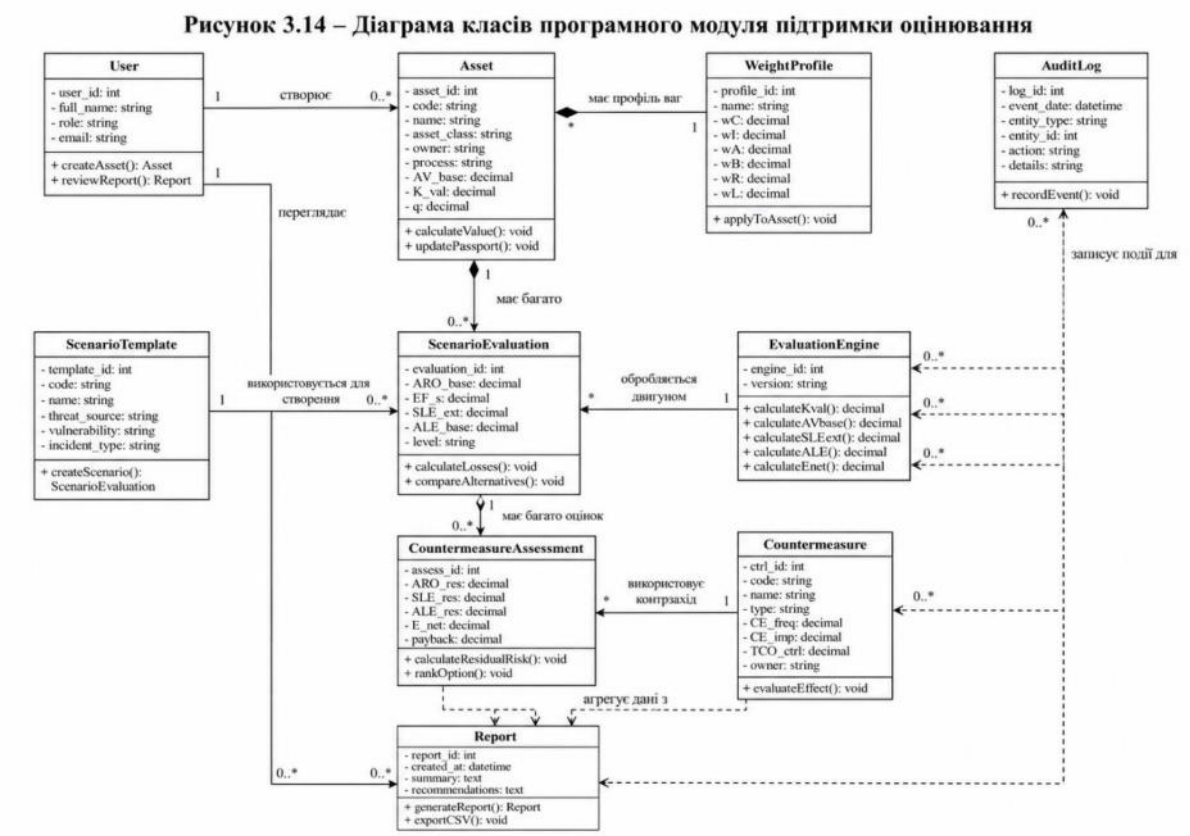

Рис 3.14 – Діаграма класів програмного модуля підтримки оцінювання

Висновки до розділу 3

У роботі реалізовано підхід до оцінювання цінності інформаційних активів та очікуваних втрат при реалізації загроз. На відміну від існуючої реалізації, це рішення поєднує багатокритеріальну оцінку цінності активу, сценарний підхід до загроз, розширений розрахунок втрат, оцінювання контрзаходів і концепцію програмної підтримки процесу.

У роботі запропоновано формалізований паспорт активу, що містить ідентифікаційні, функціональні, технічні, фінансові та доказові характеристики. Для підтвердження практичності методики додано приклад заповненого паспорта активу, на основі якого виконується перехід від якісної оцінки до грошової моделі та бальної шкали 0–3.

Спроєктовано концепцію програмного модуля підтримки оцінювання, яка охоплює архітектуру підсистем, рольову модель доступу, інформаційну модель

даних, логіку роботи користувача, форми звітності та класову модель. Додані діаграми алгоритму, переходу від грошової оцінки до бальної шкали та класів підтверджують, що розробка має не лише теоретичний, а й проєктно-прикладний характер.

Під час апробації на прикладі сервера виробничої бази даних встановлено, що метод дозволяє отримувати більш повну і пояснювану оцінку ризику, ніж спрощений підхід, який використовувався раніше. Отриманий результат підтверджує практичну цінність розробленого рішення як інструмента підтримки рішень у сфері захисту інформаційних активів.

Загальні висновки

У кваліфікаційній роботі було розглянуто задачу оцінювання цінності інформаційних активів у системі управління ризиками компанії малого та середнього бізнесу. У ході дослідження встановлено, що інформаційні активи є важливим ресурсом підприємства, оскільки від їхньої конфіденційності, цілісності та доступності залежить стабільність бізнес-процесів, безперервність роботи інформаційної інфраструктури, якість управлінських рішень і рівень можливих фінансових втрат при реалізації загроз.

У першому розділі було проаналізовано предметну область, визначено місце інформаційних активів у діяльності підприємства та розглянуто основні поняття дослідження: цінність активу, загроза, вразливість, ризик і очікувані втрати. Також було досліджено існуючі підходи до оцінювання активів і ризиків, зокрема якісні, кількісні, сценарні та гібридні методи. У результаті встановлено, що для практичного використання найбільш доцільним є саме гібридний підхід, який поєднує бальну оцінку критичності активу з грошовим розрахунком очікуваних втрат.

У другому розділі було проаналізовано існуючу реалізацію процесу оцінювання цінності інформаційних активів. Виявлено, що спрощене оцінювання не забезпечує достатньої прозорості, оскільки не завжди враховує повний паспорт

активу, вагу окремих критеріїв, сценарії реалізації загроз, частоту подій, залишковий ризик і економічну доцільність контрзаходів. На основі цього було обґрунтовано необхідність удосконалення підходу через формалізацію вхідних даних, використання шкали оцінювання, урахування вагових коефіцієнтів і перехід від грошової оцінки до бальної шкали.

У третьому розділі було розроблено гібридний метод оцінювання цінності інформаційних активів і очікуваних втрат при реалізації загроз. Запропонований метод передбачає формування паспорта активу, оцінювання критеріїв C, I, A, B, R, L, використання вагових коефіцієнтів, розрахунок інтегральної цінності активу, визначення базової грошової оцінки, оцінювання сценаріїв загроз, розрахунок SLE, ALE, залишкового ризику та економічного ефекту від упровадження контрзаходів. Така логіка дозволяє не лише визначити рівень ризику, а й обґрунтувати вибір захисних заходів з позиції їх практичної та економічної доцільності.

Практичним результатом роботи стала реалізація програмного модуля підтримки оцінювання, який дає змогу вести реєстр інформаційних активів, формувати бібліотеку сценаріїв загроз, виконувати оцінювання ризикових сценаріїв, порівнювати контрзаходи та формувати аналітичні результати для прийняття управлінських рішень. Апробація розробленого рішення показала, що запропонований підхід є більш повним і обґрунтованим порівняно зі спрощеною реалізацією, оскільки враховує як технічні характеристики активів, так і фінансові наслідки можливих інцидентів.

Отже, мету кваліфікаційної роботи досягнуто. У роботі розроблено та обґрунтовано підхід до оцінювання цінності інформаційних активів у системі управління ризиками компанії малого та середнього бізнесу, який може бути використаний для підвищення якості інвентаризації активів, пріоритезації ризиків, вибору контрзаходів і підготовки управлінських рішень щодо захисту інформаційної інфраструктури підприємства. Запропонований метод і програмний модуль можуть бути адаптовані для подальшого використання в організаціях зі схожою структурою інформаційних активів та потребою в економічно обґрунтованому управлінні ризиками інформаційної безпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection - Information security management systems - Requirements, Geneva: International Organization for Standardization, 2022. [с. 15-17, 24-29, 46-50, 52-54].

2. ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection - Information security controls, Geneva: International Organization for Standardization, 2022. [с. 40-43, 45-50, 76-84].

3. ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection - Guidance on managing information security risks, Geneva: International Organization for Standardization, 2022. [с. 15-20, 24-29, 52-69, 90-94].

4. ISO 31000:2018. Risk management - Guidelines, Geneva: International Organization for Standardization, 2018. [с. 24-29, 46-50, 52-54].

5. ISO/IEC 27035-1:2023. Information technology - Information security incident management - Part 1: Principles and process, Geneva: International Organization for Standardization, 2023. [с. 21-24, 36-39, 69-76].

6. R. Ross, M. McEvilley, J. Oren, Guide for Conducting Risk Assessments, NIST Special Publication 800-30 Revision 1, Gaithersburg: National Institute of Standards and Technology, 2012. [с. 15-21, 24-29, 52-69].

7. The Open Group, Open FAIR Body of Knowledge, Reading: The Open Group, 2021. [с. 18-21, 24-29, 39-43, 69-76].

8. OWASP Foundation. OWASP Risk Rating Methodology [Електронний ресурс].URL: https://owasp.org/www-community/OWASP_Risk_Rating_Methodology . (дата звернення: 05.05.2026)

9. T. R. Peltier, Information Security Risk Analysis, 3rd ed., Boca Raton: CRC Press, 2010. [с. 18-21, 24-29, 39-43].

10. M. E. Whitman, H. J. Mattord, Principles of Information Security, 7th ed., Boston: Cengage Learning, 2021. [с. 9-17, 21-24].

11. R. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, 3rd ed., Hoboken: Wiley, 2020. [с. 12-17, 21-24, 36-39, 76-84].

12. M. Bishop, Computer Security: Art and Science, 2nd ed., Boston: Addison-Wesley Professional, 2018. [с. 14-17, 21-24, 36-39].

13. J. R. Vacca, Computer and Information Security Handbook, 3rd ed., Cambridge: Morgan Kaufmann, 2017. [с. 9-17, 21-24, 36-43].

14. V. I. Pashorin, Bezpeka informatsiinykh system: navchalnyi posibnyk, Lviv: Magnolia, 2024. [с. 9-17, 21-24, 36-43].

15. В. Л. Бурячок, Р. В. Киричок, П. М. Складанний, Основи інформаційної та кібернетичної безпеки: навчальний посібник, Київ, 2018, 320 с. [с. 9-17, 21-24, 36-39].

16. В. В. Остроухов, М. М. Присяжнюк, О. І. Фармагей та ін., Інформаційна безпека: підручник, Київ: Видавництво Ліра, 2021, 412 с. [с. 9-17, 21-24, 30-36].

17. О. Г. Корченко, М. Є. Шелест, С. В. Казмірчук, Ю. М. Ткач, Є. В. Іванченко, Менеджмент інформаційної безпеки: навчальний посібник, Ніжин: ФОП Лук'яненко В. В., ТПК "Орхідея", 2019, 408 с. [с. 15-17, 24-29, 43-50].

18. С. О. Носок, О. М. Фаль, В. М. Ткач, Управління інформаційною безпекою. Конспект лекцій: навчальний посібник для студентів спеціальності 125 "Кібербезпека", Київ: КПІ ім. Ігоря Сікорського, 2021, 258 с. [с. 15-17, 24-29, 43-50].

19. С. О. Носок, М. В. Коломицев, І. В. Стьопочкіна, Управління інформаційною безпекою: навчальний посібник, Київ: КПІ ім. Ігоря Сікорського, 2025, 88 с. [с. 24-29, 43-50, 90-94].

20. А. М. Гребенюк, Організація управління інформаційною безпекою: навчальний посібник, Дніпро: Дніпропетровський державний університет внутрішніх справ, 2020. [с. 15-17, 24-29, 43-50].

21. Інформаційна безпека: навчальний посібник, Київ: КНЕУ, 2008, 280 с. [с.17-24].

22. Закон України “Про основні засади забезпечення кібербезпеки України” від 05.10.2017 № 2163-VIII, Відомості Верховної Ради України, 2017. [с. 21-29].

23. CERT-UA, Рекомендації щодо реагування на кіберінциденти та підвищення рівня кіберзахисту інформаційних систем, Київ: Урядова команда реагування на комп’ютерні надзвичайні події України, 2024. [с. 18-24, 36-39, 69-76].

24. ISACA, COBIT 2019 Framework: Governance and Management Objectives, Rolling Meadows: ISACA, 2018. [с. 24-29, 43-50, 84-90].

25. ENISA, Cybersecurity Risk Management: Guidelines and Good Practices, Athens: European Union Agency for Cybersecurity, 2022. [с. 24-29, 46-50, 52-69].

Додаток - 1

Зведена таблиця головних формул

Номер	Формула	Призначення
(1.1)	K_CIA = max(C, I, A)	Первинна критичність активу за правилом максимального впливу CIA.
(1.2)	SLE = AV · EF; ALE = SLE · ARO	Базова модель разових та річних очікуваних втрат.
(2.1)	SLE_ext = L_dir + L_down + L_rec + L_for + L_contr + L_rep	Розширення структури разових втрат у межах критики поточної реалізації.
(2.2)	E_net = (ALE_before - ALE_after) - TCO_ctrl	Попередня логіка оцінювання чистого ефекту контрзаходу.
(3.1)	K_val = max(max(C, I, A), K_w, S_money)	Підсумкова цінність активу з урахуванням CIA, ваг критеріїв і грошової складової.
(3.2)	K_w = (Σ(w_i · s_i · q_i)) / (Σ w_i)	Зважена оцінка критеріїв з урахуванням достовірності даних.
(3.3)	AV_base = C_rep + C_res + C_data + C_proc + C_leg	Формування базової грошової цінності активу.
(3.4)	S_money = f(AV_base) за порогами 0/1/2/3	Переведення грошової оцінки активу у бальну шкалу.
(3.5)	EF_s = λ1·D_conf + λ2·D_int + λ3·D_avail + λ4·D_chain	Коефіцієнт сценарного впливу загрози.
(3.6)	ARO_base = (μ1·f_hist + μ2·f_ext + μ3·f_exp)·M_exposure·M_control	Агрегована оцінка частоти реалізації сценарію.
(3.7)	SLE_ext = AV_base·EF_s + L_resp + L_for + L_rec + L_contr + L_rep	Розширений показник разової втрати за сценарієм.
(3.8)	ARO_res = ARO_base·(1-CE_freq); SLE_res = SLE_ext·(1-CE_imp)	Оцінювання залишкових частоти та разової втрати після контролів.
(3.9)	ALE_res = ARO_res · SLE_res	Залишкові річні очікувані втрати після контрзаходів.

(3.10)	E_net = (ALE_before - ALE_res) - TCO_ctrl	Чистий річний економічний ефект від впровадження контрзаходів.

Додаток - 2

Посилання на Таблиці

Номер табл.	**Назва (заголовок)**	**Розділ**	**Посилання в тексті (приклад)**
Таблиця 1.1	Узагальнена класифікація інформаційних активів	1	Перелік понять наведено в табл. 1.1.
Таблиця 1.2	Порівняння підходів до оцінювання цінності активів	1	...наведено в табл. 1.2.
Таблиця 1.3	Порівняння підходів до оцінювання очікуваних втрат	1	...наведено в табл. 1.3.
Таблиця 1.4	Узагальнення основних загроз інформаційним системам	1	...наведено в табл. 1.4.
Таблиця 1.5	Формалізація елементів постановки дослідження	1	...наведено в табл. 1.5.
Таблиця 1.6	Основні вимоги до методики оцінювання	1	...наведено в табл. 1.6.
Таблиця 2.1	Узагальнення етапів існуючої реалізації	2	...наведено в табл. 2.1.
Таблиця 2.2	Порівняння поточної та оптимізованої моделі	2	...наведено в табл. 2.2.
Таблиця 2.3	Недоліки поточного кількісного блоку оцінювання	2	...наведено в табл. 2.3.
Таблиця 2.4	Основні напрями оптимізації існуючої реалізації	2	...наведено в табл. 2.4.

Номер табл.	**Назва (заголовок)**	**Розділ**	**Посилання в тексті (приклад)**
Таблиця 2.5	Вимоги до удосконаленої реалізації оцінювання	2	...наведено в табл. 2.5.
Таблиця 3.1	Принципи побудови розробленого методу	3	...наведено в табл. 3.1.
Таблиця 3.2	Структура паспорта інформаційного активу	3	...наведено в табл. 3.2.
Таблиця 3.2а	Приклад заповненого паспорта активу	3	У табл. 3.2а показано приклад...
Таблиця 3.2б	Універсальна шкала оцінювання критеріїв 0-3	3	Шкалу рівнів наведено в табл. 3.2б.
Таблиця 3.3	Критерії оцінювання цінності активу	3	...наведено в табл. 3.3.
Таблиця 3.3а	Переведення грошової оцінки у бальну шкалу	3	...наведено в табл. 3.3а.
Таблиця 3.4	Фрагмент бібліотеки сценаріїв загроз	3	...наведено в табл. 3.4.
Таблиця 3.5	Параметри оцінювання контрзаходів	3	...наведено в табл. 3.5.
Таблиця 3.6	Основні підсистеми програмного модуля	3	...наведено в табл. 3.6.
Таблиця 3.7	Основні сутності інформаційної моделі	3	...наведено в табл. 3.7.
Таблиця 3.8	Приклад розрахунку для сервера БД	3	...наведено в табл. 3.8.
Таблиця 3.9	Порівняння існуючої реалізації та розробки	3	...наведено в табл. 3.9.
Таблиця 3.10	Зведена таблиця головних формул	3	Головні-формули узагальнено в табл. 3.10.

Додаток - 3

Основні фрагменти програмного коду

У додатку наведено основні фрагменти програмного коду модуля Hybrid Asset Risk. Програмний модуль реалізовано мовою Python із використанням FastAPI, SQLite, Jinja2 Templates та клієнтської частини на базі HTML/CSS. Наведені фрагменти демонструють ключову логіку роботи системи: підключення застосунку, роботу з базою даних, розрахунок цінності активів, очікуваних втрат, залишкового ризику, ефективності контрзаходів і запуск вебсерверу.

Фрагмент 1. Ініціалізація FastAPI-застосунку та підключення SQLite

```
from pathlib import Path
import sqlite3
from contextlib import closing
from datetime import datetime

from fastapi import FastAPI, Form, HTTPException, Query, Request
from fastapi.responses import HTMLResponse, RedirectResponse, StreamingResponse
from fastapi.staticfiles import StaticFiles
from fastapi.templating import Jinja2Templates
import uvicorn

BASE_DIR = Path(__file__).resolve().parent
DB_PATH = BASE_DIR / "risklab.db"
TEMPLATES_DIR = BASE_DIR / "templates"
STATIC_DIR = BASE_DIR / "static"

app = FastAPI(title="Hybrid Asset Risk Lab")
app.mount("/static", StaticFiles(directory=str(STATIC_DIR)), name="static")
templates = Jinja2Templates(directory=str(TEMPLATES_DIR))


def now_str() -> str:
    return datetime.now().strftime("%Y-%m-%d %H:%M:%S")


def get_db() -> sqlite3.Connection:
    conn = sqlite3.connect(DB_PATH)
    conn.row_factory = sqlite3.Row
    conn.execute("PRAGMA foreign_keys = ON")
    return conn


def fetch_all(query: str, params: tuple = []):
    with closing(get_db()) as conn:
        return list(conn.execute(query, params).fetchall())
```

```
def fetch_one(query: str, params: tuple = []):
    with closing(get_db()) as conn:
        return conn.execute(query, params).fetchone()
```

Фрагмент демонструє створення вебзастосунку, підключення статичних файлів, HTML-шаблонів і бази даних SQLite. Функції fetch_all та fetch_one використовуються для отримання даних із бази.

Фрагмент 2. Критерії оцінювання інформаційного активу

```
CRITERIA = [
    ("c", "Конфіденційність", "wc", "confidentiality_note"),
    ("i", "Цілісність", "wi", "integrity_note"),
    ("a", "Доступність", "wa", "availability_note"),
    ("b", "Бізнесова значущість", "wb", "business_note"),
    ("r", "Відновлюваність", "wr", "recovery_note"),
    ("l", "Правові та репутаційні наслідВідновлюваність", "wr", "recovery_note"),
    ("l", "Правові та репутаційні наслідки", "wl", "legal_note"),
]
```

У модулі актив оцінюється за критеріями C, I, A, B, R, L. Це дозволяє враховувати не лише класичну тріаду конфіденційності, цілісності та доступності, а й бізнесову роль активу, складність відновлення та можливі юридичні наслідки.

Фрагмент 3. Розрахунок інтегральної та грошової цінності активу

```
def weighted_value(asset) -> float:
    denom = sum(float(asset[w] or 0) for _, _, w, _ in CRITERIA)
    if denom == 0:
        return 0.0

    score = sum(
        float(asset[c] or 0) * float(asset[w] or 0)
        for c, _, w, _ in CRITERIA
    ) / denom

    return round(score, 3)


def asset_base_monetary_value(asset) -> float:
    replacement = float(asset["replacement_cost"] or 0)

    downtime = (
        float(asset["downtime_cost_per_hour"] or 0)
        * float(asset["allowed_downtime_hours"] or 0)
    )

    business_bonus = 4500 * float(asset.get("b", 0) or 0)
    legal_bonus = 3500 * float(asset.get("l", 0) or 0)
    recovery_bonus = 2500 * float(asset.get("r", 0) or 0)
```

```
    return round(
        replacement + downtime + business_bonus + legal_bonus + recovery_bonus,
        2
    )
```

Функція weighted_value розраховує інтегральну цінність активу з урахуванням ваг критеріїв. Функція asset_base_monetary_value формує базову грошову оцінку активу з урахуванням вартості заміщення, простою, бізнесової значущості, правових наслідків і складності відновлення.

Фрагмент 4. Розрахунок очікуваних втрат SLE та ALE

```
def scenario_sle(row) -> float:
    return round(
        sum(
            float(row.get(k, 0) or 0)
            for k in [
                "l_dir",
                "l_down",
                "l_rec",
                "l_for",
                "l_contr",
                "l_rep",
            ]
        ),
        2
    )


def scenario_ale(row) -> float:
    return round(
        scenario_sle(row) * float(row.get("aro", 0) or 0),
        2
    )
```

Функція scenario_sle розраховує розширену разову очікувану втрату, яка включає прямі втрати, простій, відновлення, форензичні роботи, договірні та репутаційні наслідки. Функція scenario_ale визначає річні очікувані втрати з урахуванням частоти реалізації сценарію ARO.

Фрагмент 5. Розрахунок залишкового ризику та економічного ефекту контрзаходів

```
def combine_control_effects(control_rows):
    if not control_rows:
        return 0.0, 0.0, 0.0

    remain_freq = 1.0
    remain_imp = 1.0
    total_tco = 0.0

    for row in control_rows:
        ce_freq = max(0.0, min(0.99, float(row["ce_freq"] or 0)))
```

```
        ce_imp = max(0.0, min(0.99, float(row["ce_imp"] or 0)))

        total_tco += float(row["tco_annual"] or 0)
        remain_freq *= (1 - ce_freq)
        remain_imp *= (1 - ce_imp)

    return round(1 - remain_freq, 3), round(1 - remain_imp, 3), round(total_tco, 2)


def residual_level(ale_res: float) -> str:
    if ale_res >= 150000:
        return "критичний"
    if ale_res >= 70000:
        return "високий"
    if ale_res >= 25000:
        return "середній"
    return "низький"


def scenario_residual_metrics(row, control_rows):
    sle = scenario_sle(row)
    ale = scenario_ale(row)

    combined_freq, combined_imp, total_tco = combine_control_effects(control_rows)

    aro_res = round(float(row.get("aro", 0) or 0) * (1 - combined_freq), 4)
    sle_res = round(sle * (1 - combined_imp), 2)
    ale_res = round(aro_res * sle_res, 2)
    e_net = round(ale - ale_res - total_tco, 2)

    return {
        "aro_res": aro_res,
        "sle_res": sle_res,
        "ale_res": ale_res,
        "e_net": e_net,
        "residual_level": residual_level(ale_res),
        "total_tco": total_tco,
    }
```

Цей фрагмент є центральним для оцінювання контрзаходів. Він показує, як контрзаходи зменшують частоту інциденту та масштаб наслідків, після чого розраховуються залишкові втрати ALE_res, рівень залишкового ризику та чистий економічний ефект E_net.

Фрагмент 6. Формування активу та сценарію з розрахунковими показниками

```
def asset_with_metrics(row):
    data = dict(row)
    data["k_opt"] = weighted_value(data)
    data["av_base"] = asset_base_monetary_value(data)
    return data
```

```
def scenario_with_metrics(row):
    data = dict(row)
    data["sle_ext"] = scenario_sle(data)
    data["ale"] = scenario_ale(data)

    controls = fetch_all(
        """
        SELECT c.* FROM controls c
        JOIN scenario_controls sc ON sc.control_id = c.id
        WHERE sc.evaluation_id = ?
        ORDER BY c.name
        """,
        (data["id"],),
    )

    data.update(scenario_residual_metrics(data, controls))
    data["controls"] = [dict(c) for c in controls]

    return data
```

Функція asset_with_metrics додає до активу інтегральну та грошову оцінку. Функція scenario_with_metrics доповнює сценарій розрахунками SLE, ALE, залишкового ризику, економічного ефекту та переліком пов’язаних контрзаходів.

Фрагмент 7. Приклади маршрутів для відображення активів, сценаріїв і звітів

```
@app.get("/assets", response_class=HTMLResponse)
def assets_list(request: Request, q: str = Query("")):
    q_like = f"%{q.strip()}%"

    rows = fetch_all(
        """
        SELECT * FROM assets
        WHERE name LIKE ? OR code LIKE ? OR business_process LIKE ?
        ORDER BY updated_at DESC
        """,
        (q_like, q_like, q_like),
    )

    assets = [asset_with_metrics(r) for r in rows]

    return templates.TemplateResponse(
        "assets.html",
        {"request": request, "page_title": "Активи", "assets": assets}
    )


@app.get("/scenarios", response_class=HTMLResponse)
def scenarios_list(request: Request):
    rows = fetch_all(
```

```
        """
        SELECT se.*, a.name AS asset_name
        FROM scenario_evaluations se
        JOIN assets a ON a.id = se.asset_id
        ORDER BY se.updated_at DESC
        """
    )

    scenarios = [scenario_with_metrics(r) for r in rows]

    return templates.TemplateResponse(
        "scenarios.html",
        {"request": request, "page_title": "Оцінки сценаріїв", "scenarios": scenarios}
    )


@app.get("/reports", response_class=HTMLResponse)
def reports(request: Request):
    assets = [
        asset_with_metrics(r)
        for r in fetch_all("SELECT * FROM assets ORDER BY name")
    ]

    scenarios = [
        scenario_with_metrics(r)
        for r in fetch_all(
            """
            SELECT se.*, a.name AS asset_name
            FROM scenario_evaluations se
            JOIN assets a ON a.id = se.asset_id
            ORDER BY se.updated_at DESC
            """
        )
    ]

    return templates.TemplateResponse(
        "reports.html",
        {
            "request": request,
            "page_title": "Аналітичний звіт",
            "assets": sorted(assets, key=lambda x: x["k_opt"], reverse=True),
            "scenarios": sorted(scenarios, key=lambda x: x["ale"], reverse=True),
        }
    )
```

У цьому фрагменті наведено приклади маршрутів FastAPI. Вони відповідають за відображення реєстру активів, списку оцінених сценаріїв і аналітичного звіту. Перед передачею даних у HTML-шаблони система автоматично додає розрахункові показники.