МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БУДІВНИЦТВА І АРХІТЕКТУРИ

КАФЕДРА КІБЕРБЕЗПЕКИ ТА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ

Бакалаврська кваліфікаційна робота

Токар Анастасії Андріївни

На тему:

«Ідентифікація вразливостей інформаційних активів об'єкту захисту»

Науковий керівник:
к.т.н. доц. Ізмайлова О.В.

Київ 2026

АКТУАЛЬНІСТЬ, МЕТА, ОБ'ЄКТ, ПРЕДМЕТ ДОСЛІДЖЕННЯ

- Актуальність роботи полягає у необхідності розробки та застосування ефективних методів ідентифікації вразливостей, що дозволяють своєчасно виявляти слабкі місця в системах захисту та мінімізувати ризики реалізації кіберзагроз.
- Метою роботи є розробка та обґрунтування методичних підходів та рекомендацій щодо ідентифікації вразливостей інформаційних активів об'єкту захисту для підвищення рівня його кібербезпеки.
- Об'єктом дослідження є інформаційна система (або інформаційно-комунікаційна система) об'єкту захисту як сукупність апаратних, програмних, програмно-апаратних засобів та інформаційних ресурсів, що підлягають захисту.
- Предметом дослідження є процеси, методи та засоби ідентифікації вразливостей інформаційних активів, а також організаційно-технічні підходи до їх виявлення та документування.
- Практичне значення отриманих результатів полягає у можливості застосування розробленої методики для підвищення ефективності роботи фахівців з кібербезпеки та аналітиків з оцінки вразливостей під час проведення обстежень інформаційних систем, а також для вдосконалення процесів управління ризиками інформаційної безпеки в організаціях різних форм власності.

Категорія	Документи	Основне призначення
Конституція та базові закони	Конституція України Закон «Про інформацію» Закон «Про захист персональних даних»	Право на інформацію та обмеження для нацбезпеки; види інформації (конфіденційна, службова, таємна); захист персональних даних
Спеціальне законодавство ІБ	Закон «Про захист інформації в ІТС» Закон «Про основні засади кібербезпеки» Закон «Про державну таємницю» Кримінальний кодекс (ст. 361-363)	Визначає НСД, КСЗІ; аудит, моніторинг вразливостей; режим ДТ; відповідальність за кіберзлочини
Підзаконні акти (КМУ)	Постанова № 373 (Правила захисту інформації) Постанова № 92 (зміни до правил) Постанова № 821 (ліцензування ТЗІ)	Загальні вимоги до захисту; адаптація до електронних комунікацій; оцінка вразливостей – тільки ліцензованими суб’єктами
Національні стандарти ТЗІ	ДСТУ 3396.0-96 (основні положення) ДСТУ 3396.2-97 (терміни та визначення) НД ТЗІ 2.5-004-99 (критерії оцінки захищеності) НД ТЗІ 3.7-003-05 (порядок створення КСЗІ) НД ТЗІ 2.5-005-99 (класифікація АС)	Орієнтири для технічного захисту; єдина термінологія; шкала, метрики, рівні захищеності; етапи створення КСЗІ; визначення класу системи
Гармонізовані європейські стандарти	ДСТУ ISO/IEC 27001:2023 (СУІБ) ДСТУ ISO/IEC 27002:2023 (засоби контролю) ДСТУ ISO/IEC 27005:2023 (управління ризиками) ДСТУ ISO/IEC 27037:2017 (цифрові докази)	Ризик-орієнтований підхід; довідник контролів для усунення вразливостей; структурований процес управління ризиками; вимоги до цифрової криміналістики
Професійний стандарт	«Аналітик з оцінки вразливостей» (Наказ Держспецзв’язку № 38 від 23.01.2024)	Компетентності, трудові функції, результати навчання

КЛАСИФІКАЦІЯ ІНФОРМАЦІЙНИХ АКТИВІВ, ВРАЗЛИВОСТЕЙ

КЛАСИФІКАЦІЯ ВРАЗЛИВОСТЕЙ ЗА ДП
Апаратні
Програмні
Організаційні
Людські

КЛАСИФІКАЦІЯ ІА
Організаційні методи ІА
Технічні методи ІА
За функціональним призначенням
За рівнем доступу інформації
За критичністю і цінністю
За властивостями інформаційної безпеки

КЛАСИФІКАЦІЯ ВРАЗЛИВОСТЕЙ ЗА МВ
Мережеві
Системні
Прикладні
Пов’язані із засобами захисту

Методи ідентифікації вразливостей

Методи:

- Пасивні базуються на зборі та аналізі наявної інформації. Аналіз документації передбачає вивчення політик безпеки, регламентів, інструкцій, проектної документації, схем топології мережі, переліків обладнання та конфігураційних файлів.
- Активні методи передбачають безпосередню взаємодію з інформаційною системою і можуть певною мірою впливати на її роботу.

ID активу	Категорія	Назва / роль	IP-адреса	Критичність	Обґрунтування
A-001	Апаратне забезпечення	Веб-сервер (додатків)	192.168.56.105	Висока	Забезпечує роботу веб-додатків, доступний з мережі
A-002	Апаратне забезпечення	Файловий сервер	192.168.56.110	Середня	Зберігає конфігураційні файли та документи
A-003	Апаратне забезпечення	Робоча станція	192.168.56.120	Низька	Тестовий клієнт, не містить критичних даних

РАНЖУВАННЯ ІНФОРМАЦІЙНИХ АКТИВІВ ЗА ЦІННІСТЮ

Нормалізована матриця (середні ранги при зв'язаних рангах)									
Експерт	Інформаційні активи	Програмні активи	Апаратні активи	Сервісні активи	Дані	Людські активи	ПК	Нематеріальні активи	Ri
1	1	3	3	3	5	6	7	8	36
2	1	2	3,5	3,5	5	7	7	7	36
3	1	2	3	4	5	6	7,5	7,5	36
4	1	2,5	2,5	4	5	6	7	8	36

Коефіцієнт конкордації W	
n (кількість експертів)	4
m (кількість активів)	8
ΣDj^2	636
ΣTi	4
W =	0,948310139

Цінність активів в діапазоні оцінювання		
Формула: Цінність = 10 - (Rj - Rj_min)/(Rj_max - Rj_min) *3 (менший ранг = вища цінність)		
Актив	Rj	Цінність
Інформаційні активи	4	10
Програмні активи	9,5	9,377358
Апаратні активи	12	9,09434
Сервісні активи	14,5	8,811321
Дані	20	8,188679
Людські активи	25	7,622642
ПК	28,5	7,226415
Нематеріальні активи	30,5	7

МОДЕЛЬ ЗАГРОЗ

Категорія	Суть загрози	Приклад (з виявлених вразливостей)	Контрзахід
Spoofing (підміна)	Несанкціонований доступ через підміну облікових даних	CVE-2020-14145 (перерахування користувачів SSH) + відсутність MFA	MFA, сертифікати, складні паролі
Tampering (втручання)	Модифікація даних, ПЗ, логів	CVE-2021-44790 (Apache RCE) – зміна веб-сторінок, баз даних	Оновлення ПЗ, WAF, контроль цілісності
Repudiation (відмова)	Заперечення факту виконання дії	Логи зберігаються локально без захисту	SIEM, централізований захист логів, DLP
Information Disclosure (розкриття)	Ознайомлення з конфіденційною інформацією	FTP Anonymous Access, слабкі шифри SSL/TLS, TCP timestamps	Шифрування (TLS/VPN), DLP, RBA

МОДЕЛЬ ПОРУШНИКА

Модель порушника
Внутрішній користувач (ненавмисний порушник)
Внутрішній користувач (умисний порушник / інсайдер)
Привілейований порушник (адміністратор, техпідтримка)
Зовнішній порушник (хакер, кіберзлочинець, конкурент)
Зовнішній порушник (випадковий / ненавмисний)

МЕТОД АНАЛІЗУ ІЄРАРХІЙ

Матриця попарних порівнянь для критеріїв

Критерій	АУ	КЦ	КД	ЗС	Добуток	ОВ	Вага
АУ	1	0,5	0,33	3	0,495	0,84	0,17
КЦ	2	1	0,5	4	4	1,41	0,29
КД	3	2	1	5	30	2,34	0,47
ЗС	0,33	0,25	0,2	1	0,0165	0,36	0,07
Сума						4,95	

Загроза	АУ (0,17)	КЦ (0,29)	КД (0,47)	ЗС (0,07)	Vi
Підміна	0,47	0,23	0,25	0,08	0,2697
Втручання	0,16	0,55	0,15	0,23	0,2733
Розкриття	0,28	0,14	0,54	0,14	0,3518
Відмова	0,10	0,08	0,07	0,55	0,1116
Вага	0,17	0,29	0,47	0,07	

Критерій	Вага	Пояснення
КД (контроль доступу / конфіденційність)	0,47	Найвищий пріоритет – захист персональних даних та комерційної таємниці
КЦ (контроль цілісності)	0,29	Високий пріоритет – захист цілісності даних та логів
АУ (автентифікація)	0,17	Середній пріоритет – контроль доступу через автентифікацію
ЗС (доступність)	0,07	Найнижчий пріоритет – забезпечення доступності

CVSS

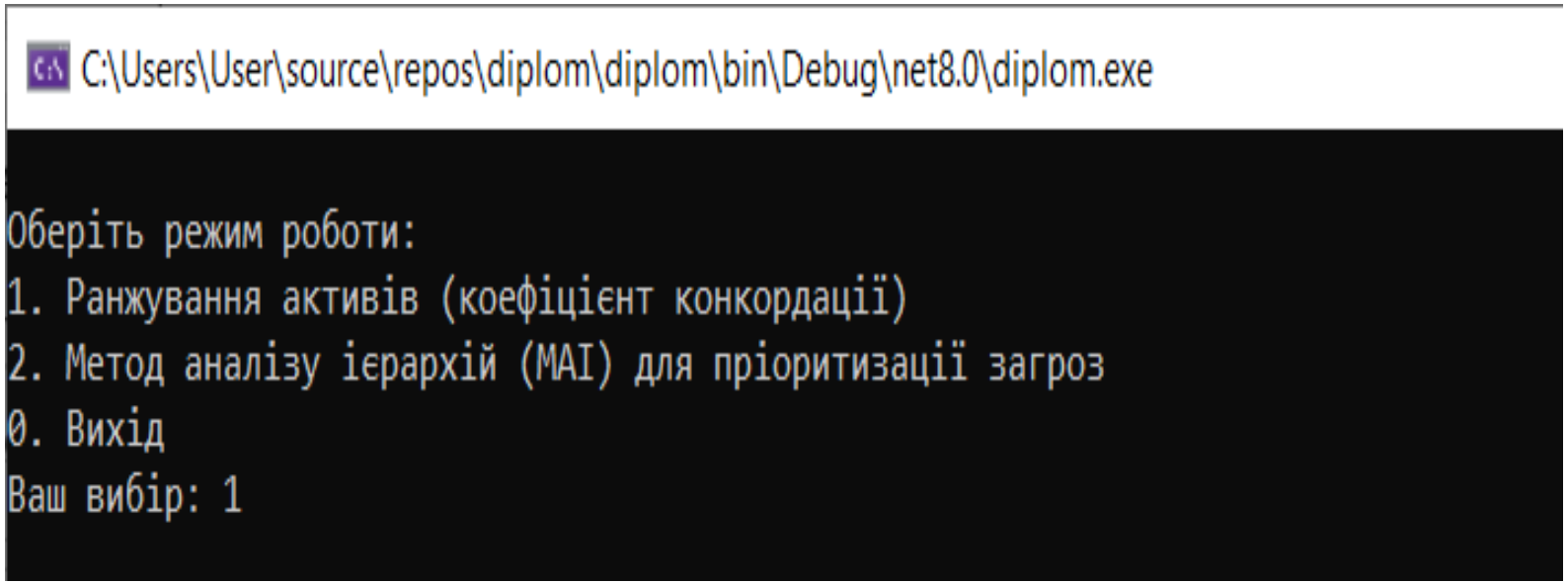
CVSS (Common Vulnerability Scoring System) — це загальноприйнятий стандарт для визначення ступеня небезпеки вразливостей в інформаційних системах.

Вразливість (CVE / опис)	Уражений актив	AV	AC	PR	UI	C	I	A	Base Score	Рівень
CVE-2021-44790 (Apache RCE)	192.168.56.105	0,85	0,77	0,85	0,85	0,56	0,56	0,56	9,8	Critical
CVE-2020-14145 (OpenSSH user enum)	192.168.56.105	0,85	0,77	0,85	0,85	0,22	0,22	0	5,3	Medium
FTP Anonymous Access	192.168.56.110	0,85	0,77	0,85	0,85	0,22	0	0	5	Medium
SSH weak MAC algorithms	192.168.56.105	0,85	0,44	0,85	0,85	0	0	0	4,3	Medium
SSL/TLS Weak Ciphers	192.168.56.110	0,85	0,44	0,85	0,85	0,22	0	0	4,8	Medium

ПРОГРАМНА РЕАЛІЗАЦІЯ

Модулі:

- RankingModule – ранжування активів (коефіцієнт конкордації, критерій Пірсона, цінність).
- AhpModule – метод аналізу ієрархій (власні вектори, перевірка узгодженості HR, глобальні пріоритети).

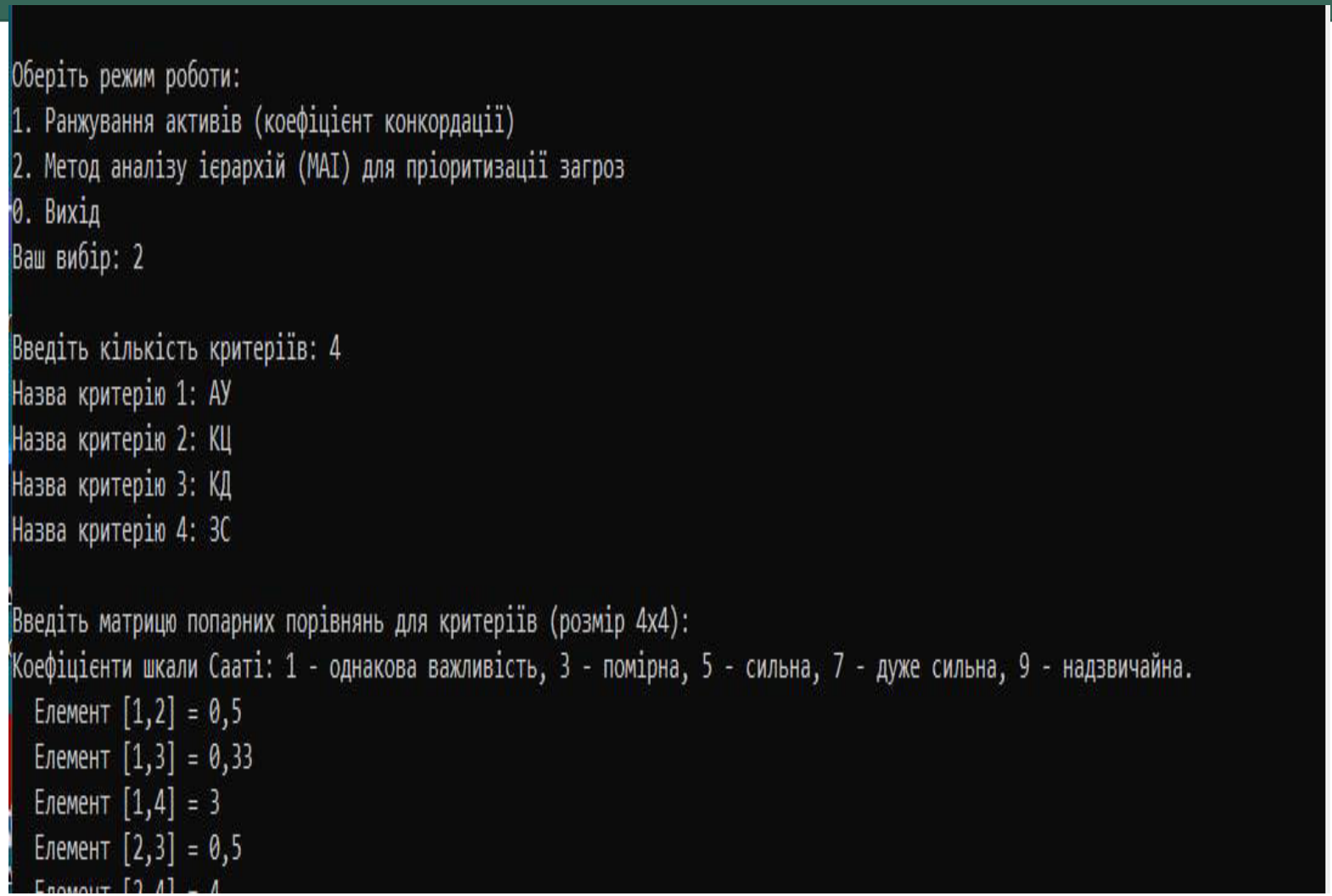


```
Введіть кількість експертів (m): 4
Введіть кількість активів (n): 8
Введіть матрицю рангів (експерти - рядки, активи - стовпці):
1 3 3 3 5 6 7 8
1 2 4 4 5 7 7 7
1 2 3 4 5 6 8 8
1 3 3 4 5 6 7 8

--- РЕЗУЛЬТАТИ РАНЖУВАННЯ АКТИВІВ ---
Кількість експертів m = 4
Кількість активів n = 8
Суми рангів Rj: 4,0  9,5  12,0  14,5  20,0  25,0  28,5  30,5
Коефіцієнт конкордації W = 0,9490
Критерій Пірсона χ² = 26,57
Табличне значення χ²(0.05, 7) = 14,07
=> Узгодженість експертів є статистично значущою (χ² > χ²_табл).

Цінність активів (шкала 7-10):
  Актив 1: 10,00
  Актив 2: 9,38
  Актив 3: 9,09
  Актив 4: 8,81
  Актив 5: 8,19
  Актив 6: 7,62
  Актив 7: 7,23
  Актив 8: 7,00
```

ПРОГРАМА (ВИБІР 2 МАІ)



```
 Елемент [3,4] = 5

Вага критеріїв:
 АУ: 0,1692
 КЦ: 0,2852
 КД: 0,4732
 ЗС: 0,0725
λ_max = 4,0515, HR = 0,0191
=> Узгодженість матриці критеріїв прийнятна (HR < 0.1).

Введіть кількість альтернатив (загроз): 4
Назва альтернативи 1: S
Назва альтернативи 2: T
Назва альтернативи 3: I
Назва альтернативи 4: D

=== Критерій 1: АУ ===

Введіть матрицю попарних порівнянь для альтернатив для критерію АУ (розмір 4x4):
Коефіцієнти шкали Сааті: 1 - однакова важливість, 3 - помірна, 5 - сильна, 7 - дуже сильна, 9 - надзвичайна.
 Елемент [1,2] = 3
 Елемент [1,3] = 2
 Елемент [1,4] = 4
 Елемент [2,3] = 0,5
 Елемент [2,4] = 2
 Елемент [3,4] = 3
Локальні пріоритети альтернатив:
 S: 0,4668
 T: 0,1603
 I: 0,2776
```

```
 D: 0,0953
λ_max = 4,0310, HR = 0,0115 (прийнятна)

=== Критерій 2: КЦ ===

Введіть матрицю попарних порівнянь для альтернатив для критерію КЦ (розмір 4x4):
Коефіцієнти шкали Сааті: 1 - однакова важливість, 3 - помірна, 5 - сильна, 7 - дуже сильна, 9 - надзвичайна.
 Елемент [1,2] = 0,333
 Елемент [1,3] = 2
 Елемент [1,4] = 3
 Елемент [2,3] = 4
 Елемент [2,4] = 5
 Елемент [3,4] = 2
Локальні пріоритети альтернатив:
 S: 0,2328
 T: 0,5451
 I: 0,1385
 D: 0,0837
λ_max = 4,0512, HR = 0,0190 (прийнятна)

=== Критерій 3: КД ===

Введіть матрицю попарних порівнянь для альтернатив для критерію КД (розмір 4x4):
Коефіцієнти шкали Сааті: 1 - однакова важливість, 3 - помірна, 5 - сильна, 7 - дуже сильна, 9 - надзвичайна.
 Елемент [1,2] = 2
 Елемент [1,3] = 0,333
 Елемент [1,4] = 4
 Елемент [2,3] = 0,25
 Елемент [2,4] = 3
 Елемент [3,4] = 5
Локальні пріоритети альтернатив:
 S: 0,2455
 T: 0,1504
 I: 0,5350
 D: 0,0691
λ_max = 4,1178, HR = 0,0436 (прийнятна)
```

ПРОГРАМА (ВИБІР 2 МАІ)

```
=== Критерій 4: ЗС ===

Введіть матрицю попарних порівнянь для альтернатив для критерію ЗС (розмір 4x4):
Коефіцієнти шкали Сааті: 1 - однакова важливість, 3 - помірна, 5 - сильна, 7 - дуже сильна, 9 - надзвичайна.
  Елемент [1,2] = 0,333
  Елемент [1,3] = 0,5
  Елемент [1,4] = 0,2
  Елемент [2,3] = 2
  Елемент [2,4] = 0,333
  Елемент [3,4] = 0,25
Локальні пріоритети альтернатив:
  S: 0,0836
  T: 0,2328
  I: 0,1384
  D: 0,5451
λ_max = 4,0512, HR = 0,0190 (прийнятна)
```

```
--- ГЛОБАЛЬНІ ПРІОРИТЕТИ ЗАГРОЗ ---
  S: 0,2676
  T: 0,2706
  I: 0,3496
  D: 0,1122
Сума глобальних пріоритетів = 1,0000 (повинна дорівнювати 1).

Оберіть режим роботи:
1. Ранжування активів (коефіцієнт конкордації)
```

ВИСНОВКИ

- У дипломній роботі розглянуто актуальну проблему ідентифікації вразливостей інформаційних активів об’єкта захисту. У результаті виконаних досліджень розроблено та обґрунтовано методичні підходи до виявлення, аналізу та оцінювання вразливостей.
- Основними досягненнями роботи стали детальний аналіз сучасних методів ідентифікації вразливостей, що дозволило визначити ключові підходи до побудови ефективного процесу оцінки ризиків. За допомогою інструментів Nmap та OpenVAS виконано інвентаризацію активів та виявлено 34 вразливості різного рівня критичності. Проведено оцінку критичності вразливостей за методикою CVSS, що дозволило визначити пріоритети їх усунення.
- Удосконалено процес ідентифікації активів шляхом застосування експертного ранжування восьми категорій активів із використанням коефіцієнта конкордації Кендалла, що підтвердило високу узгодженість думок експертів. Найвищу цінність отримали інформаційні активи (дані), що дозволило обґрунтовано визначити пріоритети захисту. Побудовано модель загроз за методологією STRIDE та модель порушника (п’ять типів), які дали змогу оцінити ймовірність реалізації загроз. За допомогою методу аналізу ієрархій (MAI) визначено глобальні пріоритети загроз: найбільш критичною виявилася загроза розкриття інформації.
- Розроблений комплексний підхід до ідентифікації вразливостей інформаційних активів є надійним інструментом для управління ризиками та забезпечення безпеки в сучасних інформаційних системах. Його впровадження дозволить організаціям ефективно захищати свої інформаційні активи та мінімізувати потенційні загроз.

ДЯКУЮ ЗА УВАГУ!