МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БУДІВНИЦТВА І АРХІТЕКТУРИ

ФАКУЛЬТЕТ АВТОМАТИЗАЦІЇ І ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА КІБЕРБЕЗПЕКИ І КОМПЮТЕРНОЇ ІНЖЕНЕРІЇ

# ДИПЛОМНА РОБОТА

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

Виконав студент 4-го курсу, групи БІКС-22

Лещенко Д.С.

Керівник к.т.н., доцент Ізмайлова О.В.

Київ 2026

# Актуальність теми

Чому оцінювання активів і втрат має практичну цінність

1. Залежність

Інформаційні системи напряму впливають на виробничі процеси, фінансову стійкість, облік, логістику та виконання зобов'язань.

2. Фрагментарність захисту

Без єдиної логіки оцінювання важко визначити, які активи є критичними і які загрози треба обробляти першочергово.

3. Економічне обґрунтування

Керівництву потрібна не лише технічна оцінка, а й відповідь: яких втрат дозволяє уникнути конкретний контрзахід.

Висновок слайду

Тема є прикладною: вона переводить ризик із загальних фраз у вимір активів, втрат і рішень.

# Проблема дослідження

Чому спрощеного оцінювання недостатньо

**Що не працює у спрощеній практиці**

Активи часто ведуться як простий перелік без власників, залежностей і меж відповідальності;
оцінки CIA без ваг згладжують різницю між типами активів;

**Ключовий розрив**

Між якісним описом активу і управлінським рішенням існує розрив: не завжди зрозуміло, як перейти від “актив важливий” до “цей контрзахід економічно доцільний”.

перелік — паспорт — сценарій — втрати — контрзахід — звіт

Розробка має усунути цей розрив: кожен актив отримує паспорт, загроза описується сценарієм, втрати рахуються у фінансовому вимірі, а контрзахід обирається за залишковим ризиком і економічним ефектом.

# Мета, об’єкт, предмет і завдання

Логіка побудови кваліфікаційної роботи

**Об’єкт**

Процес оцінювання цінності інформаційних активів та очікуваних втрат від реалізації загроз.

**Предмет**

Методи, моделі, критерії та засоби оцінювання критичності активів, ризиків і втрат.

**Мета**

Підвищити обґрунтованість рішень щодо захисту інформаційної інфраструктури підприємства.

**Основні завдання**

Проаналізувати предметну область, активи, загрози та підходи до оцінювання;

Розробити паспорт активу, шкалу 0–3, вагову та сценарну модель;

реалізувати програмний модуль та виконати апробацію.

аналіз — критика — модель — алгоритм — модуль — апробація

# Предметна область

ІТ-інфраструктура виробничого підприємства малого або середнього бізнесу

**Ключові інформаційні активи**

Виробничі та фінансові бази даних;
технологічна документація, параметри виробництва;
облікові записи;
мережеві конфігурації, журнали подій;
резервні копії та системи відновлення.

**Інформаційний ризик**

Втрата, спотворення або компрометація даних, журналів, доступів і конфігурацій.

**Управлінський ризик**

Необґрунтовані витрати на захист або неправильний порядок впровадження заходів.

**Операційний ризик**

Простій виробництва, затримка планування, зупинка внутрішніх процесів.

Практична база: реєстр активів, паспортизація, сценарії загроз і розрахунок очікуваних втрат.

# Підходи до оцінювання ризиків

Якісний, кількісний, стандартно-орієнтований та гібридний підходи

| Підхід | Сильна сторона | Обмеження |
|---|---|---|
| Якісний | швидкий старт | суб'єктивність |
| SLE/ALE | фінансова мова | чутливість до даних |
| ISO/NIST | системність | потребує адаптації |
| FAIR | ризик у грошах | високі вимоги до статистики |
| Гібридний | баланс точності й практичності | потрібні ваги та правила |

**Висновок аналізу**

Жоден підхід не вирішує задачу повністю: потрібна методика, яка поєднує експертну оцінку, фінансові втрати, сценарії загроз і порівняння контрзаходів.

SLE = AV × EF
разова очікувана втрата

ALE = SLE × ARO
річні очікувані втрати

**Важливе уточнення**

Формули корисні лише тоді, коли деталізовано склад збитків, коефіцієнт впливу та частоту подій.

# Запропонована власна розробка

Поєднання багатокритеріальної, сценарної та фінансової оцінки

1. Встановлюємо цінність активу

критерії C, I, A, B, R, L;
вагові коефіцієнти;
доказова база;
інтегральний показник K_val.

2. Формування сценарію загрози
джерело загрози;
вразливість;
тип інциденту;
наслідки та коефіцієнт впливу.

3. Прийняття рішень

SLE_ext, ALE_before;
залишковий ризик ALE_res;
чистий ефект E_net;
рекомендація щодо контролю.

Єдина основа всього методу — Паспорт інформаційного активу:
Він зв’язує всі три контури в єдину логіку оцінки.

Паспорт активу дає вихідні дані, сценарій загрози задає логіку інциденту, а фінансова частина показує очікувані втрати до та після контрзаходів.

Що фіксується в паспорті

Паспорт активу містить власника, бізнес-процес, залежності, допустимий простій, фінансові параметри, оцінки C, I, A, B, R, L та ваги критеріїв.

# Багатокритеріальна модель цінності активу

Як експертні оцінки, ваги та грошова цінність зводяться в один показник

C конфіденційність

I цілісність

A доступність

B бізнес-значущість

R відновлюваність

L регуляторні наслідки

$K\_val = \Sigma(w_i \times s_i \times q_i) / \Sigma w_i$
підсумкова цінність з урахуванням ваг критеріїв і якості доказів

$K\_CIA = \max(C, I, A)$
правило максимального впливу не дозволяє занизити критичність активу

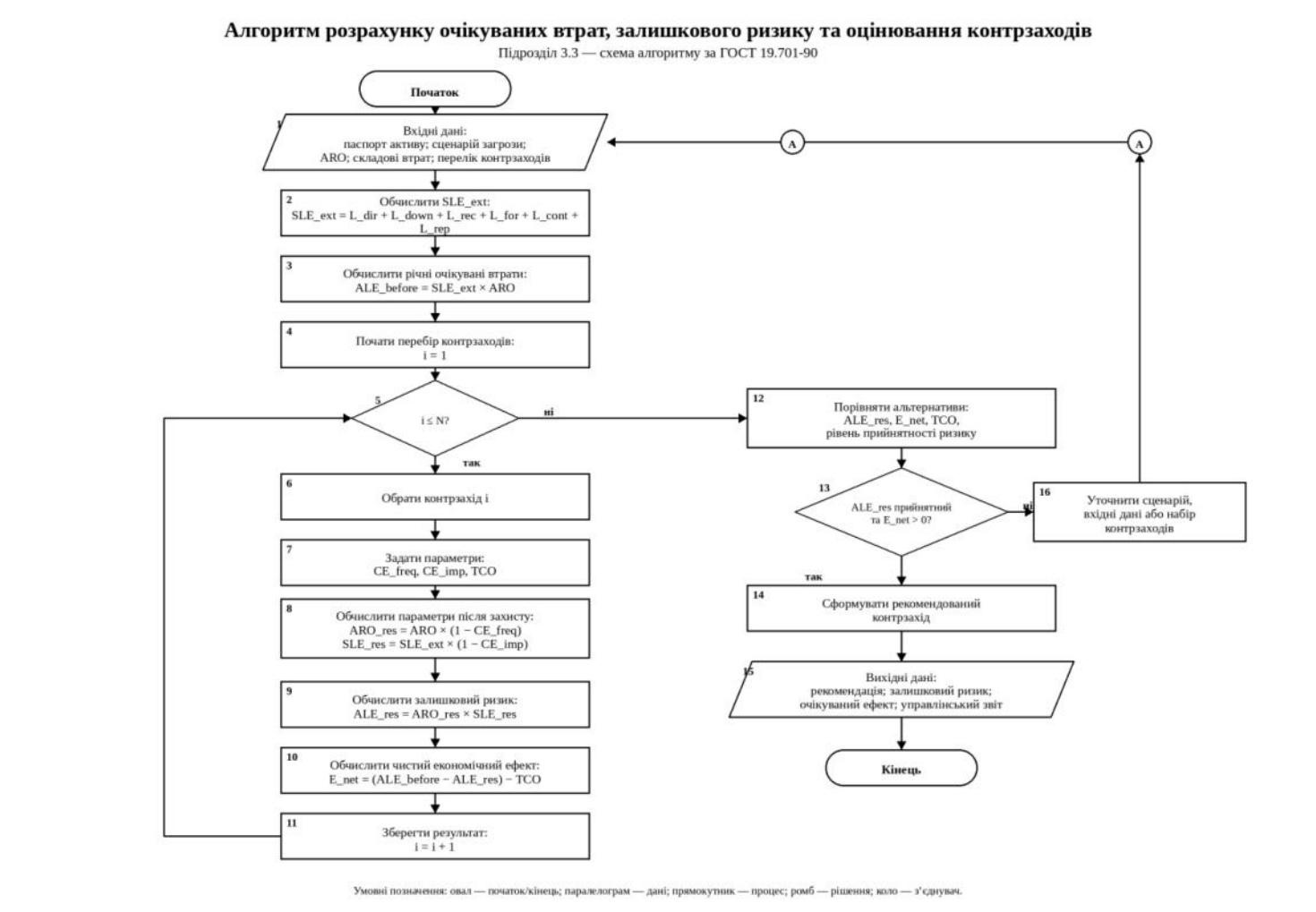
**Пояснення**
Модель C, I, A. Враховує бізнес-роль, відновлення, регуляторні наслідки та ваги. Оцінка стає доказовою, бо прив'язана до джерел даних.

У роботі використано метод безпосереднього експертного оцінювання за бальною шкалою 0–3 з елементами ранжування критеріїв.
Експертні оцінки формуються для критеріїв C, I, A, B, R, L, а ваги критеріїв визначаються залежно від класу активу та його ролі в бізнес-процесі.

**Ключова ідея**
Критичність активу визначається не одним числом, а поєднанням технічного, бізнесового й фінансового впливу.

# Алгоритм розрахунку втрат і вибору контрзаходу

## Схема показує повний шлях: від паспорта активу до управлінської рекомендації




1. Вхід: паспорт активу, сценарій, ARO, перелік контрзаходів.
2. Розрахунок до захисту: SLE_ext, ALE_before.
3. Оцінка альтернатив: CE_freq, CE_imp, TCO_ctrl, ALE_res, E_net.
4. Вибір: прийнятний залишковий ризик + позитивний або обґрунтований ефект.

Головна перевага
Алгоритм робить оцінювання повторюваним: однакова логіка застосовується до різних активів і сценаріїв.

$$E\_net = (ALE\_before - ALE\_res) - TCO\_ctrl$$

показує, чи компенсує контрзахід очікуване зменшення втрат

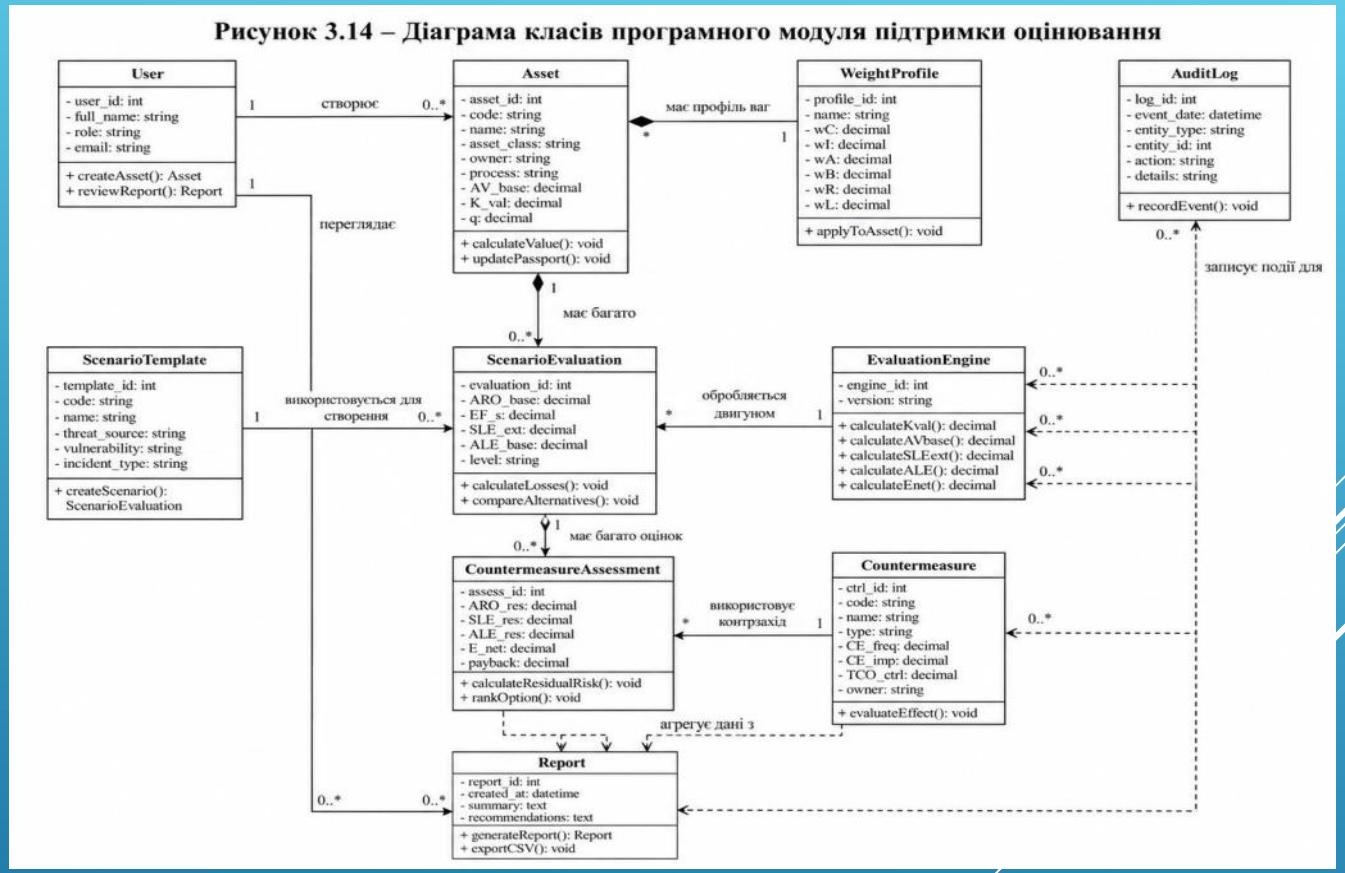
# Програмний модуль як реалізація методу

Модуль перетворює формули та алгоритм у керований процес оцінювання

## Що реалізовано

- Реєстр активів + повна паспортизація.
- Багатокритеріальна оцінка (C, I, A, B, R, L) зі шкалою 0–3.
- Бібліотека сценаріїв загроз + розрахунок K_val, AV_base, SLE_ext, ALE, ALE_res, E_net.
- Каталог контрзаходів та оцінка їх ефективності (CE_freq, CE_imp, TCO).
- Аналітичні звіти, CSV-експорт, журнал аудиту змін

Рисунок 3.14 – Діаграма класів програмного модуля підтримки оцінювання

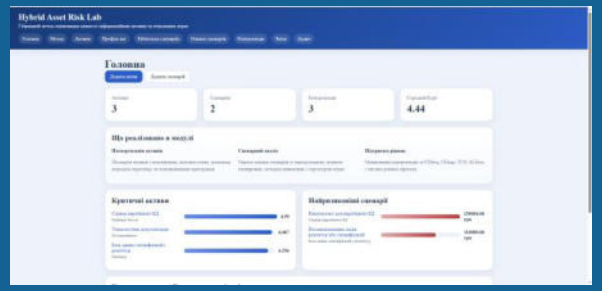



## Пояснення

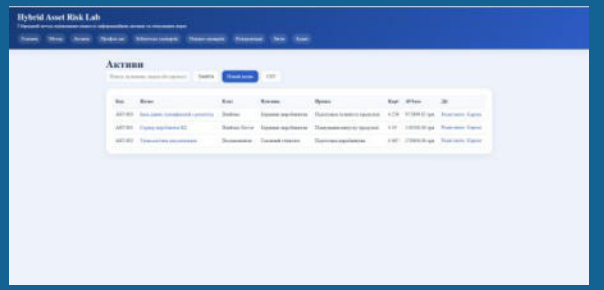
Метод визначає логіку та формули оцінки, а програмний модуль перетворює їх на зручний, повторюваний процес з фіксацією всіх змін, ролями користувачів та аналітичною звітністю.

# Інтерфейс програмного модуля:

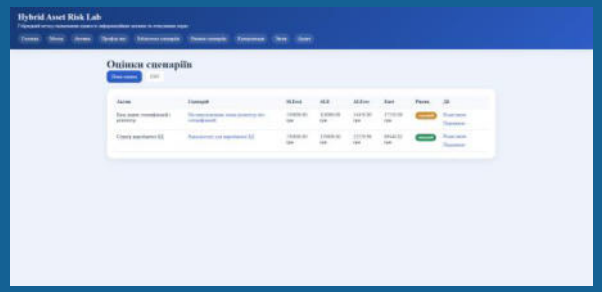
Підтверджує реалізацію повного циклу.



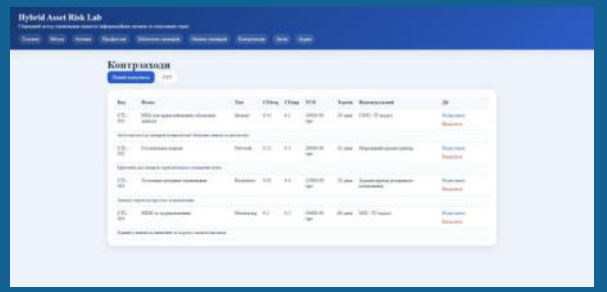

1. Головна панель: підсумкові показники




2. Реєстр активів: паспорти та значення




3. Оцінки сценаріїв: SLE/ALE та рівень




4. Контрзаходи: CE, TCO та відповідальні

## Логіка користувача

Створити паспорт активу → обрати сценарій загрози → розрахувати втрати → порівняти контрзаходи → сформувати звіт.

# Апробація: що показали розрахунки

Метод протестовано на трьох критичних активах та двох реалістичних сценаріях загроз

Сервер виробничої БД
Критичність активу = 3.00
(критичний)

AV_base: 1 180 000 грн

Технологічна документація
Критичність активу = 2.67
(висока)

AV_base: 540 000 грн

БД специфікацій і рецептур
Критичність активу = 3.00
(критичний)

AV_base: 972 999,82 грн

Сценарій 1. Ransomware для виробничої БД

до захисту: річні втрати = 269 549 грн
після захисту: ALE_res ≈ 88 409 грн
очікуване зменшення втрат ≈ 181 140 грн
чистий ефект з урахуванням TCO ≈ 89 140 грн

Сценарій 2. Несанкціонована зміна рецептур

до захисту: річні втрати = 110 000 грн
після захисту: ALE_res = 54 450 грн
очікуване зменшення втрат = 55 550 грн
чистий економічний ефект від контрзаходу
E_net = 37 550 грн

Запропонований метод дозволяє перейти від суб'єктивної оцінки «високий/низький ризик» до конкретних грошових показників - очікуваних втрат, залишкового ризику та окупності контрзаходів. Економічний ефект від впровадження заходів склав 126 690 грн на рік лише за двома сценаріями.

# Порівняльна оцінка: що стало краще

Розроблене рішення усуває методичні, організаційні й технічні слабкі місця спрощеного підходу

| Критерій | Спрощена реалізація | Розроблене рішення |
|---|---|---|
| Актив | назва і загальний опис | паспорт: власник, залежності, межі, фінансові параметри |
| Цінність | CIA без ваг | C, I, A, B, R, L + ваги + докази + S_money |
| Загроза | перелік ризиків | сценарій: актив → загроза → вразливість → наслідок |
| Контрзахід | неформальна оцінка | ALE_res, E_net, TCO_ctrl і рекомендація |
| Звітність | обмежена | аналітичний звіт, CSV, журнал аудиту |

**Умови впровадження**

1) почати з критичних активів; 2) уточнити сценарії; 3) затвердити ваги; 4) призначити відповідальних; 5) вести журнал змін; 6) використовувати звіти для бюджету ІБ.

**Практична перевага**

Рішення стає структурованим, доказовим і економічно інтерпретованим. Це зменшує суб'єктивність оцінок і пояснює вибір контрзаходу.

# Висновки та результат роботи

Що отримано в методичній, програмній та управлінській частині

## Основні результати

- обґрунтовано актуальність задачі оцінювання інформаційних активів;
- проаналізовано підходи ISO/NIST, SLE/ALE, FAIR та програмну логіку;
- розроблено паспорт активу, шкалу 0–3, вагову і сценарну модель;
- запропоновано формули AV_base, SLE_ext, ALE_res, E_net;
- реалізовано програмний модуль і виконано апробацію.

## Практична цінність

Результат роботи допомагає визначити критичні активи, порахувати очікувані втрати, порівняти контрзаходи та підготувати управлінське рішення для малого або середнього підприємства.

Мету роботи досягнуто: розроблено й апробовано підхід, який переводить оцінювання ризику у фінансово-управлінську форму та підтримує вибір пріоритетних контрзаходів.

пріоритеза ція активів → оцінка втрат → вибір контр.зах → управлінсь ке рішення

# Головні питання та відповіді



1.У чому суть вашого програмного методу?
Метод поєднує бальну оцінку активів, грошову оцінку втрат і сценарний аналіз загроз. Це дозволяє не просто визначити критичність активу, а й порахувати очікувані втрати та вибрати доцільний контрзахід.
2.Чому обрана шкала 0–3?
Шкала 0–3 проста й зрозуміла для експертного оцінювання: 0 — незначний рівень, 1 — помірний, 2 — високий, 3 — критичний. Вона не перевантажує модель і підходить для малого та середнього бізнесу.
3.Чому ви використовуєте не тільки CIA, а ще B, R, L?
CIA показує конфіденційність, цілісність і доступність, але цього недостатньо. B враховує бізнес-значущість, R — відновлюваність, L — юридичні та регуляторні наслідки. Так оцінка стає ближчою до реальних умов підприємства.
4.Що таке SLE, ALE, ARO?
SLE — очікувана разова втрата від одного інциденту. ALE — очікувані річні втрати. ARO — очікувана частота реалізації загрози за рік.
5.Чим SLE_ext відрізняється від звичайного SLE?
Звичайний SLE часто враховує лише базову втрату активу. SLE_ext ширший: він включає прямі втрати, простій, відновлення, форензику, договірні та репутаційні наслідки.
6.Як розраховується залишковий ризик?
Залишковий ризик розраховується після врахування контрзаходу. Тобто спочатку визначаються втрати до захисту, потім зменшуються частота або наслідки інциденту, після чого отримується ALE_res.
7.Як ви оцінюєте ефективність контрзаходу?
Через вплив на частоту інциденту, вплив на масштаб збитків і вартість самого заходу. Для цього використовуються CE_freq, CE_imp і TCO_ctrl.
8.Що таке E_net?
E_net — це чистий економічний ефект контрзаходу. Він показує, чи перекриває зменшення очікуваних втрат на впровадження захисту.
9.Що саме реалізовано у програмному модулі?
Реалізовано реєстр активів, паспорт активу, профілі ваг, бібліотеку сценаріїв, каталог контрзаходів, розрахунок K_val, AV_base, SLE_ext, ALE, ALE_res, E_net, а також звітність, CSV-експорт і журнал аудиту.
10.Чим ваша програма краща за Excel-таблицю?
Excel підходить для разових розрахунків, а програма підтримує повний процес: активи, сценарії, контрзаходи, звіти й аудит. Вона краще зберігає структуру даних і робить оцінювання повторюваним.
11.Як виконувалась апробація?
Апробація виконувалась на прикладах критичних активів: виробничої бази даних, технологічної документації, бази специфікацій і рецептур. Для них були розраховані втрати до та після контрзаходів.
12.Який практичний результат отримано?
Отримано методику і програмний модуль, які допомагають визначити критичні активи, порахувати очікувані втрати, оцінити контрзаходи та підготувати управлінське рішення.
13.Недоліки та обмеження?
Точність результатів залежить від якості вхідних даних: експертних оцінок, вартості простою, частоти інцидентів і параметрів контрзаходів. Також апробація виконана на обмеженій кількості прикладів.
14.Що можна покращити в майбутньому?
Можна додати інтеграцію з SIEM, журналами подій, CRM або ERP, автоматизувати отримання частоти інцидентів, розширити бібліотеку сценаріїв і додати аналіз комбінацій контрзаходів.