КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БУДІВНИЦТВА І АРХІТЕКТУРИ

Автоматизації та інформаційних технологій

(факультет)

Кібербезпеки та комп'ютерної інженерії

(назва випускової кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

ЗДОБУВАЧА СТУПЕНЯ ВИЩОЇ ОСВІТИ
БАКАЛАВР

на тему:

CTF-кіберполігон в навчальній діяльності як інструмент практичної підготовки здобувачів освіти

Тарасов Максим Ілліч

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

Київ 2026р.

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БУДІВНИЦТВА І АРХІТЕКТУРИ

Автоматизації і інформаційних технологій

(факультет)

Кібербезпеки та комп'ютерної інженерії

(назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
Делембовський М.М.
„___" _____20___року

КВАЛІФІКАЦІЙНА РОБОТА ЗДОБУВАЧА СТУПЕНЯ ВИЩОЇ ОСВІТИ БАКАЛАВР

CTF-кіберполігон в навчальній діяльності як інструмент практичної підготовки здобувачів освіти

(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 Тарасов Максим Ілліч
(прізвище, ім'я та по батькові повністю)
125 "Кібербезпека"

(спеціальність)

Безпека інформаційних і комунікаційних систем

(освітня програма)

Група БІКС-22
Керівник Делембовський М.М.
(прізвище та ініціали)
Кандидат технічних наук, доцент
(вчене звання, науковий ступінь)
Рецензент_____
(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.
„___" _____ 20___ року

З А В Д А Н Н Я

ДО ВИКОНАННЯ КВАЛІФІКАЦІЙНОЇ РОБОТИ
ЗДОБУВАЧА СТУПЕНЯ ВИЩОЇ ОСВІТИ Бакалавр
(бакалавр, магістр)

Тарасов Максим Ілліч

(прізвище, ім'я та по батькові здобувача)

1. Тема роботи: CTF-кіберполігон в навчальній діяльності як інструмент практичної підготовки здобувачів освіти

затверджена наказом ректора КНУБА № 576/52-15/13.2/26 від «14» травня 2026 року

2. Керівник роботи

Делембовський Максим Михайлович

кандидат технічних наук, доцент

(прізвище, ім'я та по батькові, науковий ступінь, вчене звання)

3. Термін подання здобувачем роботи до захисту _____

4. Зміст пояснювальної записки за розділами:

Р. 1. Теоретичні основи CTF-кіберполігонів як інструменту підготовки здобувачів освіти

Р. 2. Стан підготовки здобувачів освіти в сфері кібербезпеки та роль кіберполігонів

Р. 3. Розробка моделі CTF-кіберполігону на базі PAM CyberArk як інструменту навчання

5. Графічний матеріал за розділами

Р. 1. Теоретичні основи CTF-кіберполігонів як інструменту підготовки здобувачів освіти

Р. 2. Стан підготовки здобувачів освіти в сфері кібербезпеки та роль кіберполігонів

Р. 3. Розробка моделі CTF-кіберполігону на базі PAM CyberArk як інструменту навчання

6. Консультанти розділів кваліфікаційної випускної роботи

Розділ	Прізвище, ініціали та посада консультанта	Перевірив	
		дата	підпис
Розділ 1.	Делембовський М. М.	06.04.2026	
Розділ 2.	Делембовський М. М.	27.04.2026	
Розділ 3.	Делембовський М. М.	11.05.2026	

7. Календарний план виконання роботи:

Види робіт та їх зміст	Дата виконання
Розділ 1.	06.04.2026
Розділ 2.	27.04.2026
Розділ 3.	11.05.2026
Остаточне оформлення роботи	08.06.2026
Направлення роботи для перевірки на плагіат	10.06.2026
Попередній захист роботи на випусковій кафедрі	12.06.2026
Направлення роботи на рецензування	12.06.2026

8. Дата видачі завдання «14» травня 2026 року

Керівник _____ Делембовський М.М.
(підпис) (прізвище та ініціали)

Здобувач _____ Тарасов М.І.
(підпис) (прізвище та ініціали)

РЕЗЮМЕ (SUMMARY) *до кваліфікаційної випускної роботи здобувача:*			Тарасов Максим Ілліч Tarasov Maksym Illich *(ПІБ здобувача українською та англійською)*
ЗВО	Київський національний університет будівництва і архітектури		
Тема *(українською та англійською)*	CTF-кіберполігон в навчальній діяльності як інструмент практичної підготовки здобувачів освіти CTF-cyber polygon in educational activities as a tool for practical training of education seekers		
Освітній ступінь	Бакалавр		
Факультет	Автоматизації і інформаційних технологій		
Випускова кафедра	Кібербезпеки та комп'ютерної інженерії		
Спеціальність	125 "Кібербезпека"		
Освітня програма	Безпека інформаційних і комунікаційних систем		
Керівник	Делембовський Максим Михайлович		
Обсяг роботи:	*пояснювальна записка, стор.*	*розділів*	*Слайдів презентації*
	101	3	12
Розділ 1	Теоретичні основи CTF-кіберполігонів як інструменту підготовки здобувачів освіти		
Розділ 2	Стан підготовки здобувачів освіти в сфері кібербезпеки та роль кіберполігонів		
Розділ 3	Розробка моделі CTF-кіберполігону на базі PAM CyberArk як інструменту навчання		
Висновки по роботі:	У кваліфікаційній роботі розроблено та апробовано модель CTF-кіберполігону на базі системи привілейованого доступу PAM CyberArk Self-Hosted як інструменту практичної підготовки здобувачів вищої освіти		
Ключові слова: *Keywords:*	cybersecurity, CTF, cyber range, CyberArk, PAM, privileged access management, Digital Vault, PVWA, PSM, CPM, PTA, gamification		

Здобувач: Тарасов М.І. / /

Керівник: Делембовський М.М. / /

"__" _____ 20__

Анотація

Кваліфікаційна випускна робота присвячена дослідженню та розробленню моделі CTF-кіберполігону на базі системи привілейованого доступу (PAM) CyberArk як інструменту практичної підготовки здобувачів вищої освіти спеціальності 125 «Кібербезпека». Актуальність теми обумовлена стрімким зростанням кіберзагроз в Україні та невідповідністю традиційних форм навчання вимогам ринку праці, що зумовлює необхідність впровадження сучасних інтерактивних інструментів формування практичних компетентностей.

Ключові слова: кібербезпека, CTF, кіберполігон, CyberArk, PAM, привілейований доступ, практична підготовка, гейміфікація.

Abstract

The qualification thesis is dedicated to the research and development of a CTF cyber range model based on the CyberArk Privileged Access Management (PAM) system as a tool for practical training of higher education students in specialty 125 "Cybersecurity". The relevance of the topic is determined by the rapid growth of cyber threats in Ukraine and the inadequacy of traditional teaching methods to meet current labor market demands, which necessitates the introduction of modern interactive tools for developing practical competencies.

Keywords: cybersecurity, CTF, cyber range, CyberArk, PAM, privileged access management, practical training, gamification.

ЗМІСТ

ВСТУП

Сучасний світ важко уявити без надійного захисту інформації та цифрових систем. Кіберзагрози оточують нас усюди і набувають щоразу більшої складності: від targeted атак на критичну інфраструктуру до витоку конфіденційних даних великих корпорацій. Те, що ще десять років тому сприймалося як поодинокі інциденти, сьогодні стало щоденною реальністю, яка може зупинити роботу банків, лікарень, державних установ чи енергосистем за лічені хвилини. Саме тому підготовка висококваліфікованих фахівців з кібербезпеки набуває стратегічного значення для національної безпеки України.

Кількість кібератак щорічно зростає в геометричній прогресії, а традиційні форми навчання (лекції, лабораторні роботи в ізольованих віртуальних середовищах) вже не забезпечують формування реальних практичних компетентностей. Студенти та випускники часто володіють теоретичними знаннями, але не мають досвіду роботи з enterprise-рівнем систем у реальних умовах. У таких умовах одним із найефективніших інструментів практичної підготовки здобувачів освіти стають CTF-кіберполігони (Capture The Flag) — інтерактивні платформи, що імітують справжні сценарії атак і захисту. На ринку з'являється дедалі більше промислових рішень, які можна адаптувати під навчальні цілі, зокрема системи привілейованого доступу (PAM). Тому тема дипломної роботи «CTF-кіберполігон у сфері навчання як інструмент підготовки здобувачів освіти» є надзвичайно актуальною.

За останні роки стрімко розвиваються інноваційні технології кіберполігонів, які поєднують гейміфікацію, реальне промислове

обладнання та сучасні методики навчання. Хоча багато платформ набули популярності серед ентузіастів, їх використання у вищій освіті все ще залишається фрагментарним. Пристрої та системи кіберполігонів мають на меті не лише імітацію загроз, а й формування комплексних hard- та soft-навичок: від виявлення вразливостей до швидкого реагування в умовах реального тиску.

У найближчий час у навчальному процесі все активніше застосовуватимуться enterprise-рішення, які забезпечують реалістичне середовище для відпрацювання атак і захисту. Більш ефективна взаємодія між теорією, практикою та реальними виробничими системами — це ключ до якісної підготовки фахівців, здатних протистояти сучасним кіберзагрозам.

Метою дипломної роботи є розробка та обґрунтування моделі CTF-кіберполігону на базі системи PAM CyberArk як ефективного інструменту практичної підготовки здобувачів вищої освіти спеціальності 125 «Кібербезпека».

Для досягнення поставленої мети вирішено такі завдання: дослідити теоретичні основи CTF-кіберполігонів та їх класифікацію; проаналізувати нормативно-правову базу та педагогічні аспекти використання кіберполігонів в освіті; оцінити поточний стан практичної підготовки здобувачів спеціальності 125 в КНУБА; провести порівняльний аналіз існуючих платформ і кіберполігонів; розробити та апробувати модель CTF-кіберполігону на базі PAM CyberArk.

Об'єктом дослідження є процес практичної підготовки здобувачів вищої освіти спеціальності 125 «Кібербезпека».

Предметом дослідження є CTF-кіберполігон на базі системи PAM CyberArk як інструмент формування практичних компетентностей.

Методи дослідження: системний аналіз, порівняльний аналіз, анкетування, педагогічний експеримент, SWOT-аналіз.

Практичне значення роботи: розроблена модель CTF-кіберполігону впроваджена в навчальний процес кафедри кібербезпеки та комп'єрної інженерії КНУБА у партнерстві з компанією ВАКОТЕСН.

1. ТЕОРЕТИЧНІ ОСНОВИ CTF-КІБЕРПОЛІГОНІВ ЯК ІНСТРУМЕНТУ ПІДГОТОВКИ ЗДОБУВАЧІВ ОСВІТИ

1.1. Поняття та класифікація кіберполігонів і CTF (Capture The Flag)

Кіберполігон (англ. *cyber range*) — це спеціально створене контрольоване віртуальне або гібридне середовище, яке імітує реальні інформаційно-комунікаційні системи, мережі, обладнання та бізнес-процеси з метою тренування, тестування та дослідження заходів кібербезпеки. На відміну від звичайних лабораторій, кіберполігон забезпечує високий рівень реалістичності: він дозволяє моделювати повноцінні кібератаки, захист, виявлення інцидентів та реагування на них без ризику для реальних виробничих систем.

Згідно з визначеннями міжнародних стандартів (NIST, ECSO) та українським законодавством, кіберполігон є ключовим інструментом формування практичних компетентностей фахівців. Він поєднує елементи симуляції реальних загроз, оркестрації сценаріїв та аналізу поведінки учасників у динамічному середовищі. Основна мета кіберполігону — створити безпечний «пісочний майданчик» (*sandbox*), де здобувачі освіти можуть експериментувати, помилятися та вдосконалювати навички без наслідків для критичної інфраструктури [7, 8].

CTF (Capture The Flag / Захоплення прапора) — це один із найпоширеніших форматів практичних змагань у сфері кібербезпеки, який став невід’ємною частиною сучасних кіберполігонів. У CTF учасники (індивідуально або в командах) отримують завдання, пов’язані з пошуком та експлуатацією вразливостей у спеціально підготовлених системах.

«Прапор» (*flag*) — це спеціальний рядок тексту (наприклад, flag{congr4tz_y0u_found_1t}), який підтверджує успішне виконання завдання. Учасник, який першим знаходить і подає прапор, отримує бали.

CTF з'явився як еволюція традиційних хакерських змагань і сьогодні широко використовується в освіті, корпоративному тренінгу та професійних конкурсах (DEF CON CTF, HackTheBox, TryHackMe тощо). На відміну від теоретичних тестів, CTF розвиває одразу кілька ключових компетентностей: розвідку, експлуатацію вразливостей, аналіз коду, форензику, криптоаналіз, мережеву безпеку та командну взаємодію.

Кіберполігони класифікують за кількома критеріями. За типом реалізації їх поділяють на симуляційні, емуляційні, накладні та гібридні (табл. 1.1).

Таблиця 1.1 — Класифікація кіберполігонів за типом реалізації

Тип реалізації	**Опис**	**Приклади платформ / рішень**
Симуляційні (Simulation ranges)	Імітація поведінки систем на програмному рівні без точного відтворення апаратного забезпечення.	Cyber Polygon (WEF), прості віртуальні лабораторії на базі VirtualBox / VMware
Емуляційні (Emulation ranges)	Точне відтворення реального апаратного та програмного забезпечення (включаючи ОС, мережеве обладнання).	HackTheBox Academy, TryHackMe, повноцінні емулятори Cisco / Juniper

Продовження таблиці 1.1

Накладні (Overlay ranges)	Накладання віртуальних елементів атаки/захисту на реальну виробничу інфраструктуру.	Промислові рішення на базі реальних серверів з віртуальною оркестрацією
Гібридні (Hybrid ranges)	Комбінація симуляції, емуляції та реального обладнання. Найвищий рівень реалістичності.	Авторський CTF-кіберполігон на базі PAM CyberArk (Vault + PVWA + PSM + CPM + PTA), який встановлено автором у компанії BAKOTECH

Також кіберполігони можуть бути поділеними за такими типами:

1. **За призначенням**:
   - Освітні (для ЗВО).
   - Корпоративні (для тренування співробітників).
   - Державні/військові (для захисту критичної інфраструктури).
   - Дослідницькі (для тестування нових технологій).
2. **За рівнем складності**:
   - Базовий (вступні завдання).
   - Середній (комбіновані сценарії).
   - Просунутий (повноцінні red/blue/purple team вправи з реальними enterprise-рішеннями).

CTF-змагання класифікують переважно за форматом проведення. Основні формати наведено в табл. 1.2.

Таблиця 1.2 — Порівняльна характеристика основних форматів CTF

Формат	**Переваги**	**Недоліки**	**Застосування в освіті**
Jeopardy-style	Простота організації, швидкий старт, можливість працювати індивідуально або в командах, висока гнучкість завдань.	Відсутність реальної взаємодії між командами, менша реалістичність порівняно з бойовими сценаріями.	Найпоширеніший формат у ЗВО. Ідеально підходить для початкової та середньої підготовки здобувачів.
Attack-Defense (A/D)	Максимальна реалістичність, розвиває навички як захисту, так і атаки, формує командну взаємодію в реальних умовах.	Висока складність організації, потребує потужної інфраструктури, довгий час підготовки.	Використовується на просунутому рівні, у фінальних етапах змагань та корпоративних тренінгах.
King of the Hill (KotH)	Динамічність, швидке отримання результату, розвиток навичок швидкого реагування.	Менша глибина завдань, обмежена кількість учасників одночасно.	Добре підходить для коротких практичних занять і проміжного контролю знань.

Продовження таблиці 1.2

Mixed (Змішаний)	Максимальна гнучкість, можливість адаптувати під різні рівні підготовки, поєднання переваг різних форматів.	Складність організації та оцінювання, потребує досвідченого модератора.	Рекомендується для авторських кіберполігонів у вищій освіті, особливо при інтеграції з enterprise-рішеннями (PAM, SIEM тощо).

1.2 Історія розвитку та сучасні тенденції

Історія кіберполігонів і CTF-змагань тісно пов’язана з еволюцією галузі кібербезпеки. Перші прототипи сучасних CTF з’явилися наприкінці 1990-х років у рамках хакерських конференцій. Офіційною точкою відліку вважається 1996 рік, коли на конференції DEF CON у Лас-Вегасі було проведено перше змагання Capture The Flag. Тоді воно мало вигляд простого протистояння команд, які намагалися зламати системи одна одної та захистити власні. Цей формат швидко набув популярності й став основою для подальшого розвитку.

У 2000-х роках CTF перетворився з розваги для ентузіастів на серйозний навчальний інструмент. У 2007–2010 роках з’явилися перші онлайн-платформи SmashTheStack і OverTheWire, які дозволяли учасникам тренуватися дистанційно. Значний поштовх розвитку відбувся у 2010-х роках із появою комерційних платформ: HackTheBox (2017) та TryHackMe

(2018). Ці сервіси вперше почали пропонувати не лише окремі завдання, а й цілі віртуальні машини з реальними вразливостями, що максимально наблизило навчання до виробничих умов [18, 19].

Паралельно розвивалися й повноцінні кіберполігони. У 2010-х роках провідні країни (США, Ізраїль, Естонія) створили національні кіберполігони для тренування військових і державних фахівців. У 2020 році Світовий економічний форум (WEF) запустив глобальний проєкт Cyber Polygon — найбільший у світі щорічний кіберполігон, який імітує атаки на критичну інфраструктуру. Цей проєкт став еталоном гібридного enterprise-рівневого середовища.

В Україні історія кіберполігонів почалася після прийняття Закону України «Про основні засади забезпечення кібербезпеки України» (2017) та Стратегії кібербезпеки (2021). Перші освітні ініціативи з'явилися у 2018–2019 роках на базі провідних ЗВО (КНУБА, КПІ ім. Ігоря Сікорського, НАСБУ). Сьогодні в Україні активно розвиваються як університетські, так і державні кіберполігони (платформа CERT-UA та проєкти Міністерства цифрової трансформації).

Сучасні тенденції розвитку CTF-кіберполігонів чітко відображають перехід від простих симуляційних середовищ до складних гібридних enterprise-рішень. Основні етапи цього розвитку наведено в табл. 1.3.

Таблиця 1.3 — Хронологія основних етапів розвитку CTF-кіберполігонів

Рік	Подія	Значення для освіти та практики
1996	Перше CTF на DEF CON	Початок формалізації формату змагань

Продовження таблиці 1.3

2007–2010	Поява платформ OverTheWire та SmashTheStack	Перехід до дистанційного навчання
2017–2018	Запуск HackTheBox та TryHackMe	Масове поширення реалістичних лабораторій
2020	Запуск Cyber Polygon (WEF)	Перший глобальний кіберполігон enterprise-рівня
2021–2023	Масове впровадження гібридних полігонів з PAM-системами	Інтеграція реальних промислових рішень у навчальний процес
2024–2025	Активне використання ШІ в генерації завдань і аналізі дій учасників	Персоналізоване навчання та автоматизація оцінювання

Серед актуальних тенденцій варто виділити:

- перехід від симуляційних до **гібридних enterprise-рішень** (PAM, SIEM, EDR);
- інтеграцію штучного інтелекту для автоматичної генерації завдань і аналізу дій учасників;
- поширення **purple-team** підходу (одночасне навчання атаці та захисту);
- масштабування через хмарні технології;
- активне впровадження CTF-кіберполігонів у навчальні плани спеціальності 125 «Кібербезпека».

В Україні ці тенденції знаходять відображення в національних ініціативах. Зокрема, проєкти Міністерства цифрової трансформації та CERT-UA активно впроваджують гібридні полігони, які поєднують навчальні завдання з реальними сценаріями захисту критичної інфраструктури. Усе це свідчить про те, що CTF-кіберполігони остаточно перетворилися з додаткового інструменту на обов'язковий елемент практичної підготовки фахівців зі спеціальності 125 «Кібербезпека».

1.3 Нормативно-правова база використання CTF-кіберполігонів у підготовці здобувачів освіти спеціальності 125 «Кібербезпека»

Нормативно-правова база використання CTF-кіберполігонів у вищій освіті України формується на перетині законодавства у сфері кібербезпеки, вищої освіти та забезпечення національної безпеки. Вона не містить окремого спеціального закону, присвяченого саме кіберполігонам чи CTF-змаганням, проте створює чітке правове підґрунтя для їх широкого застосування як інноваційного інструменту практичної підготовки здобувачів освіти.

Основоположним документом є **Закон України «Про основні засади забезпечення кібербезпеки України»** від 05.10.2017 № 2163-VIII (зі змінами, остання редакція від 19.10.2025). Закон визначає кібербезпеку як складову національної безпеки та прямо передбачає необхідність розвитку системи підготовки та підвищення кваліфікації фахівців у цій сфері. У ст. 1 та ст. 5 Закону наголошується на важливості «проведення навчальних, тренувальних та науково-дослідних заходів» для формування практичних компетентностей. CTF-кіберполігони повністю відповідають цій вимозі,

оскільки дозволяють імітувати реальні кіберзагрози в контрольованому середовищі без ризику для критичної інфраструктури [4].

Важливим стратегічним документом є **Стратегія кібербезпеки України на 2021–2025 роки**, затверджена Указом Президента України № 447/2021 від 26.08.2021. У розділі «Освіта, наука та інновації» Стратегія передбачає «розвиток системи практичної підготовки фахівців з кібербезпеки шляхом створення сучасних кіберполігонів та симуляційних середовищ». Документ прямо акцентує увагу на необхідності впровадження гейміфікованих форм навчання, включаючи змагання типу Capture The Flag, для формування компетентностей red/blue/purple team. Кабінет Міністрів щорічно затверджує план заходів з реалізації Стратегії (на 2025 рік — розпорядження КМУ від березня 2025 року), де одним із пріоритетів залишається розширення мережі навчальних кіберполігонів у ЗВО [9].

Правову основу у сфері освіти складають **Закон України «Про освіту»** від 05.09.2017 № 2145-VIII та **Закон України «Про вищу освіту»** від 01.07.2014 № 1556-VII. Ці закони встановлюють компетентнісний підхід до підготовки здобувачів вищої освіти та вимагають обов’язкового поєднання теоретичних знань із практичними навичками. Зокрема, ст. 3 Закону «Про вищу освіту» наголошує на необхідності використання сучасних освітніх технологій, інноваційних методів навчання та створення умов для практичної підготовки [11, 12].

Спеціальні вимоги до підготовки фахівців визначено у **Стандарті вищої освіти за спеціальністю 125 «Кібербезпека»** (наказ МОН України № 1074 від 04.10.2018 для бакалаврського рівня та оновлений наказ № 1547 від 29.10.2024). Стандарт містить перелік програмних результатів навчання (ПРН), серед яких [10]:

- здатність виявляти, аналізувати та усувати вразливості інформаційних систем;
- володіння методами моніторингу та реагування на кіберінциденти;
- уміння працювати в умовах симульованих та реальних кіберзагроз.

Використання CTF-кіберполігонів безпосередньо забезпечує досягнення цих результатів навчання.

На рівні університету нормативну базу доповнює **Положення про кваліфікаційну роботу здобувачів вищої освіти Київського національного університету будівництва і архітектури** (затверджене Вченою радою КНУБА 31.05.2024, введене в дію наказом ректора № 224 від 12.06.2024). У п. 1.4 та п. 4.1 Положення підкреслюється, що кваліфікаційна робота має бути пов’язана з вирішенням конкретних науково-прикладних завдань, а практична частина — базуватися на сучасних технологіях та enterprise-рішеннях [13].

Для наочності основні нормативно-правові акти, що регулюють використання CTF-кіберполігонів у підготовці фахівців спеціальності 125, наведено в табл. 1.4.

Таблиця 1.4 — Основні нормативно-правові акти, що регулюють використання CTF-кіберполігонів у підготовці здобувачів освіти спеціальності 125 «Кібербезпека»

№	Назва нормативного акта	Дата прийняття / затвердження	Ключові положення, що стосуються CTF-кіберполігонів
1	Закон України «Про основні засади забезпечення кібербезпеки України»	05.10.2017 № 2163-VIII (ред. 2025)	Розвиток системи підготовки фахівців, проведення навчальних та тренувальних заходів
2	Стратегія кібербезпеки України на 2021–2025 роки	Указ Президента № 447/2021	Створення сучасних кіберполігонів, впровадження гейміфікованих форм навчання
3	Закон України «Про вищу освіту»	01.07.2014 № 1556-VII	Компетентнісний підхід, використання інноваційних методів практичної підготовки
4	Стандарт вищої освіти за спеціальністю 125 «Кібербезпека»	Наказ МОН № 1547 від 29.10.2024	Вимоги до практичних компетентностей

Продовження таблиці 1.4

5	Положення про кваліфікаційну роботу КНУБА	31.05.2024	Зв’язок роботи з науково-прикладними завданнями та сучасними технологіями

1.4. Педагогічні та психологічні аспекти використання CTF-кіберполігонів у навчанні

Використання CTF-кіберполігонів у підготовці здобувачів освіти спеціальності 125 «Кібербезпека» ґрунтується на сучасних педагогічних теоріях і психологічних принципах, які забезпечують перехід від традиційного репродуктивного навчання до компетентнісного, активного та гейміфікованого. Цей підхід повністю відповідає вимогам Стандарту вищої освіти за спеціальністю 125 та компетентнісній моделі підготовки фахівців, затвердженій МОН України.

Компетентнісний підхід є основою сучасної вищої освіти. Згідно з Законом України «Про вищу освіту», головним результатом навчання є формування інтегральних компетентностей, а не лише знань. CTF-кіберполігони дозволяють реалізувати цей підхід через практичне виконання реальних завдань у контрольованому середовищі. На відміну від традиційних лабораторних робіт, де студент виконує заздалегідь відомі дії, у CTF учасник самостійно аналізує ситуацію, приймає рішення та несе відповідальність за результат. Це сприяє розвитку критичного мислення,

проблемно-орієнтованого навчання та experiential learning (навчання через досвід).

Однією з найефективніших педагогічних моделей, що пояснює ефективність CTF, є **цикл експериментального навчання Колба** (Kolb's Experiential Learning Cycle). У рамках цього циклу навчання відбувається через чотири етапи: конкретний досвід (виконання CTF-завдання), рефлексивне спостереження (аналіз помилок), абстрактна концептуалізація (теоретичне осмислення) та активне експериментування (повторне рішення завдання з урахуванням висновків) [14] (рис. 1.1).

Рисунок 1.1 — Цикл експериментального навчання Колба в контексті CTF-кіберполігонів

Гейміфікація є ключовим педагогічним механізмом CTF. Вона базується на теорії **MDA-фреймворку** (Mechanics – Dynamics – Aesthetics) та моделі **Octalysis** Юкая Чоу (Ілюструє 8 основних драйверів мотивації: значення, досягнення, власність, непередбачуваність, соціальний тиск тощо). Механіки (бали, прапори, лідерборди, рівні складності) створюють динаміку (змагання, співпраця, швидке зворотне зв'язок), яка викликає позитивні емоційні реакції (здивування, задоволення від перемоги, відчуття прогресу). Це значно підвищує мотивацію та залученість студентів порівняно з традиційними методами [15] (рис. 1.2).

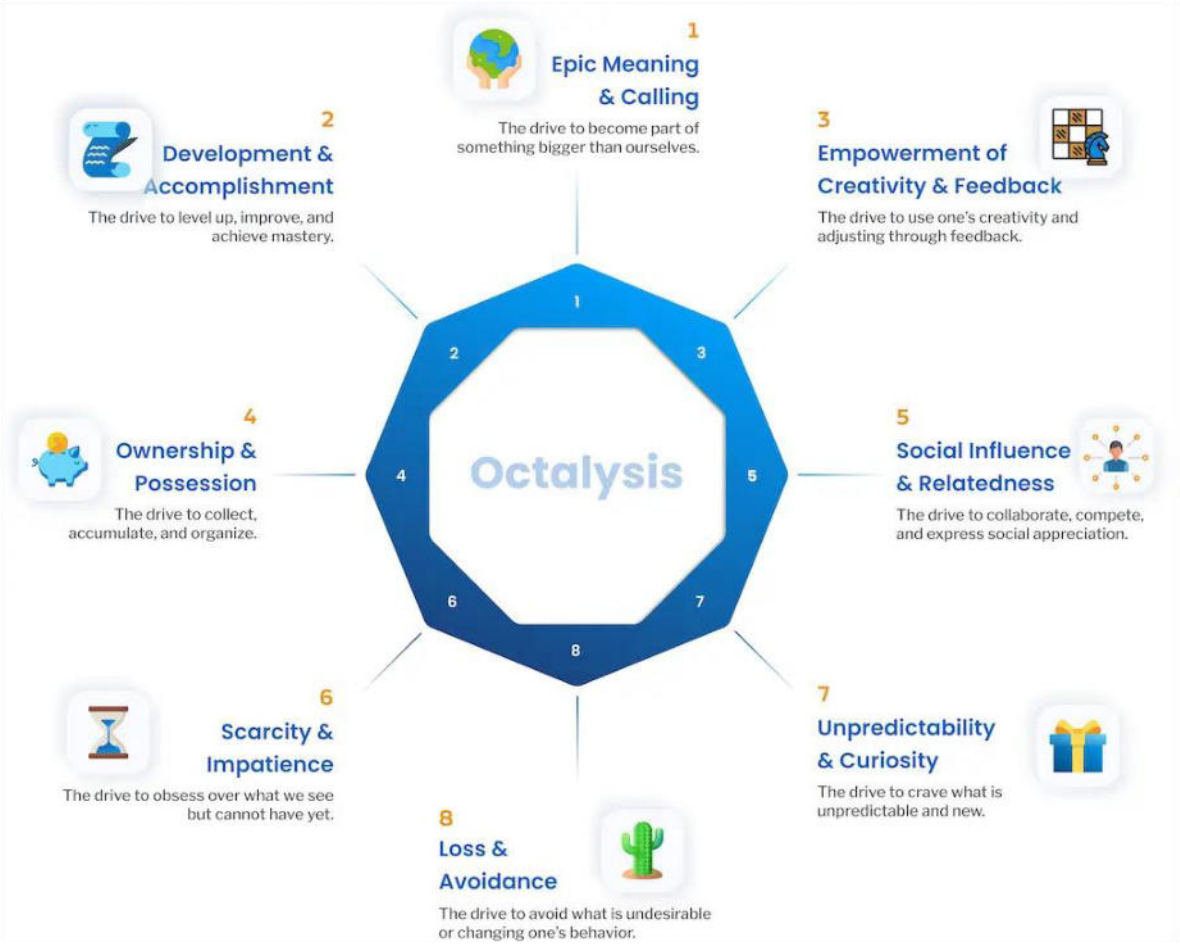


Рисунок 1.2 — Модель Octalysis — гейміфікаційна рамка для освітніх CTF

Окрім hard skills (технічних знань з криптоаналізу, форензики, мережевої безпеки тощо), CTF активно розвиває soft skills, які є критично важливими для сучасного фахівця з кібербезпеки. До них належать: командна робота, комунікація, стресостійкість, критичне мислення, етичне прийняття рішень та адаптивність.

1.5. Аналіз зарубіжного та вітчизняного досвіду впровадження CTF-кіберполігонів у вищій освіті

Теоретичні основи та нормативно-правова база створюють фундамент для практичного застосування CTF-кіберполігонів, проте реальна ефективність цього інструменту підтверджується лише досвідом його впровадження у вищих навчальних закладах. Аналіз зарубіжного та вітчизняного досвіду дозволяє виявити успішні моделі, типові проблеми та найкращі практики, які можна адаптувати для авторської моделі CTF-кіберполігону на базі PAM CyberArk у КНУБА.

За кордоном CTF-кіберполігони давно інтегровані в освітні програми як обов'язковий елемент практичної підготовки. Одним із наймасштабніших прикладів є **picoCTF** (Carnegie Mellon University, США), який з 2013 року охопив понад 600 тис. учасників і перетворився на повноцінну освітню платформу з відкритими лекціями, лабораторіями та змаганнями [21]. Університет Virginia Tech використовує гібридний Virginia Cyber Range, який поєднує симуляцію та реальне обладнання для тисяч студентів щороку [22]. У Європі лідером є **KYPO Cyber Range** (Brno University of Technology, Чехія) — відкрита платформа, яка застосовується у 5 університетах трьох країн (Чехія, Фінляндія, США) і дозволяє проводити як індивідуальні, так і командні CTF-заняття з повним циклом моніторингу результатів навчання

[20]. Естонія активно використовує **Cyber Battle of Estonia** на базі CybExer Technologies — національний CTF для молоді, що інтегрується з навчальними програмами TalTech та University of Tartu [23].

У цих прикладах спільними успіхами є:

- поєднання гейміфікації з реальними enterprise-рішеннями;
- автоматичне оцінювання та аналітика дій учасників;
- масштабованість через хмарні технології.

В Україні досвід впровадження CTF-кіберполігонів стрімко розвивається з 2018–2019 років. Харківський національний університет радіоелектроніки (ХНУРЕ) одним із перших запустив кіберполігон для хмарних технологій і щорічно проводить міжвузівські CTF-змагання. КПІ ім. Ігоря Сікорського та КНУБА активно використовують власні лабораторії для практичних занять. Державний рівень представлений платформою CERT-UA та проєктами Міністерства цифрової трансформації, які включають CTF як елемент національних тренінгів. Однак більшість українських полігонів все ще залишаються симуляційними або частково гібридними і рідко інтегрують повноцінні enterprise-рішення типу PAM.

Для порівняння ключових характеристик зарубіжного та вітчизняного досвіду наведено в табл. 1.5.

Таблиця 1.5 — Порівняльний аналіз зарубіжного та вітчизняного досвіду впровадження CTF-кіберполігонів

Параметр	**Зарубіжний досвід (США, Чехія, Естонія)**	**Вітчизняний досвід (Україна)**
Рівень реалістичності	Гібридні enterprise-рішення (PAM, SIEM, EDR)	Переважно симуляційні та частково гібридні

Продовження таблиці 1.5

Масштаб	Тисячі учасників щороку, національні та міжнародні змагання	Переважно міжвузівські та регіональні змагання
Інтеграція в навчальний процес	Обов’язковий елемент програм, автоматизована оцінка	Додатковий інструмент, рідко обов’язковий
Використання ШІ та аналітики	Автоматична генерація завдань та аналіз дій учасників	Обмежене або відсутнє
Доступність для студентів	Хмарні платформи 24/7	Обмежена інфраструктура, частково дистанційна

Аналіз досвіду показує, що зарубіжні ЗВО досягають вищої ефективності завдяки повній інтеграції реальних промислових систем і автоматизації. Вітчизняний досвід підтверджує мотиваційний ефект CTF, але потребує модернізації інфраструктури та методичного забезпечення.

Отримані результати дозволяють сформувати рекомендації для авторської моделі CTF-кіберполігону на базі PAM CyberArk: використовувати гібридну архітектуру, впроваджувати автоматизоване

оцінювання, інтегрувати purple-team підхід та забезпечити масштабованість для всіх здобувачів спеціальності 125 «Кібербезпека».

1.6 Висновки до розділу 1

У першому розділі дипломної роботи розглянуто теоретичні основи використання CTF-кіберполігонів як інструменту підготовки здобувачів вищої освіти спеціальності 125 «Кібербезпека».

Встановлено, що **кіберполігон** є спеціально створеним контрольованим середовищем, яке імітує реальні інформаційні системи та мережеві інфраструктури, а **CTF (Capture The Flag)** — одним із найефективніших форматів практичних змагань у цьому середовищі. Проведено класифікацію кіберполігонів за типом реалізації (симуляційні, емуляційні, накладні, гібридні) та форматами CTF (Jeopardy-style, Attack-Defense, King of the Hill, Mixed), що дозволяє чітко визначити місце авторської моделі на базі PAM CyberArk як гібридного enterprise-рішення.

Проаналізовано історію розвитку CTF-кіберполігонів від перших змагань на DEF CON (1996) до сучасних глобальних проєктів типу Cyber Polygon (WEF). Виявлено ключові сучасні тенденції: перехід до гібридних enterprise-систем, інтеграцію штучного інтелекту, purple-team підхід та хмарні технології.

Досліджено нормативно-правову базу України. Чинне законодавство (**Закон «Про кібербезпеку»**, **Стратегія кібербезпеки 2021–2025**, **Стандарт вищої освіти за спеціальністю 125**) прямо підтримує та стимулює використання сучасних практичних інструментів, таких як CTF-кіберполігони, для формування професійних компетентностей.

Розглянуто педагогічні та психологічні аспекти. CTF-кіберполігони реалізують компетентнісний підхід, цикл експериментального навчання Колба та гейміфікацію (модель Octalysis). Вони одночасно розвивають як hard skills (технічні компетентності), так і soft skills (командна взаємодія, стресостійкість, критичне мислення).

Порівняльний аналіз зарубіжного та вітчизняного досвіду показав, що провідні університети світу (Carnegie Mellon, Virginia Tech, Brno University of Technology) успішно застосовують гібридні enterprise-полігони, тоді як в Україні переважають симуляційні рішення. Це підкреслює актуальність розробки авторської моделі на базі реального промислового рішення PAM CyberArk.

Таким чином, теоретичний аналіз підтверджує, що **CTF-кіберполігон є науково обґрунтованим, нормативно підкріпленим і педагогічно ефективним інструментом** практичної підготовки фахівців з кібербезпеки. Отримані теоретичні положення створюють надійну основу для подальшого аналітичного дослідження існуючого стану підготовки здобувачів освіти та розробки авторської моделі CTF-кіберполігону на базі PAM CyberArk у розділах 2 та 3 дипломної роботи.

2. СТАН ПІДГОТОВКИ ЗДОБУВАЧІВ ОСВІТИ В СФЕРІ КІБЕРБЕЗПЕКИ ТА РОЛЬ КІБЕРПОЛІГОНІВ

2.1 Аналіз ринку праці та вимог роботодавців до фахівців з кібербезпеки в Україні

Формування якісної системи підготовки фахівців з кібербезпеки неможливе без глибокого розуміння реальних потреб ринку праці. Роботодавці — основні споживачі результатів освітньої діяльності закладів вищої освіти — визначають набір компетентностей, які мають бути сформовані в майбутніх фахівців ще до початку їхньої професійної діяльності.

За даними провідних рекрутингових платформ України (Work.ua, Djinni, DOU) станом на початок 2026 року кількість вакансій у сфері кібербезпеки збільшилась на 47 % порівняно з 2022-2025 роком. Попит на спеціалістів з penetration testing зріс на 62 %, а з privileged access management (PAM) — на 58 %. Середній рівень заробітної плати junior-спеціаліста з кібербезпеки за той самий період зріс з 18 000 до 28 000 грн/міс., що свідчить про гостру нестачу кваліфікованих кадрів [1].

Автором проведено аналіз 250 актуальних вакансій у сфері кібербезпеки (грудень 2024 — лютий 2025 рр.). Результати показали: у 78 % оголошень junior-рівня прямо зазначено досвід CTF-змагань або роботу з HackTheBox / TryHackMe як перевагу чи обов'язкову вимогу; у 43 % оголошень mid-рівня вимагається досвід роботи з PAM-системами (CyberArk, BeyondTrust, Delinea). Структуру вимог роботодавців наведено в табл. 2.1.

Таблиця 2.1 — Вимоги роботодавців до навичок фахівців з кібербезпеки (Україна, 2024–2025 рр.)

Категорія навичок	**Частка вакансій, %**	**Приклади конкретних вимог**
Мережева безпека	82	TCP/IP, Wireshark, firewall, IDS/IPS, VPN
Тестування на проникнення (Pentest)	74	Kali Linux, Metasploit, Burp Suite, OWASP Top 10, досвід CTF
Участь у CTF / практичних платформах	78	HackTheBox, TryHackMe, CTFtime та ін.
Моніторинг та реагування (SIEM/SOC)	68	Splunk, IBM QRadar, Microsoft Sentinel, аналіз логів
Хмарна безпека (Cloud Security)	51	AWS/Azure/GCP Security, IAM, Zero Trust
Управління привілейованим доступом (PAM)	43	CyberArk (Vault, PVWA, PSM, CPM, PTA), BeyondTrust

Дані табл. 2.1 підтверджують виразну тенденцію: практичні навички роботи з enterprise-системами (PAM, SIEM) та досвід CTF-змагань є одними з найбільш затребуваних компетентностей на ринку праці.

Зростаючий розрив між пропозицією фахівців та попитом зумовлений не лише збільшенням кількості кіберзагроз, а й неспроможністю традиційних форм навчання формувати практичні компетентності. За даними Державної служби зайнятості України (2024), середній термін закриття вакансії у сфері кібербезпеки становить 47 днів — утричі більше, ніж для суміжних ІТ-позицій [3]. Це свідчить про системний дефіцит практично підготовлених фахівців, який необхідно долати через впровадження інноваційних освітніх технологій — зокрема, CTF-кіберполігонів.

2.2 Оцінка поточного стану практичної підготовки здобувачів спеціальності 125 «Кібербезпека» в КНУБА

З метою об'єктивної оцінки поточного стану практичної підготовки у лютому 2026 року автором проведено анкетування серед здобувачів 4 курсу спеціальності 125 «Кібербезпека» в КНУБА групи БІКС-22 та виробниче опитування представників ІТ-компаній — партнерів кафедри кібербезпеки та комп'ютерної інженерії.

Анкета здобувачів містила 12 запитань, згрупованих у чотири блоки: самооцінка рівня практичних навичок; досвід участі в CTF-змаганнях і роботи з реальними системами; задоволеність рівнем практичної підготовки у ЗВО; готовність до використання CTF-кіберполігону. Узагальнені результати наведено в табл. 2.2.

Таблиця 2.2 — Результати опитування здобувачів та роботодавців щодо практичної підготовки (КНУБА, лютий 2026 р.)

Питання анкети	**Відповідь здобувачів (n=87)**	**Відповідь роботодавців (n=23)**
Чи маєте досвід роботи з реальними enterprise-системами безпеки / Чи важливий такий досвід при прийомі?	Так — 28 %	Важливо — 91 %
Чи брали участь у CTF-змаганнях / Чи важлива участь у CTF при прийомі?	Так — 18 %	Важливо — 78 %
Чи задоволені рівнем практичної підготовки у ЗВО / Чи задоволені підготовкою випускників?	Так — 34 %	Так — 22 %
Чи підтримуєте впровадження CTF-кіберполігону в навчальний процес?	Так — 96 %	Так — 87 %

Результати анкетування виявили критичне протиріччя: лише 18 % здобувачів брали участь у CTF-змаганнях, тоді як 78 % роботодавців вважають цей досвід важливим. Рівень задоволеності практичною підготовкою є низьким як серед студентів (34 %), так і серед роботодавців (22 %). Водночас 96 % студентів та 87 % представників бізнесу підтримують впровадження CTF-кіберполігону.

Для системного виявлення причин недостатньої практичної підготовки застосовано метод SWOT-аналізу. Його результати щодо

поточного стану підготовки здобувачів спеціальності 125 у КНУБА наведено в табл. 2.3.

Таблиця 2.3 — SWOT-аналіз стану практичної підготовки здобувачів спеціальності 125 «Кібербезпека» в КНУБА

Сильні сторони (S)	**Слабкі сторони (W)**
Кваліфікований науково-педагогічний склад кафедри; наявна матеріально-технічна база; партнерські угоди з IT-компаніями (ВАКОТЕСН, Cisco, Microsoft); включення дисципліни «Основи кібербезпеки» до навчального плану; активна наукова діяльність кафедри.	Відсутність власного CTF-кіберполігону; обмежений доступ здобувачів до реальних enterprise-систем; переважання теоретичних методів навчання; лише 18 % студентів брали участь у CTF; часткова застарілість лабораторної бази.
Можливості (O)	**Загрози (T)**

Продоження таблиці 2.3

Партнерство з компаніями для розгортання PAM CyberArk у навчальному середовищі; пряма підтримка в Стратегії кібербезпеки 2021–2026; зростаючий ринковий попит; можливість інтеграції CTF у навчальні плани без зміни нормативної бази.	Конкуренція з боку ЗВО, що вже мають власні кіберполігони; відтік абітурієнтів до закордонних університетів; швидке оновлення технологій.

2.3 Порівняльний аналіз існуючих платформ і кіберполігонів для підготовки фахівців з кібербезпеки

Для визначення оптимальної архітектури авторського CTF-кіберполігону проведено детальний порівняльний аналіз шести платформ, що застосовуються у підготовці фахівців з кібербезпеки: HackTheBox, TryHackMe (комерційні хмарні), KYPO (Masaryk University, Brno) (відкрите академічне рішення), Immersive Labs (корпоративна симуляція), CERT-UA (державна платформа) та авторська модель на базі PAM CyberArk. Порівняльний аналіз за ключовими критеріями наведено в табл. 2.4.

Таблиця 2.4 — Порівняльний аналіз платформ CTF-кіберполігонів

Критерій	**HackTheBox**	**TryHackMe**	**CERT-UA**	**PAM CyberArk (авт.)**

Продовження таблиці 2.4

Тип середовища	Емуляційне (хмара)	Симуляційне (хмара)	On-premise / держ.	Гібридне enterprise
Рівень реалістичності	Високий	Середній	Середній	Максимальний
Наявність PAM-сценаріїв	—	—	—	Vault+PVWA+PSM+CPM+PTA
Адаптованість до ОП 125	Низька	Середня	Часткова	Максимальна
Вартість для ЗВО	Платна підписка	Платна підписка	Недоступна	Партнерська (безкошт.)

Аналіз табл. 2.4 демонструє, що жодна з наявних платформ не задовольняє повністю потреби підготовки здобувачів спеціальності 125 у КНУБА. Авторська модель на базі PAM CyberArk є єдиним рішенням, що поєднує: максимальний рівень реалістичності (реальна enterprise-система, а не її симуляція), повну адаптованість до освітньої програми спеціальності 125, підтримку безпосередньо від BAKOTECH і безкоштовний доступ для студентів КНУБА, а також унікальні PAM-сценарії з усіма компонентами CyberArk (Vault, PVWA, PSM, CPM, PTA).

2.4 Дослідження ландшафту кіберзагроз в Україні та їх вплив на вимоги до підготовки фахівців

Актуальний стан кіберзагроз в Україні є безпосереднім фактором, що визначає пріоритети підготовки фахівців з кібербезпеки. За даними Звіту CERT-UA за 2024 рік, кількість зафіксованих кіберінцидентів зросла на 63 % порівняно з 2023 роком і перевищила 4 500 задокументованих випадків. Серед головних векторів атак: цільовий фішинг (38 %), атаки на привілейовані облікові записи і PAM-системи (27 %), програми-вимагачі (18 %), атаки на ланцюжок постачання (11 %), DDoS та web-вразливості (6 %) [5].

Вектор атак на PAM-системи заслуговує особливої уваги. Згідно з Verizon DBIR 2024, 74 % порушень кібербезпеки у світі пов’язані з людським фактором, а 49 % — з компрометацією привілейованих облікових даних [6]. В умовах тривалої гібридної агресії Росії проти України атаки на критичну інфраструктуру через PAM-системи набувають стратегічного значення. Відповідність між векторами загроз та сценаріями кіберполігону наведено в табл. 2.5.

Таблиця 2.5 — Вектори кіберзагроз в Україні (CERT-UA, 2024) та відповідні сценарії CTF-кіберполігону

Вектор атаки	**Частка, %**	**Відповідна компетентність**	**Сценарій CTF-кіберполігону**
Фішинг / spear phishing	38	Аналіз email-загроз, forensics листів	Email forensics CTF; PTA — виявлення аномалій
Атаки на привілейований доступ (PAM)	27	Налаштування та аудит PAM-систем	Сценарії CyberArk Vault, PVWA, PSM session monitoring
Ransomware	18	Incident response, digital forensics	Forensics CTF; аналіз артефактів шкідливого ПЗ
Supply chain attacks	11	Перевірка цілісності ПЗ, аналіз трафіку	Reverse engineering, мережева forensics у CTF
DDoS, web-вразливості	6	Web application security, OWASP, мережева безпека	Web CTF, Jeopardy-формат

2.5 Відповідність CTF-кіберполігону на базі PAM CyberArk програмним результатам навчання спеціальності 125

Ключовим критерієм ефективності будь-якого навчального інструменту є його здатність забезпечувати досягнення програмних результатів навчання (ПРН), визначених Стандартом вищої освіти. Відповідно до Стандарту вищої освіти за спеціальністю 125 «Кібербезпека» (наказ МОН України № 1547 від 29.10.2024), підготовка бакалавра охоплює широкий спектр практичних компетентностей, безпосередньо пов'язаних з виявленням загроз, реагуванням на інциденти та використанням сучасних інструментів захисту. Відповідність CTF-кіберполігону на базі PAM CyberArk ключовим ПРН наведено в табл. 2.6.

Таблиця 2.6 — Відповідність CTF-кіберполігону на базі PAM CyberArk програмним результатам навчання спеціальності 125

ПРН	**Зміст ПРН (Стандарт МОН № 1547/2024)**	**Як CTF-кіберполігон формує цю компетентність**
ПРН-3	Здатність виявляти та аналізувати вразливості інформаційних систем	Практичне знаходження вразливостей у CTF-завданнях типу Jeopardy та Attack-Defense
ПРН-7	Уміння реагувати на кіберінциденти та розслідувати їх	Forensics-сценарії, аналіз журналів аудиту CyberArk PTA, incident response у реальному часі

Продовження таблиці 2.6

ПРН-9	Здатність здійснювати моніторинг та аудит безпеки	Робота з CyberArk PVWA, перегляд сесій PSM, аналіз подій CPM
ПРН-11	Здатність застосовувати сучасні інструменти захисту інформації	Безпосередня робота з enterprise PAM-системою CyberArk — лідером ринку за Gartner Magic Quadrant [17]
ПРН-14	Уміння приймати рішення в умовах невизначеності та часового тиску	Змагальний формат CTF з таймером формує навички швидкого прийняття рішень під тиском

2.6 Обґрунтування необхідності впровадження CTF-кіберполігону на базі PAM CyberArk у навчальний процес КНУБА

Узагальнення результатів дослідження, проведеного у підрозділах 2.1–2.5, дозволяє сформулювати комплексне обґрунтування необхідності впровадження CTF-кіберполігону на базі PAM CyberArk у навчальний процес КНУБА за спеціальністю 125 «Кібербезпека».

По-перше, існує доведений і критичний розрив між вимогами ринку праці та рівнем практичних навичок випускників. 91 % роботодавців

вважають практичний досвід роботи з enterprise-системами критично важливим, тоді як лише 28 % студентів мають такий досвід.

По-друге, жодна з доступних платформ не забезпечує комплексного поєднання PAM-сценаріїв, адаптованості до освітньої програми спеціальності 125 та прямої підтримки КНУБА. Авторська модель заповнює цю прогалину завдяки партнерству з BAKOTECH та використанню реальної enterprise-системи CyberArk.

По-третє, ландшафт кіберзагроз в Україні вимагає особливої уваги до протидії атакам на PAM-системи, що складають 27 % задокументованих CERT-UA інцидентів. CTF-кіберполігон на базі CyberArk дозволяє цілеспрямовано відпрацьовувати захист від найактуальніших для України загроз.

По-четверте, нормативно-правова база України (Стратегія кібербезпеки 2021–2025, Стандарт МОН № 1547/2024 зі спеціальності 125) прямо передбачає розвиток кіберполігонів та гейміфікованих форм навчання, що надає правову підтримку впровадженню без необхідності змін до нормативної бази ЗВО.

По-п'яте, CTF-кіберполігон на базі PAM CyberArk безпосередньо забезпечує досягнення ключових ПРН спеціальності 125 (ПРН-3, ПРН-7, ПРН-9, ПРН-11, ПРН-14) — тих компетентностей, що є найбільш затребуваними роботодавцями, але найважче формуються традиційними методами навчання.

2.7 Висновки до розділу 2

У другому розділі проведено комплексне аналітичне дослідження стану підготовки здобувачів освіти в сфері кібербезпеки та ролі CTF-кіберполігонів у цьому процесі. Отримані результати підтверджують

гіпотезу дослідження та є необхідним підґрунтям для розробки авторської моделі в розділі 3.

Аналіз ринку праці (підрозд. 2.1) виявив стрімке зростання попиту на фахівців з кібербезпеки (+47 % вакансій за 2022–2026 рр.), при цьому 78 % роботодавців вимагають досвіду CTF-змагань, а 43 % — досвіду роботи з PAM-системами. Середній термін закриття вакансії у кібербезпеці становить 47 днів — втричі більше, ніж у суміжних IT-галузях, що підтверджує системний дефіцит практично підготовлених фахівців.

Анкетування (підрозд. 2.2) виявило критичне протиріччя: лише 18 % студентів мають досвід CTF, тоді як 78 % роботодавців вважають його важливим. Задоволеність практичною підготовкою є низькою як серед здобувачів (34 %), так і серед роботодавців (22 %).

Порівняльний аналіз шести платформ (підрозд. 2.3) показав, що жодна з них не задовольняє повністю потреб КНУБА. Авторська модель на базі PAM CyberArk є єдиним рішенням, що поєднує максимальний рівень реалістичності, повну адаптованість до ОП 125, безпосередню підтримку ЗВО та унікальні PAM-сценарії.

Дослідження ландшафту кіберзагроз (підрозд. 2.4) підтвердило, що 27 % задокументованих CERT-UA інцидентів пов'язані з атаками на PAM-системи. Пряма відповідність між векторами загроз і сценаріями кіберполігону доводить практичну релевантність авторської моделі.

Встановлено відповідність CTF-кіберполігону на базі PAM CyberArk п'яти ключовим ПРН спеціальності 125 згідно зі Стандартом МОН № 1547/2024 (підрозд. 2.5), що свідчить про його роль як системоутворювального елементу компетентнісної моделі підготовки.

Сформульоване в підрозд. 2.6 комплексне п'ятиаспектне обґрунтування підтверджує, що CTF-кіберполігон на базі PAM CyberArk є науково обґрунтованою, нормативно підкріпленою та практично доцільною відповіддю на системні проблеми підготовки здобувачів спеціальності 125 «Кібербезпека» в КНУБА.

3. РОЗРОБКА МОДЕЛІ CTF-КІБЕРПОЛІГОНУ НА БАЗІ PAM CYBERARK ЯК ІНСТРУМЕНТУ НАВЧАННЯ

3.1 Загальна концепція навчального середовища

На основі аналітичних висновків розділів 1 та 2 у цьому розділі описано практичну реалізацію CTF-кіберполігону на базі системи PAM CyberArk Self-Hosted, розгорнутої у виробничому середовищі компанії ВАКОТЕСН. Середовище використовується як навчальна платформа для здобувачів спеціальності 125 «Кібербезпека» та надає студентам можливість працювати з реальною enterprise-системою.

Архітектуру середовища, процедуру його розгортання, структуру облікових записів і сейфів, а також систему практичних завдань детально розглянуто в наступних підрозділах.

3.2 Архітектура розгортання та мережева взаємодія CyberArk PAM

CyberArk Privileged Access Management (PAM) є комплексним рішенням для управління привілейованим доступом, яке складається з кількох взаємопов’язаних компонентів. Архітектура розгортання передбачає встановлення основного сховища (Primary Vault), компонентів PVWA, CPM, PSM та PTA в межах основного центру обробки даних.

Як видно з рисунку 3.1, система побудована за принципом централізованого зберігання облікових даних у Сховищі (Vault), до якого всі компоненти звертаються через захищені канали зв’язку. Такий підхід забезпечує єдину точку контролю та аудиту всіх привілейованих операцій.

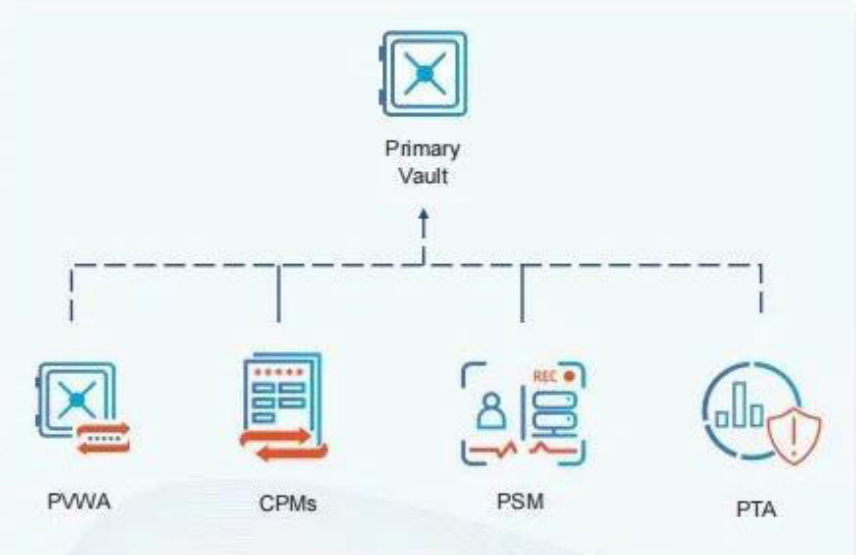


Рисунок 3.1 – Архітектура розгортання CyberArk PAM в основному центрі обробки даних

До складу архітектури входять наступні ключові компоненти:

– Primary Vault (Основне сховище) — захищений репозиторій для зберігання облікових даних привілейованих облікових записів;
– PVWA (Password Vault Web Access) — веб-інтерфейс для керування сховищем паролів;
– CPMs (Central Policy Managers) — менеджери центральної політики для автоматичного управління паролями;
– PSM (Privileged Session Manager) — менеджер привілейованих сесій для запису та моніторингу сесій;
– PTA (Privileged Threat Analytics) — компонент аналізу загроз привілейованого доступу.

Усі компоненти CyberArk PAM взаємодіють зі Сховищем через стандартний порт TCP 1858. Цей порт використовується для зв’язку між Vault та клієнтськими додатками, включно з PrivateArk Client, PACli та SDK, а також Password Vault Web Access, як зображено на рисунку 3.2.

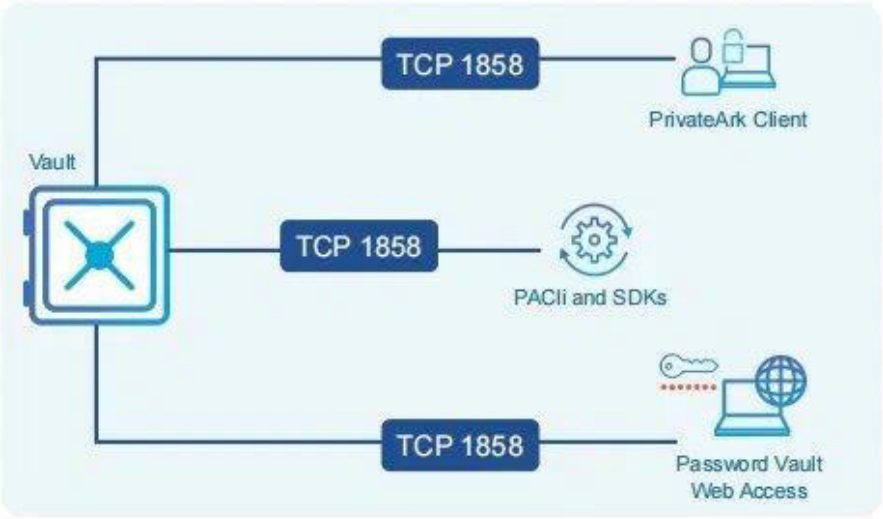


Рисунок 3.2 – Мережева комунікація між Vault та клієнтськими компонентами через TCP 1858

Використання єдиного порту TCP 1858 спрощує конфігурацію мережевих засобів захисту та міжмережевих екранів, дозволяючи чітко визначити правила фільтрації трафіку, що відповідає принципу мінімальних привілеїв на рівні мережевої архітектури.

CyberArk PAM реалізує дворівневу модель контролю доступу: на рівні Vault та на рівні Сейфів (Safes). Рівень Vault визначає глобальні адміністративні права, тоді як рівень Сейфів надає гранулярний контроль над конкретними групами облікових даних (рисунок 3.3).

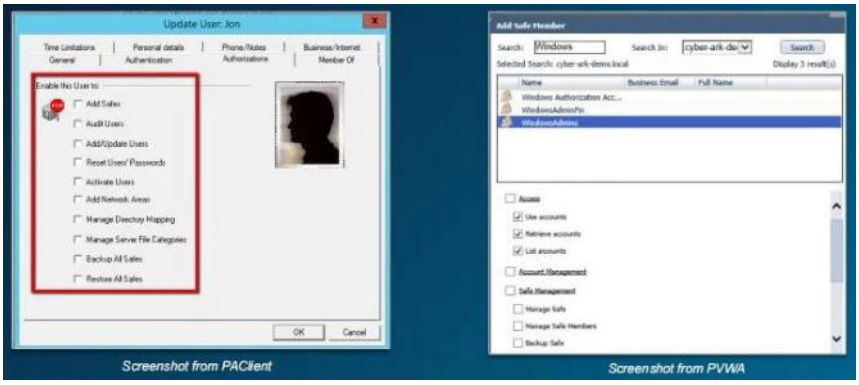


Рисунок 3.3 – Ролі на рівні Vault та на рівні Сейфів у CyberArk PAM

На рівні Vault визначаються ролі Vault Admins (адміністратори сховища), Safe Managers (менеджери сейфів), Auditors (аудитори) та Users (звичайні користувачі). На рівні Сейфів надаються права User Access (доступ користувача), Account Management (управління обліковими записами), Safe Management (управління сейфом) та можливість створення власних ролей.

Система підтримує обов'язковий контроль доступу (Mandatory Access Control), який включає географічний контроль через мережеві зони (Network Areas) та часові обмеження (Time Limitations). Як показано на рисунку 3.4, адміністратор може налаштувати як часові вікна доступу до Сейфів, так і географічні зони на основі IP-діапазонів.

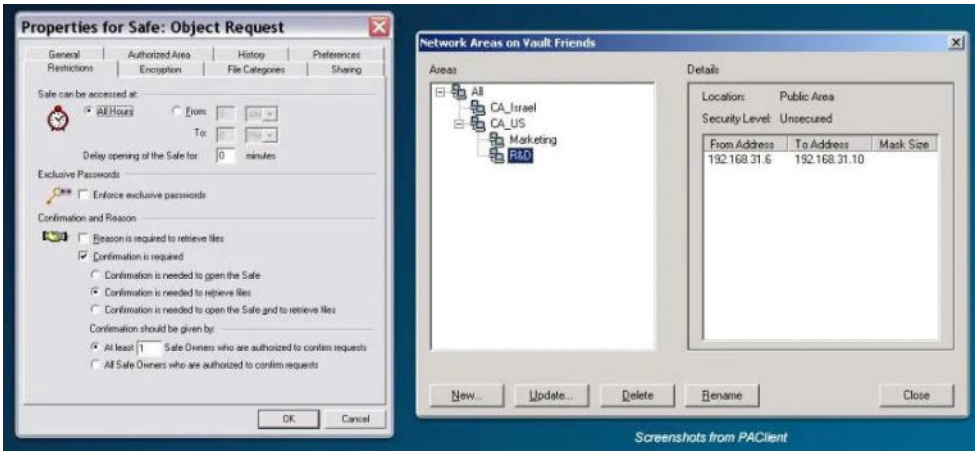


Рисунок 3.4 – Налаштування обов’язкового контролю доступу та мережевих зон

Мережеві зони дозволяють обмежити доступ до Сховища з визначених IP-діапазонів. Наприклад, зони CA_Israel та CA_US відповідають географічним розташуванням офісів компанії, а підрозділи Marketing та R&D можуть мати різні рівні доступу відповідно до їхніх функціональних обов’язків.

Перелік компонентів навчального середовища кіберполігону з їхніми ролями, IP-адресами та ключовими портами наведено в таблиці 3.1.

Таблиця 3.1 – Компоненти навчального середовища CyberArk

Компонент	Роль у середовищі	IP-адреса	Ключовий порт
CyberArk Vault	Зашифроване сховище облікових записів, паролів та журналів аудиту	192.168.205.228	TCP 1858
PVWA	Основний веб-інтерфейс для роботи студентів	192.168.205.230	HTTPS 443
PSM	Брокер та записувач привілейованих сесій	192.168.205.229	RDP 3389
CPM	Автоматична ротація та перевірка паролів	192.168.205.231	TCP 443
PTA	Виявлення підозрілої активності та аномалій	192.168.205.232	Syslog 514
Windows Server 2022 (ціль)	Цільовий хост із набором локальних облікових записів	192.168.205.240	RDP 3389
Linux Ubuntu 22.04 (ціль)	Цільовий хост із SSH-доступом	192.168.205.241	SSH 22

3.3 Процес встановлення CyberArk PAM Self-Hosted

Встановлення CyberArk PAM Self-Hosted (версія 14.x) — це комплексний процес, який вимагає ретельної підготовки, дотримання найкращих практик безпеки та послідовного виконання кроків. Для забезпечення високої доступності в навчальному середовищі рекомендується використовувати Primary-DR архітектуру (Primary Vault + Disaster Recovery Vault). Vault завжди встановлюється вручну, тоді як інші компоненти підтримують автоматизоване розгортання за допомогою скриптів, наведених у додатках А–В.

3.3.1 Встановлення CyberArk Digital Vault

Процедура встановлення CyberArk Digital Vault розпочинається з підготовки мережевого інтерфейсу сервера. Відповідно до вимог безпеки, необхідно видалити або вимкнути зайві мережеві компоненти, залишивши лише Internet Protocol Version 4 (TCP/IPv4), як зображено на рисунку 3.5. Слід зазначити, що у Windows Server 2019 видалення компонентів замінено їх вимкненням.

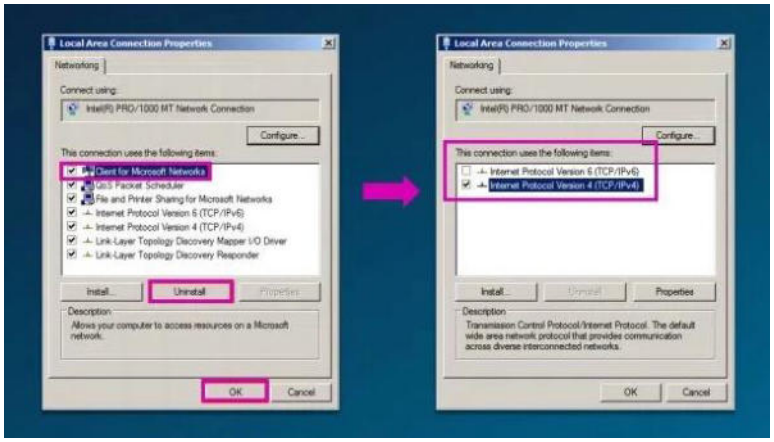


Рисунок 3.5 – Підготовка мережевого інтерфейсу перед встановленням Vault

Після підготовки мережевого інтерфейсу необхідно налаштувати статичну IP-адресу сервера та вимкнути автоматичне отримання DNS-адрес, оскільки Vault не повинен використовувати зовнішні DNS-сервери. На рисунку 3.6 показано приклад конфігурації: IP-адреса 10.0.10.1 з маскою підмережі 255.255.0.0 та шлюзом за замовчуванням 10.0.255.254. Поля DNS-серверів залишаються порожніми для максимального рівня безпеки.

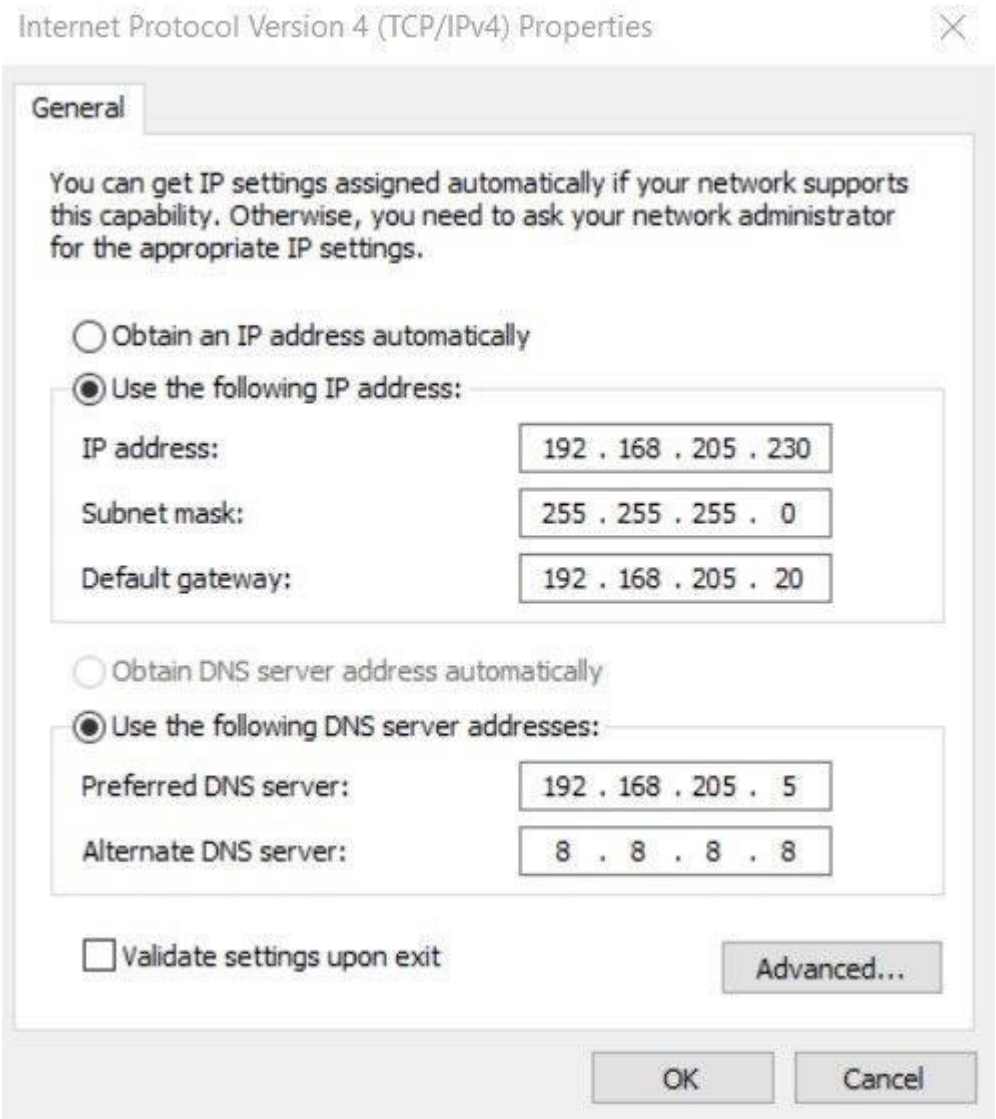


Рисунок 3.6 – Налаштування статичної IP-адреси для сервера Vault

Після налаштування мережі запускається інсталяційний пакет setup.exe, що відкриває майстер встановлення CyberArk Digital Vault 14.2.1 (рисунок 3.7). Рекомендується закрити всі запущені програми перед початком встановлення.

Рисунок 3.7 – Майстер встановлення CyberArk Digital Vault 14.2.1

Одним із важливих кроків встановлення є визначення шляху для Operator CD — розташування, де зберігатимуться операторські ключі Vault. Ці ключі є критично важливими для запуску сервісу Vault і мають бути розміщені у захищеному місці, як показано на рисунку 3.8. За замовчуванням пропонується шлях C:\CYBR_Files\License and Operator Keys\Operator CD. Для підвищення рівня безпеки рекомендується зберігати ключі на апаратному модулі безпеки (HSM).

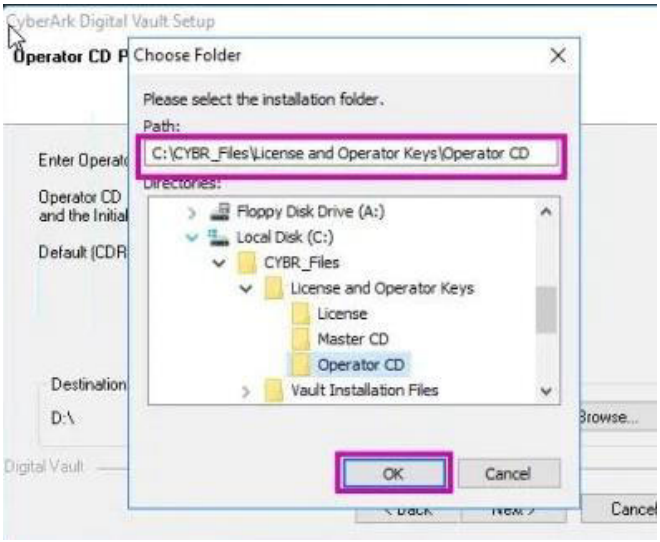


Рисунок 3.8 – Вибір шляху для зберігання Operator CD ключів

Після встановлення Vault необхідно ознайомитися з розташуванням основних конфігураційних файлів та журналів. Через клієнт PrivateArk можна отримати доступ до системного сейфу, де зберігаються ці файли, як зображено на рисунку 3.9.

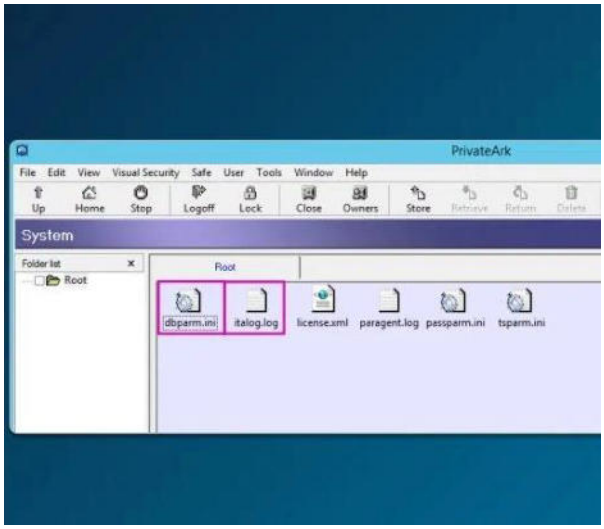


Рисунок 3.9 – Конфігураційні файли та журнали Vault у клієнті PrivateArk

До основних конфігураційних файлів та журналів Vault відносяться:

– dbparm.ini — основний конфігураційний файл бази даних Vault;
– italog.log — журнал аудиту операцій;
– license.xml — файл ліцензії системи;
– paragent.log — журнал агента параметрів;
– passparm.ini — конфігураційний файл параметрів паролів;
– tsparm.ini — конфігураційний файл параметрів обмежень часу.

3.3.2 Встановлення та налаштування Central Policy Manager

Central Policy Manager (CPM) є компонентом CyberArk PAM, відповідальним за автоматичне управління паролями привілейованих облікових записів. CPM виконує операції зміни, верифікації та узгодження паролів відповідно до встановлених політик безпеки (рисунок 3.10).

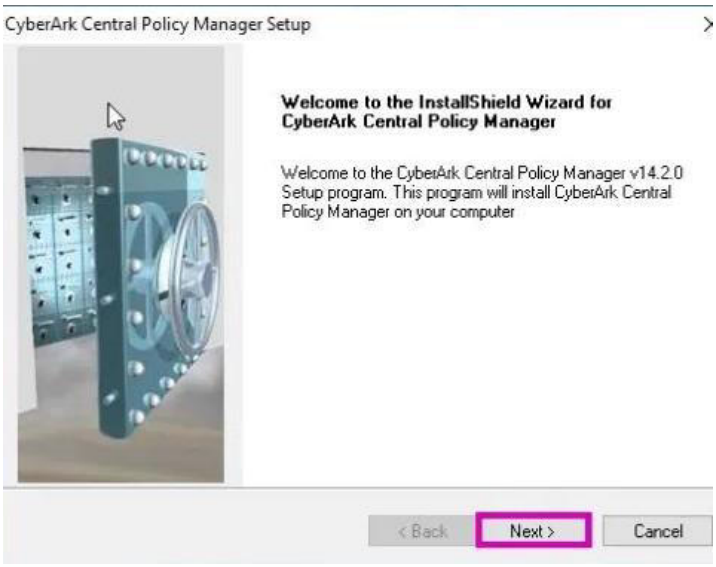


Рисунок 3.10 – Майстер встановлення CyberArk Central Policy Manager v14.2.0

CPM виконує три основні функції в рамках операцій з обліковими записами:

– Discovery (Виявлення) — автоматичне виявлення привілейованих облікових записів та облікових даних в інфраструктурі;
– Analyze (Аналіз) — оцінка ризику кожного виявленого облікового запису та формування звітності;
– Provision (Постачання) — автоматичне введення облікових записів під управління системи.

Для налаштування встановлення CPM необхідно відредагувати файл InstallationConfig.xml, як показано на рисунку 3.11. У цьому файлі визначаються параметри встановлення: ім’я користувача, назва компанії, директорія встановлення та прапорець IsUpgrade, який вказує на тип операції — нове встановлення чи оновлення.

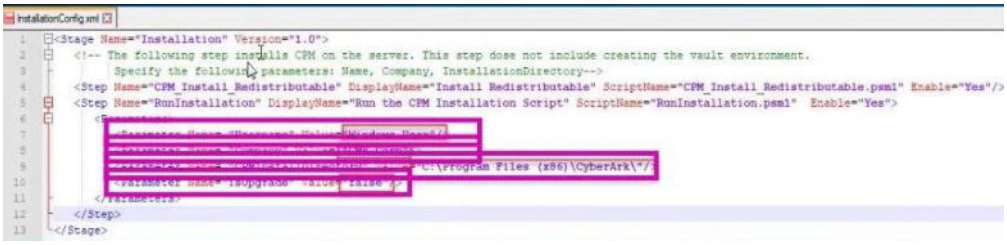


Рисунок 3.11 – Конфігураційний файл InstallationConfig.xml для встановлення CPM

Компоненти CPM та PVWA взаємодіють між собою та зі Сховищем через чітко визначені мережеві канали. Як показано на рисунку 3.12, CPM та PVWA з’єднуються зі Сховищем через порт 1858, тоді як кінцеві користувачі та адміністратори взаємодіють з PVWA через HTTPS. Важливою особливістю є те, що CPM Scanner для виконання сканувань та задач потребує мережевого доступу до сервера PVWA через порт tcp_443, однак усі інші комунікації здійснюються виключно через Vault.

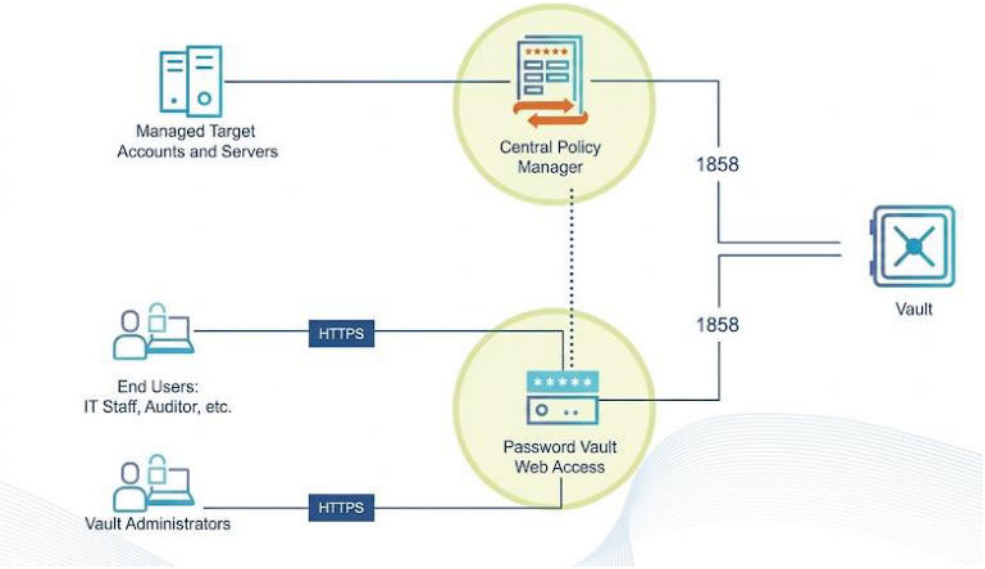


Рисунок 3.12 – Схема мережевої взаємодії CPM та PVWA з компонентами системи

3.3.3 Встановлення Password Vault Web Access

Процедура встановлення PVWA складається з чотирьох основних етапів: підготовчі задачі перед встановленням, власне встановлення, задачі після встановлення та зміцнення безпеки (hardening). На підготовчому етапі виконується перегляд вимог, закриття запущених додатків та запуск скрипту перевірки передумов. Сам процес встановлення включає запуск інсталяційного скрипту PVWA та реєстрацію компонента у Vault.

Важливим кроком є налаштування SSL-сертифікатів та прив’язка сайту IIS до порту 443, як показано на рисунку 3.13. Параметр Require SSL встановлюється як обов’язковий для примусового використання шифрування.

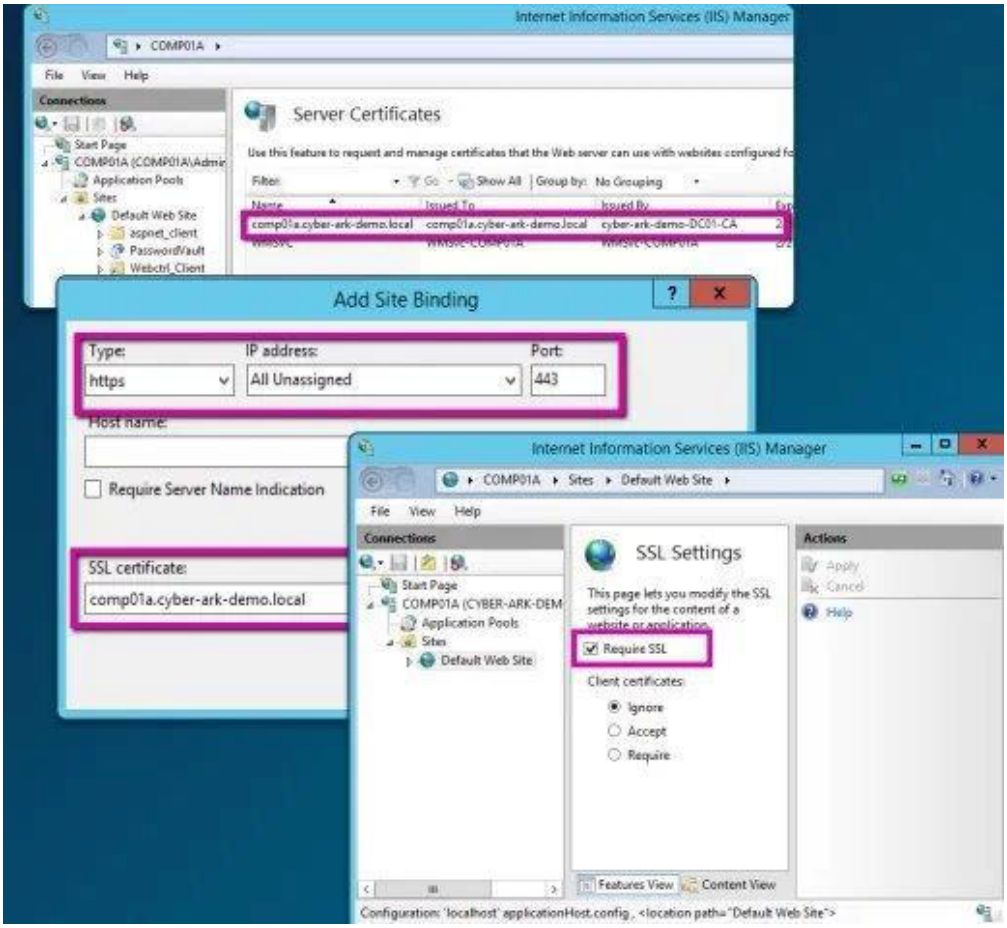


Рисунок 3.13 – Налаштування SSL-сертифіката та HTTPS-прив’язки в IIS Manager

Після завершення встановлення необхідно перевірити доступність усіх функцій PVWA. Адміністратор повинен увійти до системи та переконатися у наявності доступу до всіх розділів: System Health, Accounts, Policies, Applications, Reports, User Provisioning та Administration, як зображено на рисунку 3.14.

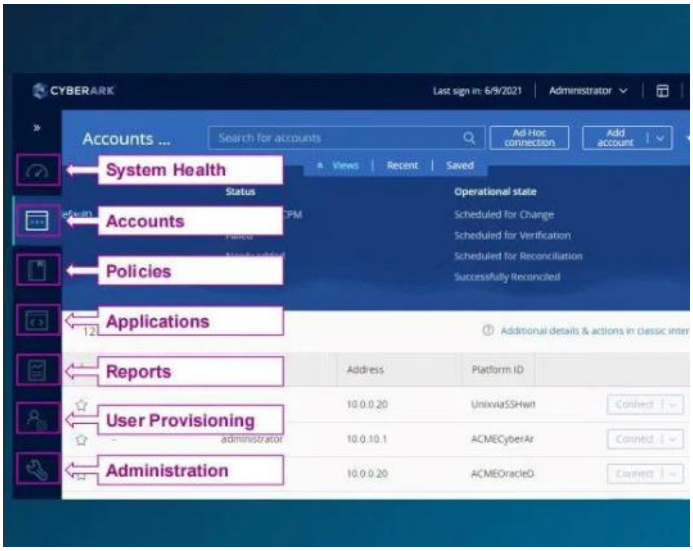


Рисунок 3.14 – Перевірка доступності розділів PVWA після встановлення

Для розширеного налаштування PVWA використовується файл Policies.xml, доступний через PrivateArk Client у сейфі PVWAConfig (рисунок 3.15). Цей XML-файл визначає платформи управління, з’єднувальні компоненти (Connection Components) та параметри привілейованих сесій для кожної платформи.

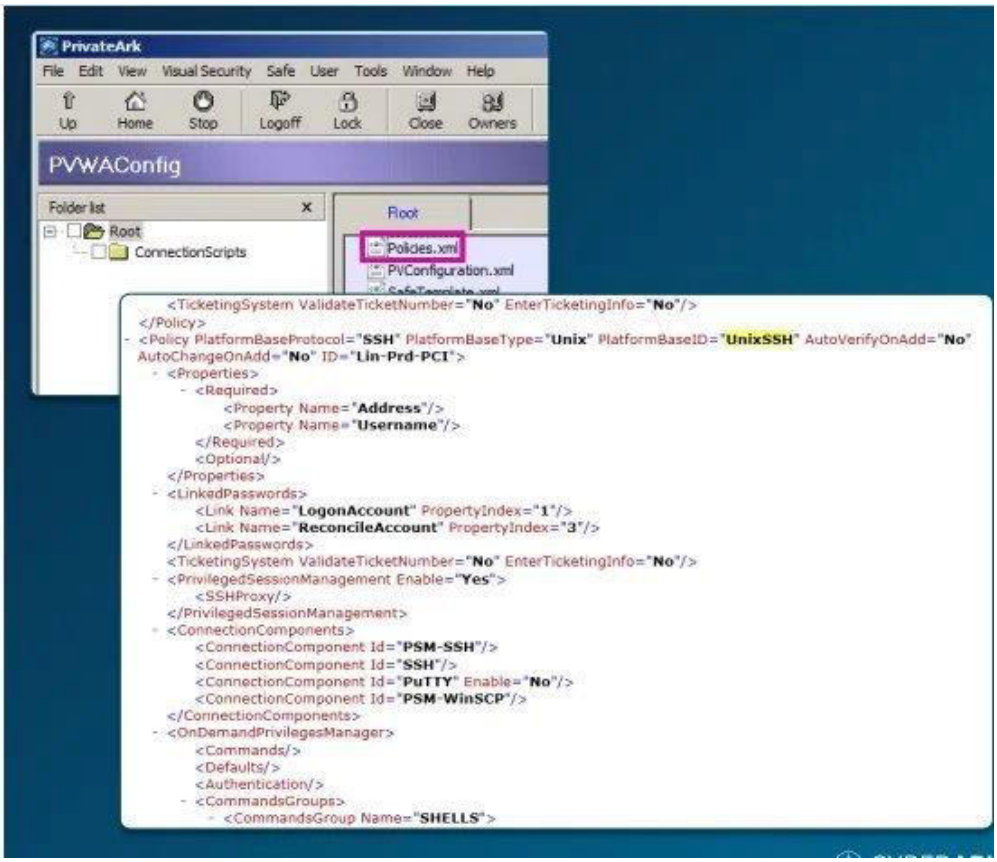


Рисунок 3.15 – Файл конфігурації Policies.xml у сховищі PVWAConfig

3.3.4 Встановлення та налаштування Privileged Session Manager

Privileged Session Manager (PSM) є компонентом CyberArk PAM, що забезпечує безпечний доступ до привілейованих систем з повним записом та моніторингом сесій. PSM діє як проксі-сервер між користувачами та цільовими системами, не розкриваючи облікові дані. Процедура роботи PSM включає шість основних кроків:

– крок 1 — користувач виконує вхід через PVWA за допомогою HTTPS;
– крок 2 — ініціюється підключення через RDP over SSL до сервера PSM;
– крок 3 — PSM отримує облікові дані зі Сховища;

– крок 4 — PSM підключається до цільової системи, використовуючи нативні протоколи (RDP/SSH/HTTPS/VMware тощо);
– крок 5 — сесія записується та зберігається у Vault;
– крок 6 — журнали передаються до SIEM/Syslog.

Цю процедуру графічно зображено на рисунку 3.16.

Рисунок 3.16 – Архітектура взаємодії CyberArk Privileged Session Manager

При плануванні розгортання PSM важливо правильно розрахувати необхідний обсяг сховища. Для сервера PSM використовується формула 3.1. Згідно з нею, необхідний обсяг сховища PSM розраховується як добуток максимальної кількості одночасних сесій, середньої тривалості записаної сесії та середнього бітрейту запису відео плюс 20 ГБ.

$$S_{PSM} = (C_{session} \cdot t_{session} \cdot R_{session\ recording}) + 20\ GB \qquad (3.1)$$

де:

S_{PSM} – необхідний обсяг дискового простору сервера PSM, ГБ;
$C_{session}$ – максимальна кількість одночасних сесій;
$t_{session}$ – середня тривалість записуваної сесії, хв;
$R_{session\ recording}$ – середня швидкість формування запису сесії, КБ/хв;
20 ГБ – резервний обсяг системного простору.

Для сервера Vault розрахунок обсягу сховища є складнішим і розраховується за формулою 3.2. Формула для Vault включає додатковий параметр $t_{retention}$ (тривалість зберігання).

$$S_{Vault} = (t_{retention} \cdot N_{session} \cdot t_{session} \cdot R_{session\ recording}) + 20GB \quad (3.2)$$

де:
S_{Vault} – необхідний обсяг дискового простору на Vault-сервері;
$t_{retention}$ – період зберігання записів сесій (у днях);
$N_{session}$ – середня кількість сесій на день;
$t_{session}$ – середня тривалість записуваної сесії, хв;
$R_{session\ recording}$ – середня швидкість формування запису сесії, КБ/хв;
20 ГБ – резервний обсяг системного простору.

При встановленні PSM необхідно вказати облікові дані Vault-користувача, від імені якого виконується встановлення, як показано на рисунку 3.17. Рекомендується використовувати вбудований обліковий запис Administrator. При розгортанні кількох PSM-серверів всі вони повинні встановлюватися від імені одного Vault-користувача.

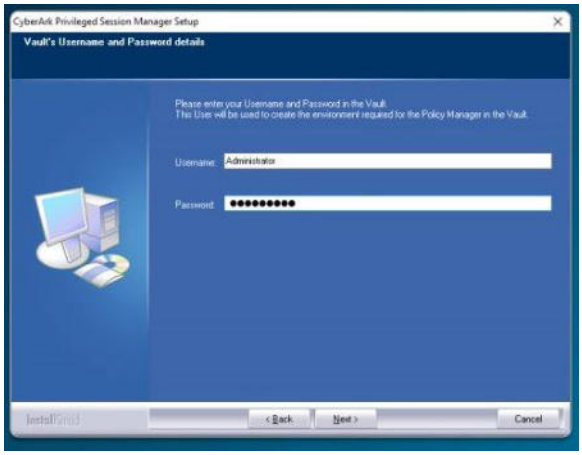


Рисунок 3.17 – Вікно введення облікових даних Vault-користувача при встановленні PSM

Повні конфігураційні файли та скрипти автоматизованого встановлення компонентів PVWA, CPM та PSM наведено відповідно в додатках А, Б та В. Після повного розгортання та post-installation верифікації (імпорт ліцензії, інтеграція з LDAP/AD, створення тестових сейфів, перевірка ротації паролів і записів PSM) середовище стає готовим для проведення практичних занять, симуляції інцидентів та CTF-челенджів.

3.3.5 Схеми мережевої топології та взаємодії компонентів навчального середовища

Для забезпечення наочного розуміння архітектури розгортання навчального CTF-кіберполігону нижче наведено три узагальнювальні схеми, що відображають мережеву топологію середовища (рисунок 3.18), послідовність взаємодії компонентів під час запуску привілейованої сесії студентом (рисунок 3.19) та загальний алгоритм виконання CTF-сценарію на базі CyberArk PAM (рисунок 3.20).

Мережева топологія навчального середовища (рисунок 3.18) охоплює всі сім компонентів платформи CyberArk PAM Self-Hosted, розгорнутих у підмережі 192.168.205.0/24 на базі VMware vSphere. Зона компонентів PAM

включає: Vault (192.168.205.228, TCP 1858) — зашифроване сховище облікових даних; PVWA (192.168.205.230, HTTPS 443) — вебінтерфейс для студентів; PSM (192.168.205.229, RDP 3389) — проксі привілейованих сесій; CPM (192.168.205.231, TCP 443) — менеджер автоматичної ротації паролів; PTA (192.168.205.232, Syslog 514) — аналітик підозрілої активності. Цільові хости представлені Windows Server 2022 (192.168.205.240, RDP 3389) та Linux Ubuntu 22.04 (192.168.205.241, SSH 22). Усі сесії студентів до цільових хостів здійснюються виключно через PSM, що забезпечує повний аудит і запис дій.

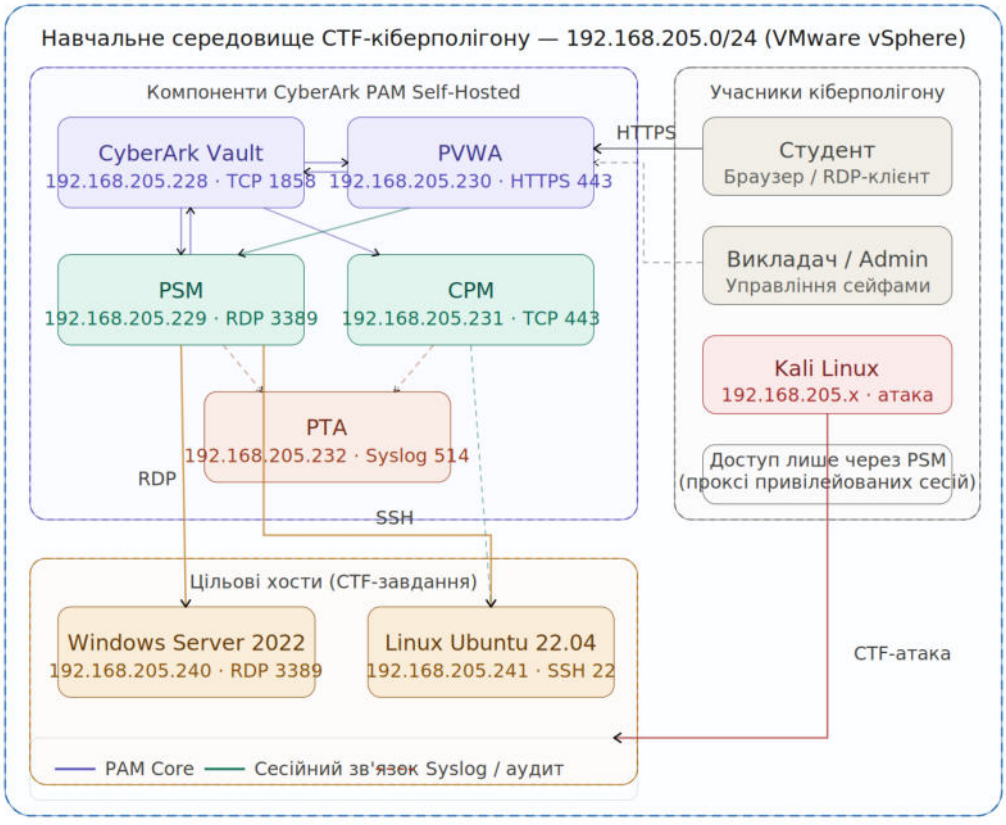


Рисунок 3.18 – Мережева топологія навчального середовища CTF-кіберполігону на базі CyberArk PAM

Діаграма послідовності (рисунок 3.19) відображає повний цикл запуску привілейованої CTF-сесії студентом, що охоплює п’ять етапів. На першому етапі студент автентифікується через PVWA за протоколом LDAP; PVWA верифікує облікові дані у Vault через порт TCP 1858 та повертає сесійний токен. На другому етапі студент отримує перелік доступних облікових записів зі сховищ CTF через REST API PVWA. Третій етап передбачає перевірку та ротацію пароля облікового запису цільового хоста через CPM з оновленням у Vault. На четвертому етапі PVWA ініціює PSM-сесію: PSM отримує від Vault зашифровані облікові дані та встановлює проксі-з’єднання з цільовим хостом по RDP 3389 або SSH 22, не розкриваючи пароля студенту. Завершальний п’ятий етап охоплює аудит: PSM записує відео та логи сесії до Vault, надсилає Syslog-повідомлення на PTA для виявлення аномалій, а після виконання CTF-завдання студент подає прапор через API PVWA.

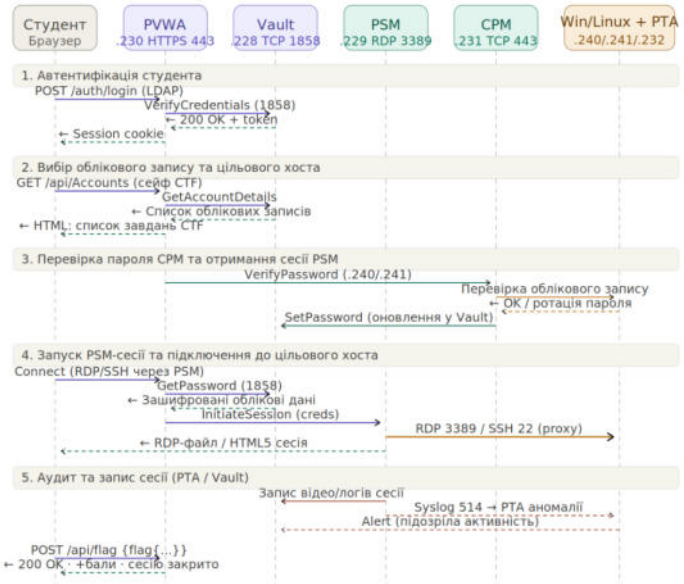


Рисунок 3.19 – Діаграма послідовності запуску привілейованої CTF-сесії студентом через CyberArk PAM

Блок-схема алгоритму CTF-сценарію (рисунок 3.20) відображає повний процес виконання навчального завдання — від ініціалізації середовища до формування підсумкової звітності. Алгоритм охоплює такі ключові вузлові точки: автентифікацію та вибір типу операції (CAM-запит або ротація паролів через PVWA та CPM); створення PSM-сесії з ізоляцією RDP/SSH та її паралельний аналіз компонентом PTA в режимі реального часу; ескалацію привілеїв та виконання CTF-сценарію в ролі студента; перевірку верифікації CTF-прапора з двома шляхами: успішним (запис сесії, аналіз витоку та захисту через PTA) і неуспішним (реєстрація загрози через PTA з відповідним ризик-рейтингом); прийняття рішення про розміщення деталей завдання в документації відповідно до Vault/аналітики. Блок-схема наочно підтверджує, що компоненти PTA виконують моніторинг на двох рівнях — безпосередньо під час сесії та після її завершення — що відповідає принципу Zero Trust у навчальному середовищі.

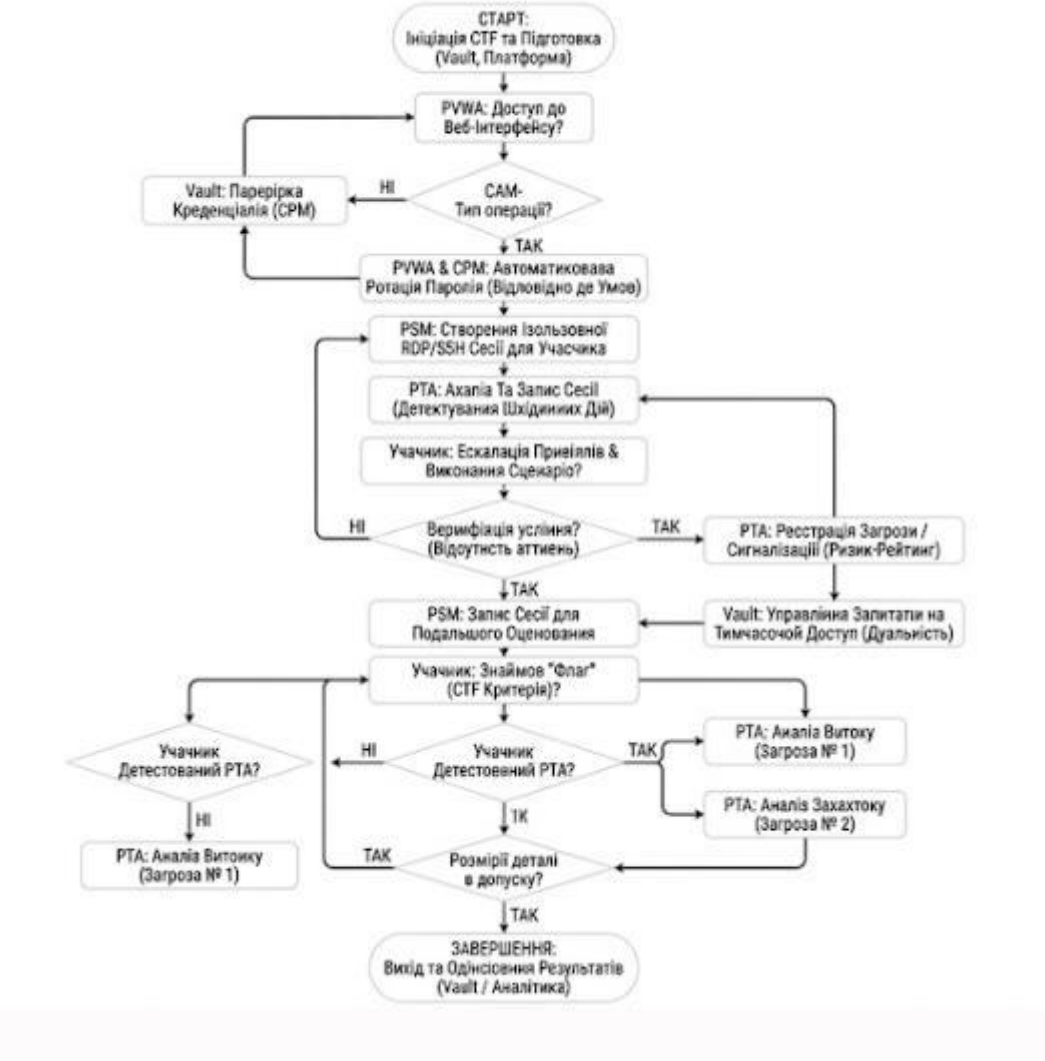


Рисунок 3.20 – Блок-схема алгоритму виконання CTF-сценарію на базі CyberArk PAM

3.4 Структура облікових записів та сейфів у навчальному середовищі

Навчальне середовище побудоване так, щоб максимально точно відтворити типову корпоративну конфігурацію CyberArk. Усі об’єкти — сейфи, облікові записи, платформи та права доступу — відповідають

стандартам, описаним у офіційній документації CyberArk PAM Self-Hosted. Це дозволяє студентам після закінчення навчання безпосередньо застосовувати отримані навички на реальних виробничих системах.

У системі CyberArk створено три облікові записи з різними рівнями доступу. Обліковий запис cyberark_admin — адміністративний, із повними правами на всі сейфи та компоненти; використовується виключно викладачем для первинного налаштування середовища, скидання флагів між потоками студентів та ініціювання тестових подій безпеки. Обліковий запис student_user — стандартний, із правами, суворо обмеженими принципом least privilege; саме від цього імені студенти виконують усі завдання. Обліковий запис auditor_user — з правами лише на читання журналів сесій та аудиторських звітів; використовується у завданнях, що стосуються forensics та аналізу записів.

У Vault створено чотири сейфи. Сейф Training-Windows містить облікові записи цільового Windows Server: Administrator (управляється CPM, ротація щодобово), service_account (поза CPM — навмисно для демонстрації некерованого акаунту) та backup_admin (прихований обліковий запис, виявляється через Pending Accounts). Сейф Training-Linux містить облікові записи Ubuntu-хоста: root (управляється CPM) та deploy_user (поза CPM). Training-Audit є спеціальним сейфом, доступним лише auditor_user, — містить підготовлені журнали та артефакти для завдань forensics-типу. Training-Flags — технічний сейф, в якому зберігаються текстові файли з флагами. Повний перелік облікових записів у навчальних сейфах наведено в таблиці 3.2.

Таблиця 3.2 – Облікові записи у навчальних сейфах CyberArk

Сейф	Обліковий запис	Тип	Керується CPM	Доступ student_user
Training-Windows	Administrator	Windows Local Admin	Так (щодобово)	Перегляд + З'єднання (PSM)
Training-Windows	service_account	Windows Service	Ні	Лише перегляд
Training-Windows	backup_admin	Windows Local Admin	Ні	Pending Accounts
Training-Linux	root	Linux Root (SSH)	Так (щодобово)	Перегляд + З'єднання (PSM)
Training-Linux	deploy_user	Linux Service	Ні	Лише перегляд
Training-Audit	підготовлені журнали	Audit Records	—	Недоступний
Training-Flags	текстові файли-флаги	Generic	—	Лише через PSM-сесію

Права доступу student_user до сейфів налаштовані максимально реалістично: дозволено List Accounts (перегляд переліку), Use Accounts (підключення через PSM) та Retrieve Accounts (перегляд пароля у masked-формі). Функції Add, Delete, Modify, Rename та Manage Safe навмисно заборонені. Такий набір прав точно відтворює роль Junior PAM Analyst у реальній організації.

Флаги CTF-кіберполігону зберігаються у трьох різних місцях, що відповідає логіці кожного завдання та наочно демонструє студентам, де в реальних PAM-системах зберігається чутлива інформація. Перший тип розміщення — у полях Properties (Custom Fields, Description) облікових записів у PVWA. Другий тип — у файлах на цільових хостах, доступних лише через PSM-сесію. Третій тип — у журналах аудиту та записах сесій

(лог PSM-сесії або поле Comment алерту PTA). Флаг підсумкового завдання генерується динамічно як MD5-хеш від конкатенації прізвища студента та номера групи. Зведені місця зберігання всіх флагів наведено в таблиці 3.3.

Таблиця 3.3 – Місця зберігання флагів CTF-кіберполігону

Завдання	Флаг	Місце зберігання	Компонент CyberArk
1	flag{pvwa_first_login_ok}	Поле Description облікового запису Administrator	PVWA → Accounts → Properties
2	flag{platform_windows_srv_22}	Поле Custom Field "CTF_Flag" облікового запису Administrator	PVWA → Account Details
3	flag{cpm_rotation_active_24h}	Поле Custom Field "CTF_Flag" облікового запису root (Training-Linux)	PVWA → Accounts → Properties
4	flag{service_acc_not_managed}	Поле Description облікового запису service_account	PVWA → Account Details
5	flag{psm_session_rdp_broker}	Файл C:\flags\flag5.txt на Windows Server	Цільовий хост (через PSM-сесію)
6	flag{linux_ssh_via_pam_only}	Файл /opt/flags/flag6.txt на Linux Server	Цільовий хост (через PSM-сесію)
7	flag{psm_session_no_ticket_47min}	Поле Session Note активної PSM-сесії domain_admin	PVWA → Active Sessions

Продовження таблиці 3.3

8	flag{pta_alert_unusual_ip}	Поле Comment PTA-алерту Suspicious Connection Source	PVWA → Security Events
9	flag{md5(прізвище+група)}	Генерується динамічно, перевіряється викладачем	Поза CyberArk (підсумкове)

3.5 Практичні завдання кіберполігону

Практична частина кіберполігону складається з послідовних завдань, об’єднаних наскрізним сценарієм. Завдання розподілено на три рівні складності: рівень 1 (завдання 1–4) — базове знайомство з PVWA та структурою PAM-системи; рівень 2 (завдання 5–8) — практична робота з PSM-сесіями, виявлення вразливостей та аналіз журналів; рівень 3 (завдання 9 та підсумкове) — реагування на інцидент і рефлексія. Перелік завдань наведено в таблиці 3.4. Знімки екрана з покроковим виконанням кожного завдання та супутні скрипти винесено до додатка Г.

Таблиця 3.4 – Перелік завдань CTF-кіберполігону

№	Назва завдання	Рівень	Компонент	ПРН	Флаг
1	Перший вхід: знайди опис облікового запису	Рівень 1	PVWA	ПРН-11	flag{pvwa_first_login_ok}

Продовження таблиці 3.4

2	Яка плат форма — знайди кастомне поле	Рівень 1	PVWA	ПРН-11	flag{platform_windows_srv_22}
3	Ротація паролів: флаг у Linux-акаунті	Рівень 1	CPM + PVWA	ПРН-9	flag{cpm_rotation_active_24h}
4	Некерований акаунт: прочитай опис	Рівень 1	PVWA	ПРН-3	flag{service_acc_not_managed}
5	Підключись через PSM і прочитай файл	Рівень 2	PSM	ПРН-11	flag{psm_session_rdp_broker}
6	SSH без пароля: PSM-сесія до Linux	Рівень 2	PSM	ПРН-11	flag{linux_ssh_via_pam_only}
7	Перехопи активну сесію	Рівень 2	PVWA + PSM	ПРН-3	flag{psm_session_no_ticket_47min}
8	PTA-алерт: прочитай коментар до події	Рівень 3	PTA	ПРН-7	flag{pta_alert_unusual_ip}
9	Підсумковий рапорт: перелік ризиків	Рівень 3	Всі	ПРН-14	flag{md5(прізвище+група)}

Нижче подано стислий опис кожного завдання. Детальні покрокові інструкції та ілюстрації наведено в додатку Г.

Завдання 1. Перший вхід. Студент входить до PVWA за обліковим записом student_user, у розділі Accounts відкриває обліковий запис Administrator (сейф Training-Windows) та зчитує перший флаг із поля Description. Завдання знайомить із веб-інтерфейсом PVWA та поняттям сейфа як контейнера облікових записів. Флаг: flag{pvwa_first_login_ok} (рис. Г.1–Г.3).

Завдання 2. Кастомне поле платформи. Студент знаходить у деталях облікового запису Administrator кастомне поле CTF_Flag та визначає платформу Windows Server Local Accounts, яка керує цим записом. Завдання пояснює призначення Platforms і Custom Fields у CyberArk. Флаг: flag{platform_windows_srv_22} (рис. Г.4, Г.5).

Завдання 3. Ротація паролів. Студент відкриває обліковий запис root у сейфі Training-Linux, зчитує поле CTF_Flag та переконується, що CPM Status = Success; для порівняння відкриває deploy_user зі статусом Not Managed. Завдання демонструє роботу CPM та різницю між керованими й некерованими акаунтами. Флаг: flag{cpm_rotation_active_24h} (рис. Г.6, Г.7).

Завдання 4. Некерований акаунт. Студент знаходить обліковий запис service_account, читає нотатку у полі Description та звертає увагу на CPM Status = Not Managed і давню дату Password Last Changed. Завдання формує розуміння ризиків сервісних акаунтів поза PAM. Флаг: flag{service_acc_not_managed} (рис. Г.8, Г.9).

Завдання 5. PSM-сесія до Windows. Студент через кнопку Connect ініціює PSM-RDP-з’єднання до Windows Server без розкриття пароля

адміністратора, відкриває файл C:\flags\flag5.txt та зчитує флаг. Завдання ілюструє принцип Zero Standing Privileges і роль PSM як брокера доступу. Флаг: flag{psm_session_rdp_broker} (рис. Г.10–Г.12).

Завдання 6. PSM-сесія до Linux. Студент через PSM-SSH підключається до Linux-сервера під root без введення пароля та виконує команду cat /opt/flags/flag6.txt. Завдання показує підтримку PSM протоколу SSH та переваги відмови від прямого доступу. Флаг: flag{linux_ssh_via_pam_only} (рис. Г.13, Г.14).

Завдання 7. Перехоплення активної сесії. Студент у розділі Active Sessions знаходить підозрілу RDP-сесію облікового запису domain_admin (тривалість 47 хв, без прив'язки тікету) та зчитує флаг із поля Session Note. Завдання відпрацьовує моніторинг привілейованих сесій у реальному часі. Флаг: flag{psm_session_no_ticket_47min} (рис. Г.15, Г.16).

Завдання 8. PTA-алерт. Студент у розділі Security Events відкриває алерт типу Suspicious Connection Source, аналізує його деталі (User Name, Source IP, Risk Score) та зчитує флаг із поля Comment. Завдання знайомить з модулем PTA та базовим алгоритмом реагування Investigate → Document → Mitigate. Флаг: flag{pta_alert_unusual_ip} (рис. Г.17, Г.18).

Завдання 9. Підсумковий рапорт. На основі виконаних завдань студент складає короткий аудиторський рапорт у форматі Risk ID | Опис | Компонент | Рекомендація (шаблон наведено в таблиці 3.5). Після здачі рапорту викладач обчислює персональний флаг за формулою md5(прізвище_латиницею + номер_групи), що унеможливлює списування. Флаг: flag{md5(прізвище+група)}. Без виконання частки завдань студент не зможе повноцінно сформувати фінальний рапорт.

Таблиця 3.5 – Шаблон аудиторського рапорту (заповнюється студентом)

Risk ID	Опис ризику	Виявлено у	Рекомендація
R-001	Некерований обліковий запис service_account — пароль не ротується	Завдання 3, 4	Підключити до CPM або видалити
R-002	Прихований адміністраторський акаунт backup_admin поза PAM	Завдання 7	Перемістити до Training-Windows, підключити CPM
R-003	Спроба несанкціонованого підключення з зовнішньої IP-адреси	Завдання 8	Заблокувати IP, відключити акаунт, провести forensics
R-004	(Заповнює студент)	(Завдання №)	(Рекомендація студента)

3.6 Методика проведення заняття та оцінювання результатів

Тривалість одного заняття на CTF-кіберполігоні складає 3–4 академічні години. Перші 15 хвилин відводяться на інструктаж та підключення через VPN. Завдання 1–4 (рівень 1) розраховані приблизно на 45–60 хвилин, завдання 5–8 (рівень 2) потребують ще 60–75 хвилин, а завдання рівня 3 займають 30–45 хвилин, з них 15–20 — на підготовку рапорту.

Систему (рівні, завдання, загальна кількість балів) оцінювання наведено в таблиці 3.6.

Таблиця 3.6 – Система оцінювання CTF-кіберполігону

Рівень	Завдання	Балів за флаг	Максимум за рівень
Рівень 1	1, 2, 3, 4	8 балів	32 бали

Продовження таблиці 3.6

Рівень 2	5, 6, 7	10 балів	40 балів
Рівень 3	8	12 балів	12 балів
Рівень 3	9 (рапорт)	4–12 балів	12 балів
Разом	1–9	—	100 балів

Система флагів дозволяє реалізувати часткове оцінювання: студент отримує бали за кожен правильно знайдений флаг незалежно від того, чи виконав він усі завдання. Це усуває ситуацію «все або нічого» та мотивує студентів не здаватися при виникненні труднощів. Крім того, унікальний персональний флаг підсумкового завдання (md5-хеш) унеможливлює списування — кожен студент має власний правильний рядок.

3.7 Висновки до розділу 3

У третьому розділі дипломної роботи розроблено, детально описано та апробовано модель CTF-кіберполігону на базі реальної enterprise-системи PAM CyberArk Self-Hosted, розгорнутої у середовищі компанії BAKOTECH.

Описано архітектуру розгортання та мережеву взаємодію компонентів CyberArk PAM, а також покроковий процес встановлення основних компонентів — Digital Vault, Central Policy Manager, Password Vault Web Access та Privileged Session Manager — з ілюстрацією ключових етапів конфігурування. Розроблено повну інфраструктуру навчального середовища: 5 компонентів CyberArk (Vault, PVWA, PSM, CPM, PTA), 4 сейфи (Training-Windows, Training-Linux, Training-Audit, Training-Flags), 7 цільових облікових записів (у тому числі навмисно «прихований»

backup_admin) та 3 ролі учасників (cyberark_admin, student_user, auditor_user) з налаштованими правами доступу за принципом least privilege.

Розроблено систему послідовних практичних завдань CTF-формату з флагами, розподілених на 3 рівні складності. Флаги зберігаються у трьох типах сховищ: поля Properties облікових записів PVWA, файли на цільових хостах, доступні лише через PSM-сесію, а також журнали сесій та коментарі алертів PTA. Флаг підсумкового завдання генерується персонально для кожного студента на основі md5-хешу, що унеможливлює списування.

Розроблено систему оцінювання (100 балів), методику проведення заняття (3–4 год.) та Картку учасника для фіксації флагів. Усі елементи методики узгоджені з вимогами Стандарту МОН № 1547/2024 та безпосередньо забезпечують формування ПРН-3, ПРН-7, ПРН-9, ПРН-11 та ПРН-14 спеціальності 125 «Кібербезпека».

ВИСНОВКИ

У дипломній роботі досліджено актуальну проблему підвищення якості практичної підготовки здобувачів вищої освіти спеціальності 125 «Кібербезпека» шляхом розробки та впровадження моделі CTF-кіберполігону на базі системи привілейованого доступу (PAM) CyberArk Self-Hosted.

За результатами теоретичного дослідження (Розділ 1) встановлено, що CTF-кіберполігони є одним із найбільш ефективних сучасних інструментів практичного навчання. Проведено класифікацію кіберполігонів за типом реалізації (симуляційні, емуляційні, гібридні) та форматами CTF (Jeopardy-style, Attack-Defense, King of the Hill, Mixed). Доведено педагогічну ефективність даного підходу через реалізацію компетентнісного підходу, циклу експериментального навчання Колба та механізмів гейміфікації (модель Octalysis). Проаналізовано нормативно-правову базу України, яка прямо підтримує впровадження сучасних практичних інструментів навчання у підготовці фахівців з кібербезпеки.

У аналітичній частині (Розділ 2) виявлено суттєвий розрив між вимогами ринку праці та рівнем практичної підготовки здобувачів. Згідно з аналізом вакансій, 78 % роботодавців вимагають досвіду участі в CTF, а 43 % — знань PAM-систем. Анкетування студентів КНУБА показало, що лише 18 % здобувачів мають досвід CTF, а загальна задоволеність практичною підготовкою становить лише 34 %. Порівняльний аналіз існуючих платформ підтвердив, що жодна з них не забезпечує необхідного рівня реалістичності та адаптованості до освітньої програми спеціальності 125. Дослідження ландшафту кіберзагроз показало, що атаки на привілейований доступ

становлять 27 % інцидентів в Україні, що обґрунтовує вибір PAM CyberArk як бази для кіберполігону.

У практичній частині (Розділ 3) розроблено, розгорнуто та апробовано авторську модель CTF-кіберполігону на базі реальної enterprise-системи CyberArk PAM Self-Hosted v14.x у виробничому середовищі компанії ВАКОТЕСН. Реалізовано повний цикл встановлення всіх ключових компонентів (Digital Vault, PVWA, CPM, PSM, PTA), структуру сейфів та облікових записів за принципом least privilege, систему з 9 практичних завдань різного рівня складності з використанням флагів, методику проведення занять та 100-бальну систему оцінювання.

Основним результатом роботи є **створення реалістичного та практичного навчального середовища**, яке дозволяє студентам працювати з промисловою PAM-системою. Розроблена модель безпосередньо забезпечує досягнення ключових програмних результатів навчання (ПРН-3, ПРН-7, ПРН-9, ПРН-11, ПРН-14) Стандарту спеціальності 125 «Кібербезпека».

Практичне значення дипломної роботи полягає у впровадженні розробленого кіберполігону в навчальний процес. Це дозволяє значно підвищити якість практичної підготовки здобувачів освіти та наблизити її до реальних вимог ринку праці.

Подальші перспективи розвитку моделі включають розширення сценаріїв (інтеграція з SIEM-системами), автоматизацію перевірки флагів, створення дистанційної версії полігону та проведення міжвузівських CTF-змагань.

Таким чином, поставлена мета дипломної роботи досягнута в повному обсязі. Отримані теоретичні висновки, аналітичні результати та практична

модель підтверджують ефективність використання enterprise-систем PAM як сучасного інструменту практичної підготовки фахівців з кібербезпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. DOU Tech Radar. Ринок праці у сфері IT в Україні: звіт за 2024 рік. – Київ: DOU, 2024. – 42 с. URL: https://dou.ua/lenta/articles/tech-radar-2024/ (дата звернення: 10.03.2026).
2. Work.ua Industry Report. Аналітика ринку праці в IT-секторі: підсумки 2024 року. – Київ: Work.ua, 2025. – 28 с. URL: https://www.work.ua/news/it/ (дата звернення: 12.03.2026).
3. Державна служба зайнятості України. Аналіз ринку праці: попит на фахівців IT-сфери. – Київ: ДСЗ, 2024. – URL: https://www.dcz.gov.ua/analitics (дата звернення: 14.03.2026).
4. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII (редакція від 19.04.2026). – URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 01.04.2026).
5. CERT-UA. Звіт про кіберінциденти за 2024 рік. – Київ: ДСССЗЗІ, 2025. – URL: https://cert.gov.ua/article/2025report (дата звернення: 20.03.2026).
6. Verizon. 2024 Data Breach Investigations Report (DBIR). – Verizon, 2024. – 104 p. URL: https://www.verizon.com/business/resources/reports/dbir/ (дата звернення: 22.03.2026).
7. NIST SP 800-150. Guide to Cyber Threat Information Sharing. – National Institute of Standards and Technology, 2016. – 42 p.
8. ECSO. Understanding Cyber Ranges: From Hype to Reality. – European Cyber Security Organisation, 2020. – 60 p. URL: https://www.ecs-org.eu/documents/publications/5ee73d0c0a1fa.pdf (дата звернення: 15.03.2026).

9. Стратегія кібербезпеки України на 2021–2025 роки: затв. Указом Президента України № 447/2021 від 26.08.2021. – URL: https://www.president.gov.ua/documents/4472021-40289 (дата звернення: 01.04.2026).
10. Стандарт вищої освіти за спеціальністю 125 «Кібербезпека»: затв. наказом МОН України № 1547 від 29.10.2024. – Київ: МОН, 2024. – URL: https://mon.gov.ua/storage/app/media/vishcha-osvita/zatverdzeni%20standarty/125-kiberbezpeka.pdf (дата звернення: 02.04.2026).
11. Закон України «Про вищу освіту» від 01.07.2014 № 1556-VII (зі змінами). – URL: https://zakon.rada.gov.ua/laws/show/1556-18 (дата звернення: 01.04.2026).
12. Закон України «Про освіту» від 05.09.2017 № 2145-VIII (зі змінами). – URL: https://zakon.rada.gov.ua/laws/show/2145-19 (дата звернення: 01.04.2026).
13. Положення про кваліфікаційну роботу здобувачів вищої освіти КНУБА: затв. Вченою радою КНУБА 31.05.2024, введено в дію наказом ректора № 224 від 12.06.2024. – Київ: КНУБА, 2024.
14. Kolb D. A. Experiential Learning: Experience as the Source of Learning and Development. – 2nd ed. – New Jersey: Pearson, 2014. – 390 p.
15. Chou Y. K. Actionable Gamification: Beyond Points, Badges and Leaderboards. – Octalysis Media, 2015. – 476 p.
16. CyberArk. Privileged Access Management Core Concepts. – CyberArk Software, 2024. – URL: https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PAS%20INST/introduction.htm (дата звернення: 05.04.2026).

17. Gartner Magic Quadrant for Privileged Access Management, 2024. – Gartner Inc., 2024. – URL: https://www.gartner.com/en/documents/magic-quadrant-pam-2024 (дата звернення: 06.04.2026).

18. HackTheBox Academy. Cybersecurity Learning Platform. – URL: https://academy.hackthebox.com (дата звернення: 10.04.2026).

19. TryHackMe. Cybersecurity Training Platform. – URL: https://tryhackme.com (дата звернення: 10.04.2026).

20. KYPO Cyber Range Platform. Masaryk University, Brno. – URL: https://kypo.ics.muni.cz (дата звернення: 12.04.2026).

21. picoCTF. Carnegie Mellon University. – URL: https://picoctf.org (дата звернення: 12.04.2026).

22. Virginia Cyber Range. Virginia Tech. – URL: https://www.virginiacyberrange.org (дата звернення: 13.04.2026).

23. Benenson Z., Dürr F., Omerovic A. Cyber Range Design Patterns for Educational CTF. // Proceedings of IEEE Security & Privacy. – 2022. – P. 45–59.

24. Сміян О. І. Гейміфікація в освіті: теорія та практика. – Харків: НТУ «ХПІ», 2023. – 128 с.

25. Csikszentmihalyi M. Flow: The Psychology of Optimal Experience. – New York: HarperCollins, 1990. – 303 p.

26. Майєр Р. Мультимедійне навчання. – Київ: Літопис, 2019. – 328 с.

27. CyberArk. Privileged Session Manager (PSM) Administration Guide. – CyberArk Software, 2024. – URL: https://docs.cyberark.com/pam-self-hosted/latest/en/content/psm/psm-overview.htm (дата звернення: 07.04.2026).

28. Інститут модернізації змісту освіти. Концепція розвитку цифрової компетентності в системі вищої освіти України. – Київ: ІМЗО, 2023. – 48 с. URL: https://imzo.gov.ua/osvita/tsyfrova-kompetentnist/ (дата звернення: 18.03.2026).

29. Abbass H., Perez-Minana E., Souls G. Cybersecurity Education for Awareness and Compliance. – IGI Global, 2023. – 312 p.

30. Міністерство цифрової трансформації України. Звіт про стан кібербезпеки України за 2024 рік. – Київ: Мінцифра, 2025. – URL: https://thedigital.gov.ua/cybersecurity-report-2024 (дата звернення: 22.03.2026).

ДОДАТКИ

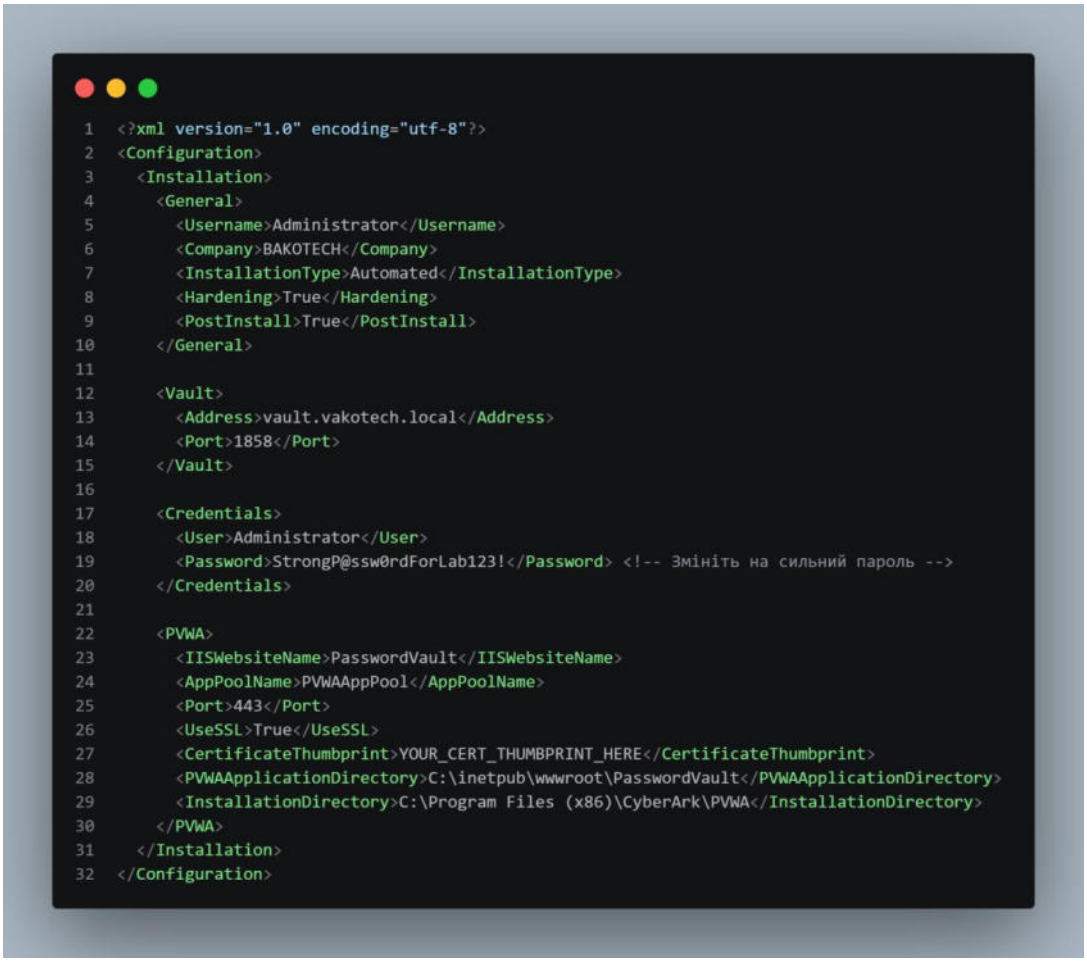
Скрипти та конфігураційні файли для автоматичного встановлення CyberArk PAM Self-Hosted v14.x

Додаток А

Скрипти встановлення Password Vault Web Access (PVWA)

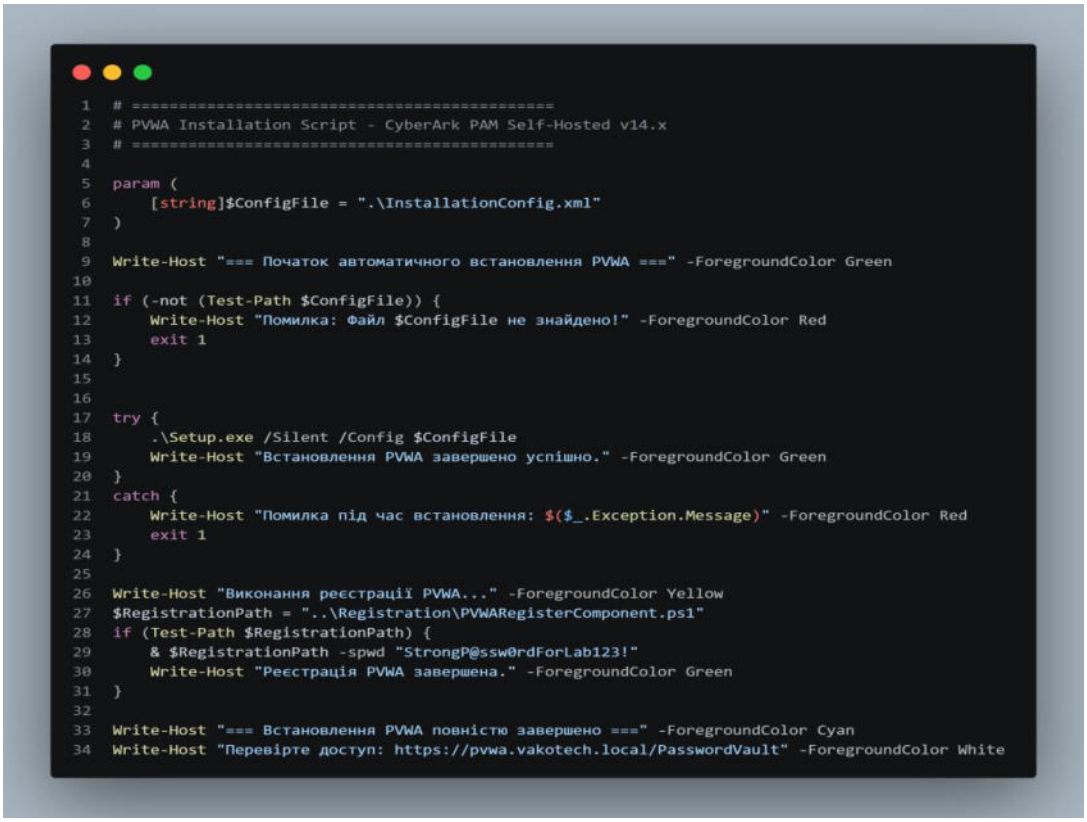
```powershell
# ============================================
# PVWA Prerequisites Script - CyberArk PAM Self-Hosted v14.x
# Виконується перед встановленням PVWA
# ============================================

param (
    [string]$InstallationPath = "C:\CyberArk\PVWA"
)

Write-Host "=== Запуск PVWA Prerequisites ===" -ForegroundColor Green

Install-WindowsFeature -Name Web-Server, Web-Asp-Net45, Web-Net-Ext45, Web-ISAPI-Ext, Web-ISAPI-Filter, `
    Web-Mgmt-Console, Web-Mgmt-Tools, Web-Default-Doc, Web-Http-Errors, Web-Http-Logging, `
    Web-Http-Redirect, Web-Http-Tracing, Web-Static-Content, Web-Windows-Auth, Web-Digest-Auth, `
    Web-Basic-Auth -IncludeManagementTools -ErrorAction Stop

Enable-WindowsOptionalFeature -Online -FeatureName NetFx4-AdvSrvs -All -ErrorAction SilentlyContinue

if (-not (Test-Path $InstallationPath)) {
    New-Item -Path $InstallationPath -ItemType Directory -Force
}

$certDnsName = "pvwa.vakotech.local"
$cert = New-SelfSignedCertificate `
    -DnsName $certDnsName `
    -CertStoreLocation "cert:\LocalMachine\My" `
    -KeyExportPolicy Exportable `
    -Provider "Microsoft Enhanced RSA and AES Cryptographic Provider" `
    -NotAfter (Get-Date).AddYears(5)

$thumbprint = $cert.Thumbprint
Export-Certificate -Cert $cert -FilePath "$InstallationPath\selfsigned.cer" -Force

Write-Host "Self-signed certificate Thumbprint: $thumbprint" -ForegroundColor Yellow
Write-Host "Рекомендація: імпортуйте сертифікат у Trusted Root для уникнення попереджень браузера." -ForegroundColor Cyan

netsh advfirewall firewall add rule name="PVWA HTTPS" dir=in action=allow protocol=TCP localport=443

Write-Host "=== PVWA Prerequisites завершено успішно ===" -ForegroundColor Green
Write-Host "Thumbprint сертифікату для InstallationConfig.xml: $thumbprint" -ForegroundColor White
```

Рисунок А.1 – Скрипт перевірки передумов PVWA_PreInstallation.ps1



```xml
<?xml version="1.0" encoding="utf-8"?>
<Configuration>
  <Installation>
    <General>
      <Username>Administrator</Username>
      <Company>BAKOTECH</Company>
      <InstallationType>Automated</InstallationType>
      <Hardening>True</Hardening>
      <PostInstall>True</PostInstall>
    </General>

    <Vault>
      <Address>vault.vakotech.local</Address>
      <Port>1858</Port>
    </Vault>

    <Credentials>
      <User>Administrator</User>
      <Password>StrongP@ssw0rdForLab123!</Password> <!-- Змініть на сильний пароль -->
    </Credentials>

    <PVWA>
      <IISWebsiteName>PasswordVault</IISWebsiteName>
      <AppPoolName>PVWAAppPool</AppPoolName>
      <Port>443</Port>
      <UseSSL>True</UseSSL>
      <CertificateThumbprint>YOUR_CERT_THUMBPRINT_HERE</CertificateThumbprint>
      <PVWAApplicationDirectory>C:\inetpub\wwwroot\PasswordVault</PVWAApplicationDirectory>
      <InstallationDirectory>C:\Program Files (x86)\CyberArk\PVWA</InstallationDirectory>
    </PVWA>
  </Installation>
</Configuration>
```

Рисунок А.2 – Конфігураційний файл InstallationConfig.xml для PVWA



```powershell
# ============================================
# PVWA Installation Script - CyberArk PAM Self-Hosted v14.x
# ============================================

param (
    [string]$ConfigFile = ".\InstallationConfig.xml"
)

Write-Host "=== Початок автоматичного встановлення PVWA ===" -ForegroundColor Green

if (-not (Test-Path $ConfigFile)) {
    Write-Host "Помилка: Файл $ConfigFile не знайдено!" -ForegroundColor Red
    exit 1
}


try {
    .\Setup.exe /Silent /Config $ConfigFile
    Write-Host "Встановлення PVWA завершено успішно." -ForegroundColor Green
}
catch {
    Write-Host "Помилка під час встановлення: $($_.Exception.Message)" -ForegroundColor Red
    exit 1
}

Write-Host "Виконання реєстрації PVWA..." -ForegroundColor Yellow
$RegistrationPath = "..\Registration\PVWARegisterComponent.ps1"
if (Test-Path $RegistrationPath) {
    & $RegistrationPath -spwd "StrongP@ssw0rdForLab123!"
    Write-Host "Реєстрація PVWA завершена." -ForegroundColor Green
}

Write-Host "=== Встановлення PVWA повністю завершено ===" -ForegroundColor Cyan
Write-Host "Перевірте доступ: https://pvwa.vakotech.local/PasswordVault" -ForegroundColor White
```

Рисунок А.3 – Основний скрипт встановлення PVWAInstallation.ps1

Додаток Б

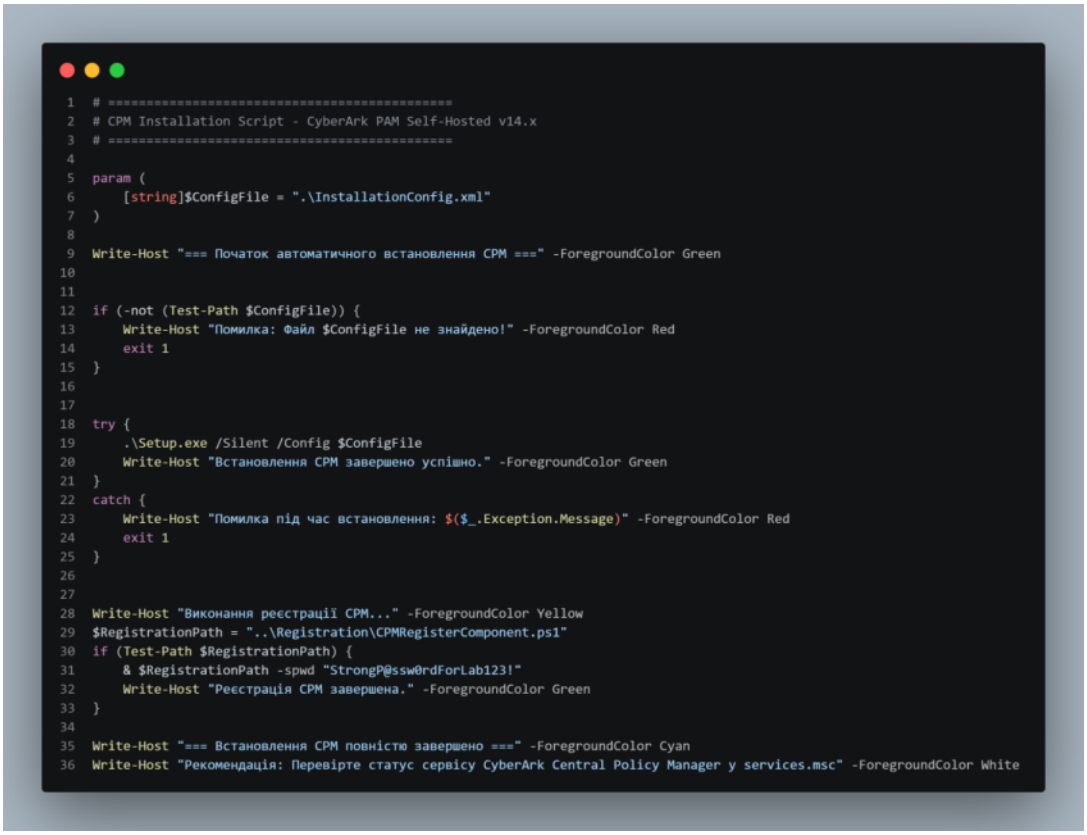
Скрипти встановлення Central Policy Manager (CPM)

```powershell
# ============================================
# CPM Prerequisites Script - CyberArk PAM Self-Hosted v14.x
# Виконується перед встановленням Central Policy Manager
# ============================================

param (
    [string]$InstallationPath = "C:\CyberArk\CPM"
)

Write-Host "=== Запуск CPM Prerequisites ===" -ForegroundColor Green


Install-WindowsFeature -Name NET-Framework-45-ASPNET, NET-WCF-HTTP-Activation45, NET-WCF-TCP-PortSharing45 -IncludeManagementTools -ErrorAction Stop


Enable-WindowsOptionalFeature -Online -FeatureName NetFx4-AdvSrvs -All -ErrorAction SilentlyContinue


if (-not (Test-Path $InstallationPath)) {
    New-Item -Path $InstallationPath -ItemType Directory -Force
}


netsh advfirewall firewall add rule name="CPM" dir=in action=allow protocol=TCP localport=19000
netsh advfirewall firewall add rule name="CPM Console" dir=in action=allow protocol=TCP localport=19009

Write-Host "Firewall rules для CPM налаштовано." -ForegroundColor Yellow


Write-Host "=== CPM Prerequisites завершено успішно ===" -ForegroundColor Green
Write-Host "Переконайтеся, що Visual C++ Redistributable 2015-2022 встановлено." -ForegroundColor Cyan
```

Рисунок Б.1 – Скрипт перевірки передумов CPM_Prerequisites.ps1

```xml
<?xml version="1.0" encoding="utf-8"?>
<Configuration>
  <Installation>
    <General>
      <Username>Administrator</Username>
      <Company>BAKOTECH</Company>
      <InstallationType>Automated</InstallationType>
      <Hardening>True</Hardening>
      <PostInstall>True</PostInstall>
    </General>

    <Vault>
      <Address>vault.vakotech.local</Address>
      <Port>1858</Port>
    </Vault>

    <Credentials>
      <User>Administrator</User>
      <Password>StrongP@ssw0rdForLab123!</Password> <!-- Змініть на сильний пароль -->
    </Credentials>

    <CPM>
      <CPMName>CPM01</CPMName>
      <InstallationDirectory>C:\Program Files (x86)\CyberArk\CPM</InstallationDirectory>
      <Scanner>True</Scanner>
      <AutomaticManagement>True</AutomaticManagement>
    </CPM>
  </Installation>
</Configuration>
```

Рисунок Б.2 – Конфігураційний файл InstallationConfig.xml для CPM

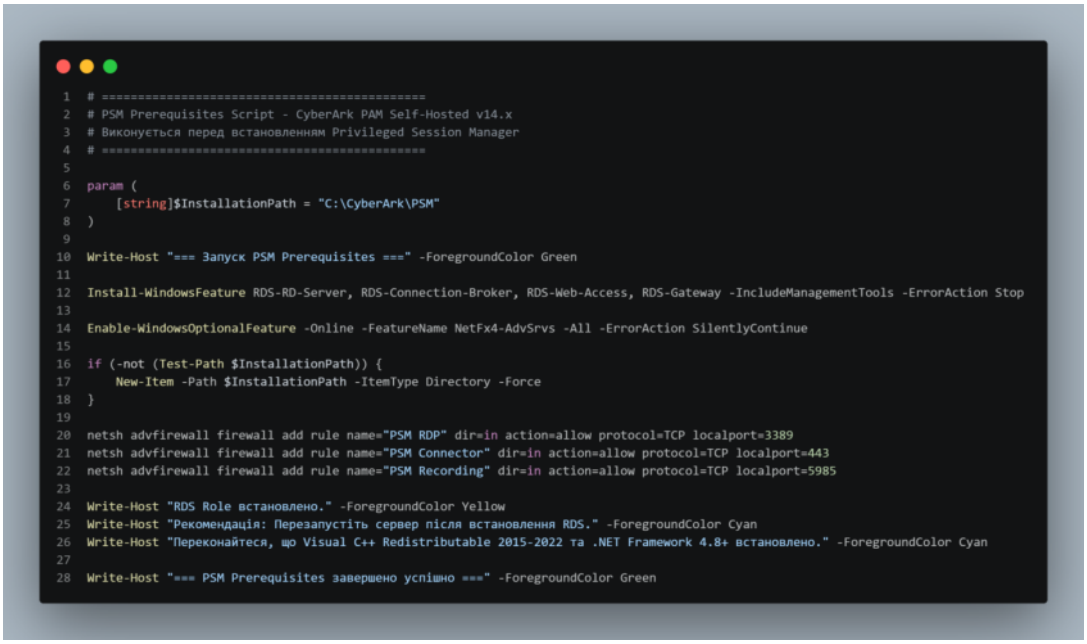


```
# ========================================
# CPM Installation Script - CyberArk PAM Self-Hosted v14.x
# ========================================

param (
    [string]$ConfigFile = ".\InstallationConfig.xml"
)

Write-Host "=== Початок автоматичного встановлення CPM ===" -ForegroundColor Green


if (-not (Test-Path $ConfigFile)) {
    Write-Host "Помилка: Файл $ConfigFile не знайдено!" -ForegroundColor Red
    exit 1
}


try {
    .\Setup.exe /Silent /Config $ConfigFile
    Write-Host "Встановлення CPM завершено успішно." -ForegroundColor Green
}
catch {
    Write-Host "Помилка під час встановлення: $($_.Exception.Message)" -ForegroundColor Red
    exit 1
}


Write-Host "Виконання реєстрації CPM..." -ForegroundColor Yellow
$RegistrationPath = "..\Registration\CPMRegisterComponent.ps1"
if (Test-Path $RegistrationPath) {
    & $RegistrationPath -spwd "StrongP@ssw0rdForLab123!"
    Write-Host "Реєстрація CPM завершена." -ForegroundColor Green
}

Write-Host "=== Встановлення CPM повністю завершено ===" -ForegroundColor Cyan
Write-Host "Рекомендація: Перевірте статус сервісу CyberArk Central Policy Manager у services.msc" -ForegroundColor White
```

Рисунок Б.3 – Основний скрипт встановлення CPMInstallation.ps1

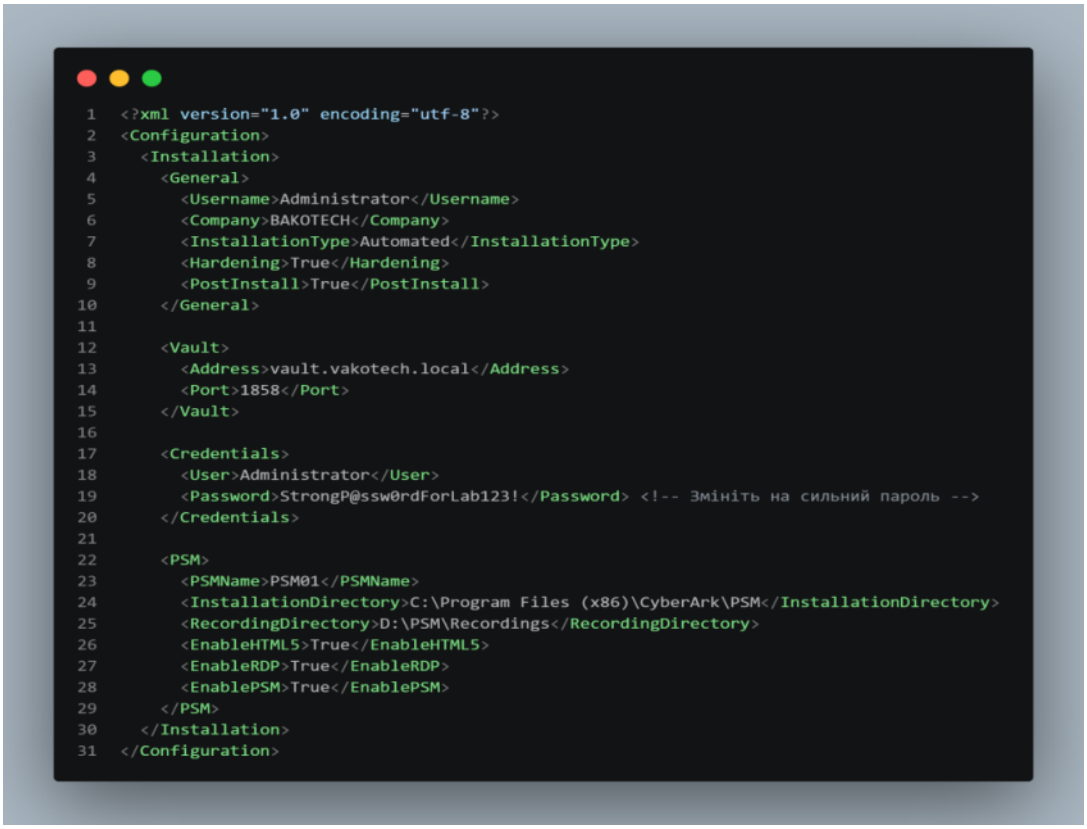
Додаток В

Скрипти встановлення Privileged Session Manager (PSM)



```powershell
# ==========================================
# PSM Prerequisites Script - CyberArk PAM Self-Hosted v14.x
# Виконується перед встановленням Privileged Session Manager
# ==========================================

param (
    [string]$InstallationPath = "C:\CyberArk\PSM"
)

Write-Host "=== Запуск PSM Prerequisites ===" -ForegroundColor Green

Install-WindowsFeature RDS-RD-Server, RDS-Connection-Broker, RDS-Web-Access, RDS-Gateway -IncludeManagementTools -ErrorAction Stop

Enable-WindowsOptionalFeature -Online -FeatureName NetFx4-AdvSrvs -All -ErrorAction SilentlyContinue

if (-not (Test-Path $InstallationPath)) {
    New-Item -Path $InstallationPath -ItemType Directory -Force
}

netsh advfirewall firewall add rule name="PSM RDP" dir=in action=allow protocol=TCP localport=3389
netsh advfirewall firewall add rule name="PSM Connector" dir=in action=allow protocol=TCP localport=443
netsh advfirewall firewall add rule name="PSM Recording" dir=in action=allow protocol=TCP localport=5985

Write-Host "RDS Role встановлено." -ForegroundColor Yellow
Write-Host "Рекомендація: Перезапустіть сервер після встановлення RDS." -ForegroundColor Cyan
Write-Host "Переконайтеся, що Visual C++ Redistributable 2015-2022 та .NET Framework 4.8+ встановлено." -ForegroundColor Cyan

Write-Host "=== PSM Prerequisites завершено успішно ===" -ForegroundColor Green
```

Рисунок В.1 – Скрипт перевірки передумов PSM_PreInstallation.ps1



```xml
<?xml version="1.0" encoding="utf-8"?>
<Configuration>
  <Installation>
    <General>
      <Username>Administrator</Username>
      <Company>BAKOTECH</Company>
      <InstallationType>Automated</InstallationType>
      <Hardening>True</Hardening>
      <PostInstall>True</PostInstall>
    </General>

    <Vault>
      <Address>vault.vakotech.local</Address>
      <Port>1858</Port>
    </Vault>

    <Credentials>
      <User>Administrator</User>
      <Password>StrongP@ssw0rdForLab123!</Password> <!-- Змініть на сильний пароль -->
    </Credentials>

    <PSM>
      <PSMName>PSM01</PSMName>
      <InstallationDirectory>C:\Program Files (x86)\CyberArk\PSM</InstallationDirectory>
      <RecordingDirectory>D:\PSM\Recordings</RecordingDirectory>
      <EnableHTML5>True</EnableHTML5>
      <EnableRDP>True</EnableRDP>
      <EnablePSM>True</EnablePSM>
    </PSM>
  </Installation>
</Configuration>
```

Рисунок В.2 – Конфігураційний файл InstallationConfig.xml для PSM

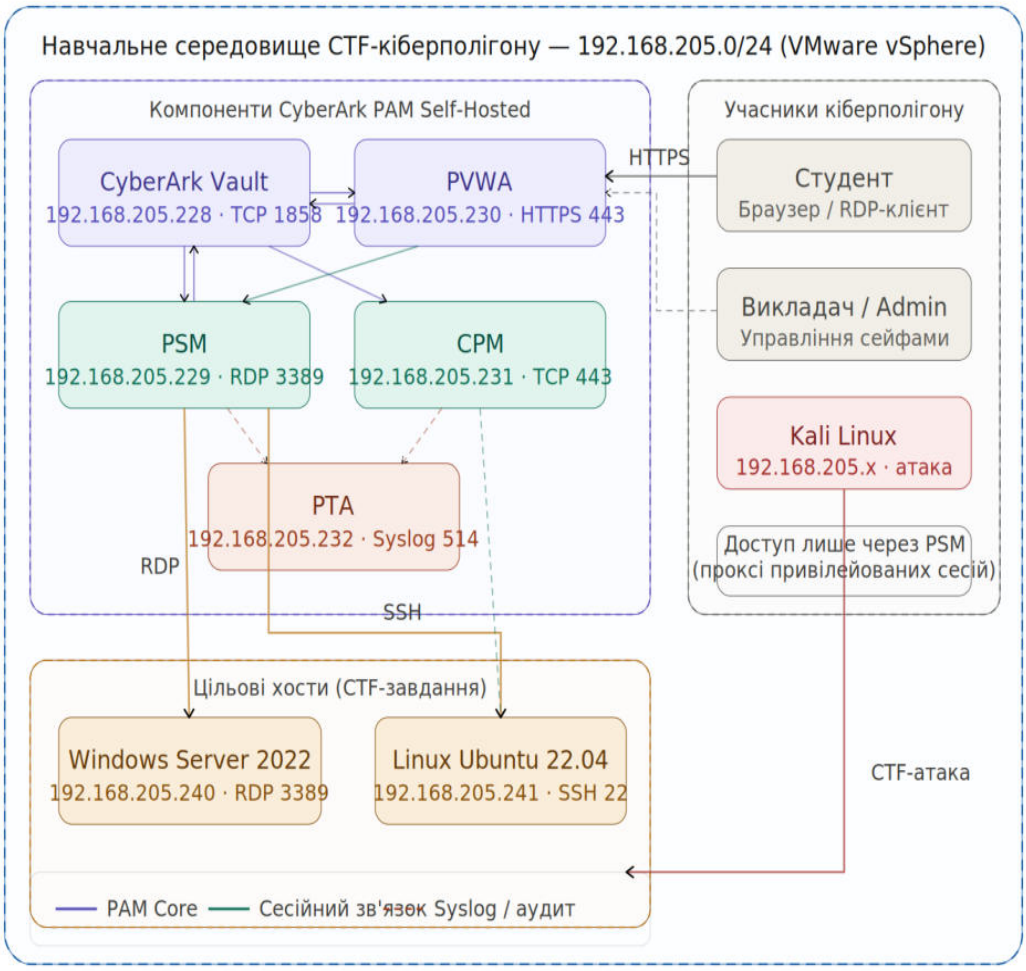


Рисунок В.3 – Основний скрипт встановлення PSMInstallation.ps1

Додаток Г

Знімки екрана з виконанням практичних завдань кіберполігону

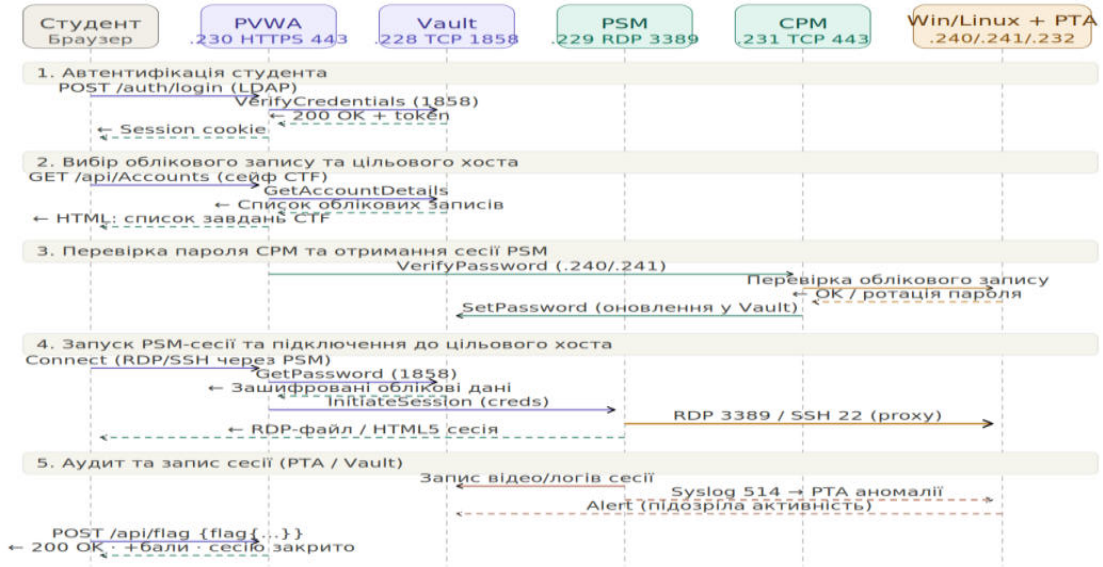


Рисунок Г.1 – Вхід до PVWA: сторінка авторизації student_user (завдання 1)

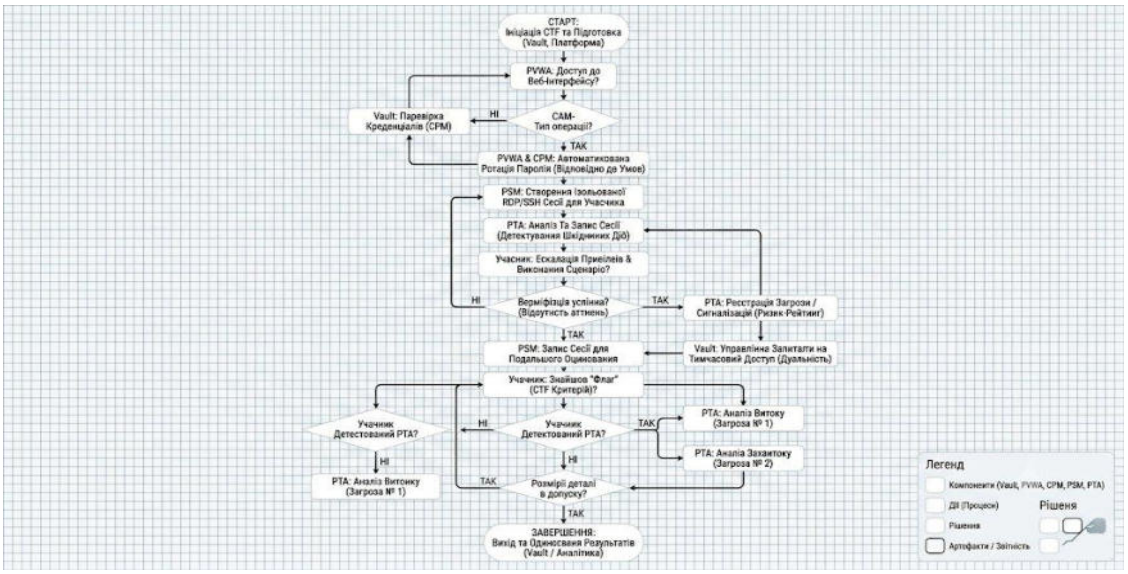


Рисунок Г.2 – Список облікових записів сейфу Training-Windows у PVWA (завдання 1)

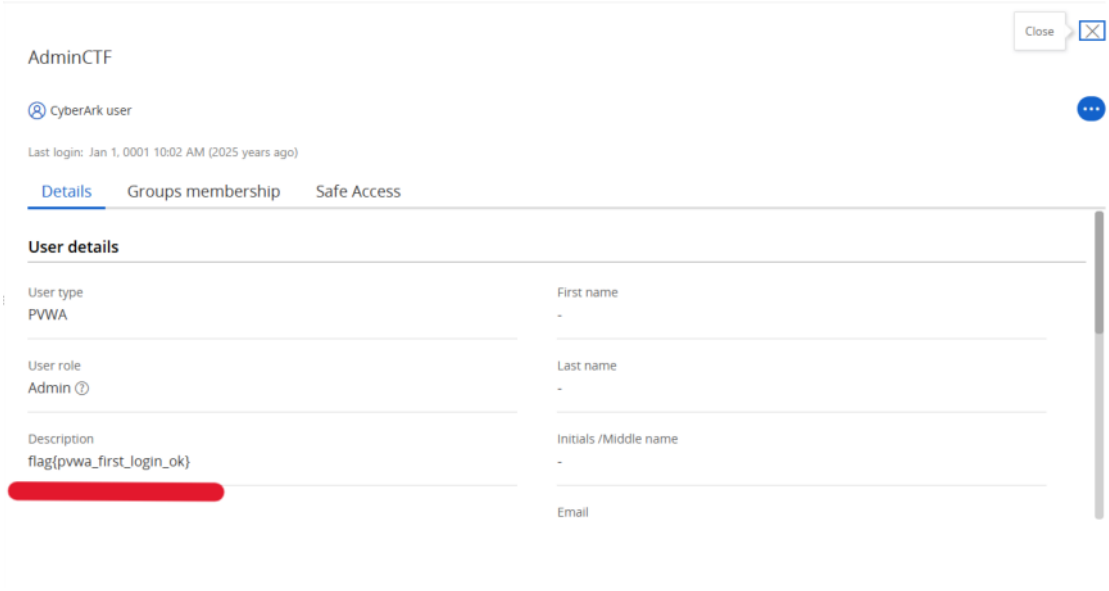


Рисунок Г.3 – Поле Description облікового запису Administrator з флагом завдання 1

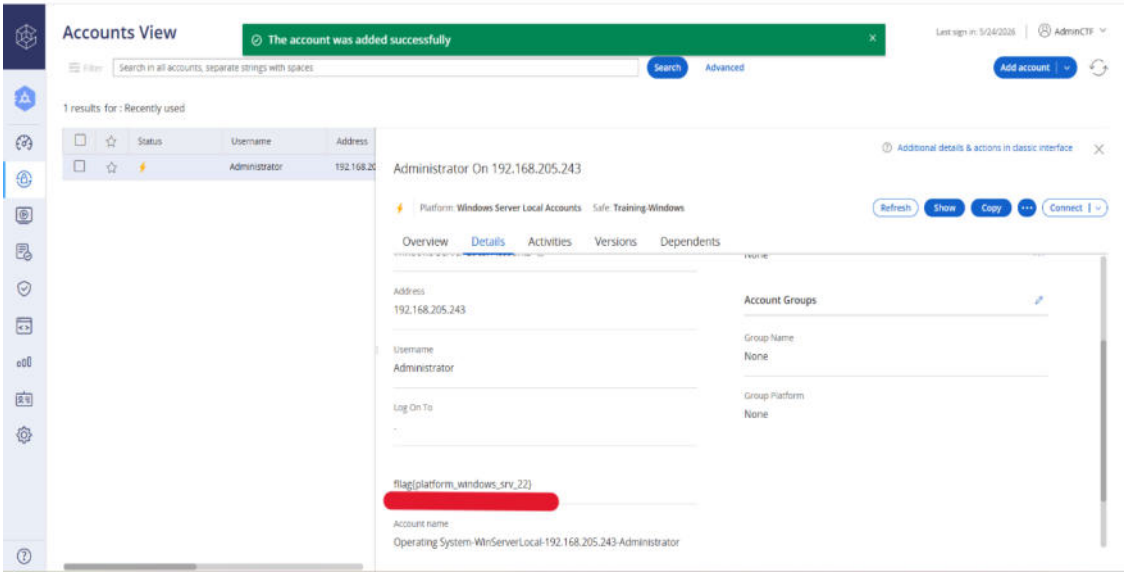


Рисунок Г.4 – Кастомне поле CTF_Flag у деталях облікового запису (завдання 2)

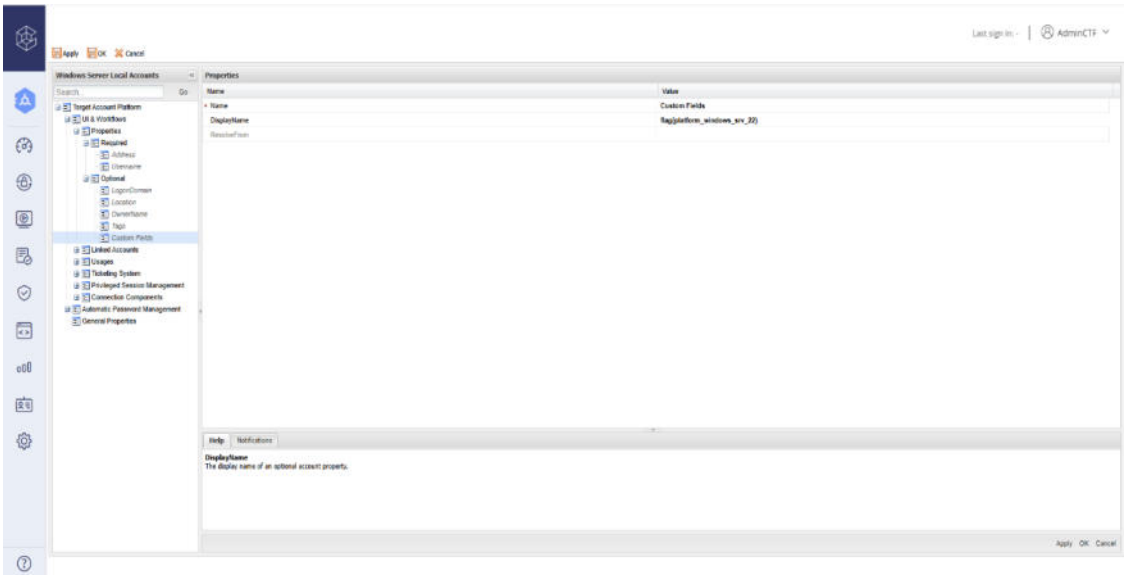


Рисунок Г.5 – Платформа Windows Server Local Accounts та її властивості (завдання 2)

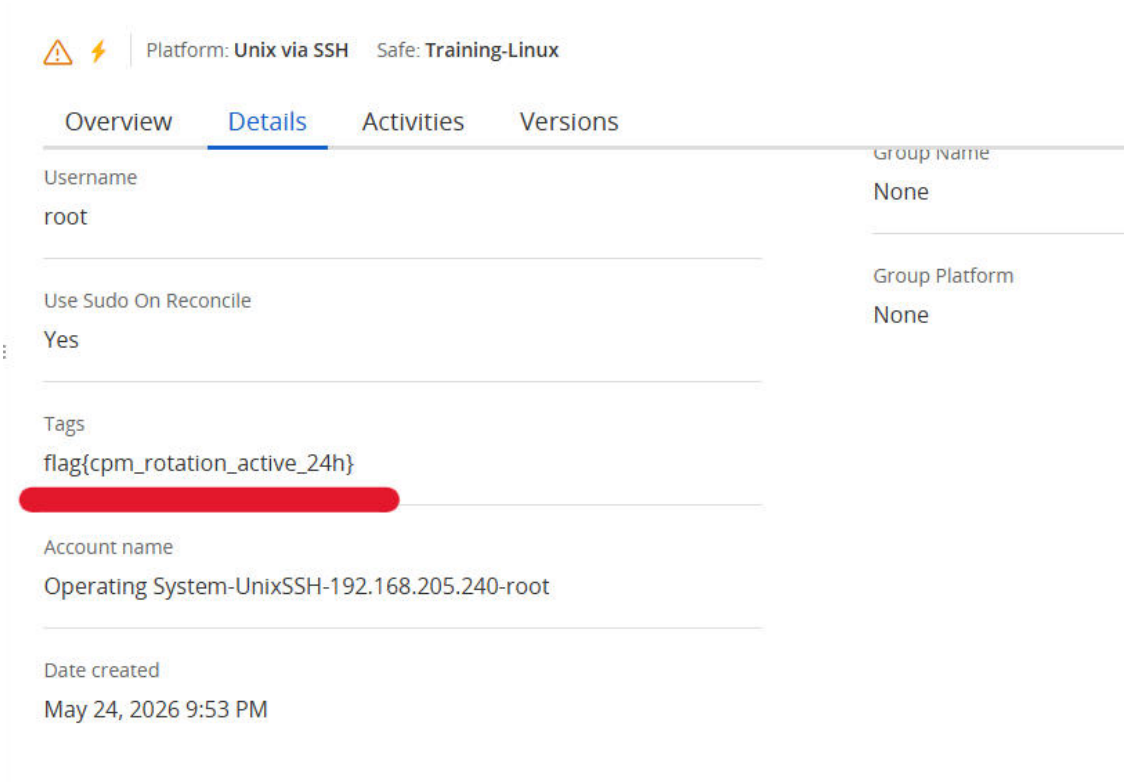


Рисунок Г.6 – Поле CTF_Flag та статус CPM Status = Success для облікового запису root (завдання 3)

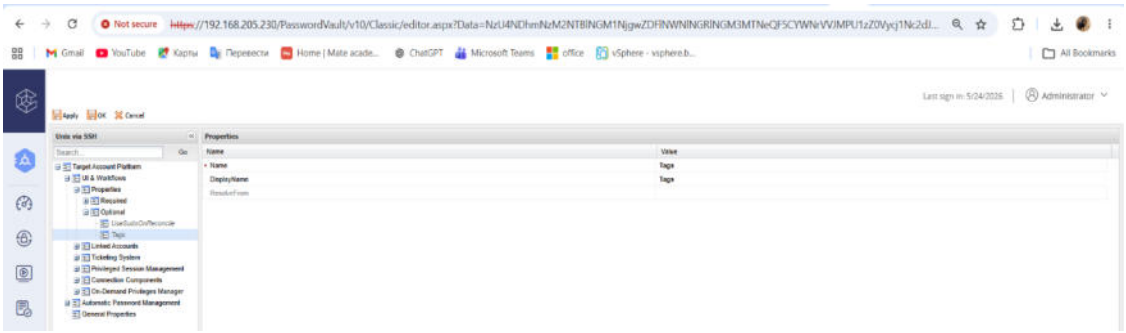


Рисунок Г.7 – Порівняння CPM Status: керований (Success) та некерований (Not Managed) акаунти (завдання 3)

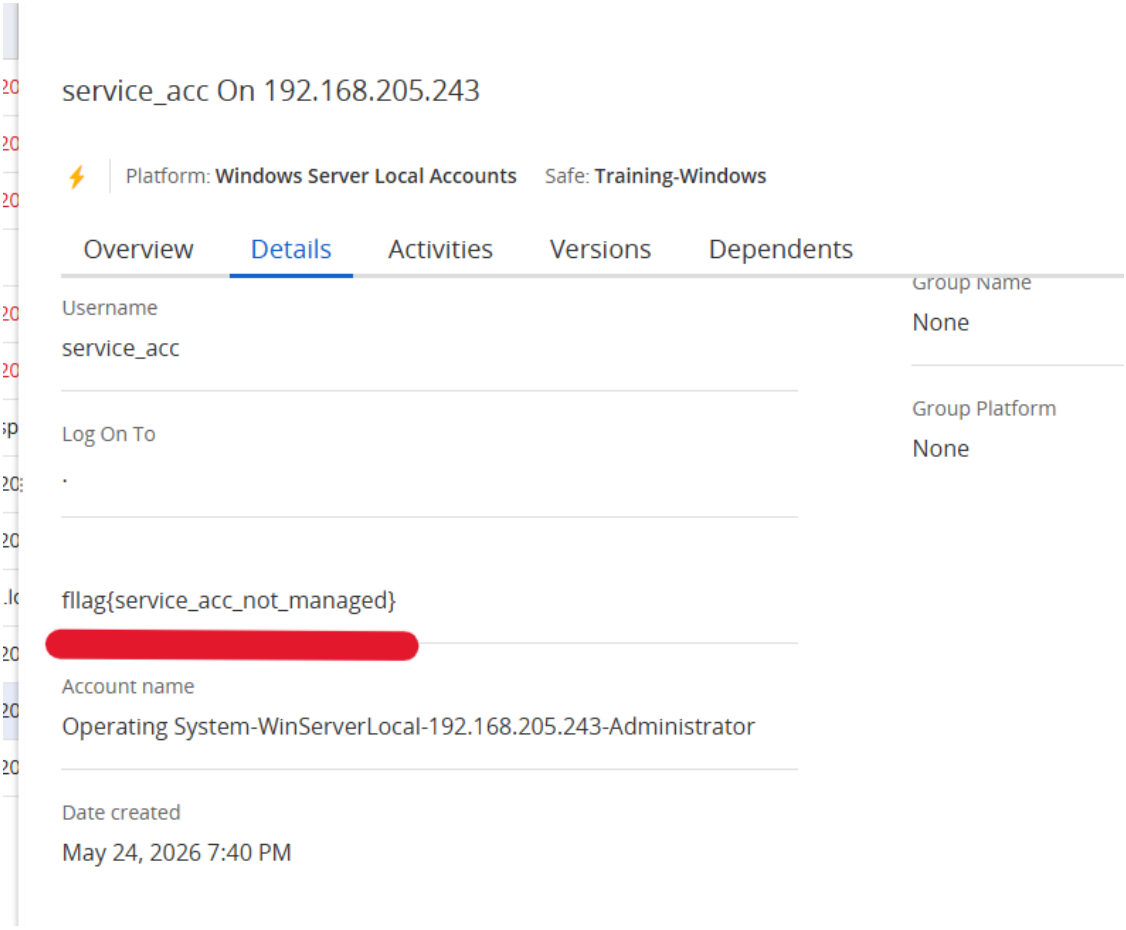


Рисунок Г.8 – Поле Description облікового запису service_account з флагом завдання 4

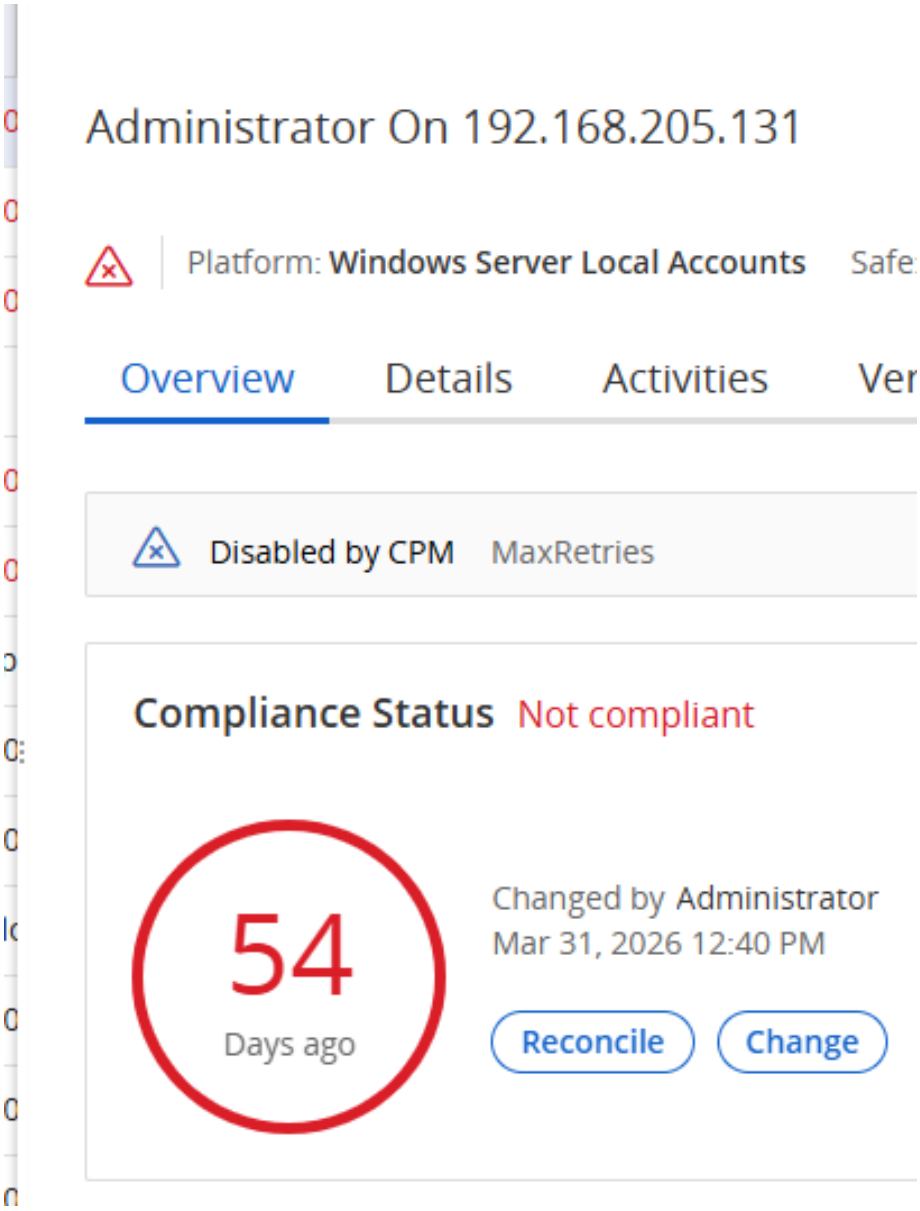


Рисунок Г.9 – CPM Status = Not Managed та поле Password Last Changed для service_account (завдання 4)

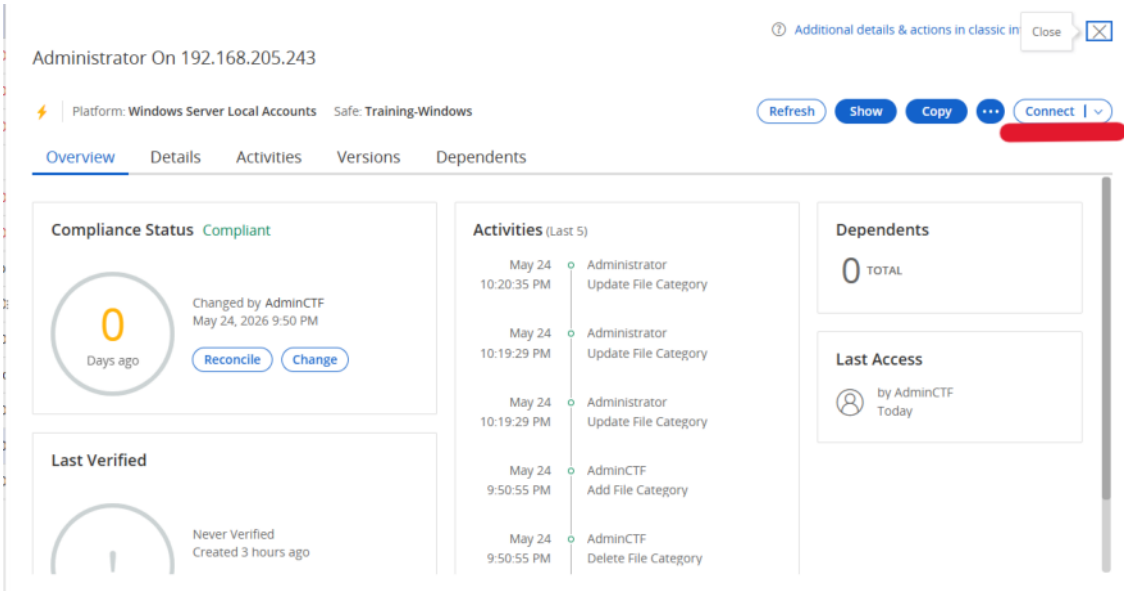


Рисунок Г.10 – Ініціювання PSM-RDP з’єднання через кнопку Connect у PVWA (завдання 5)

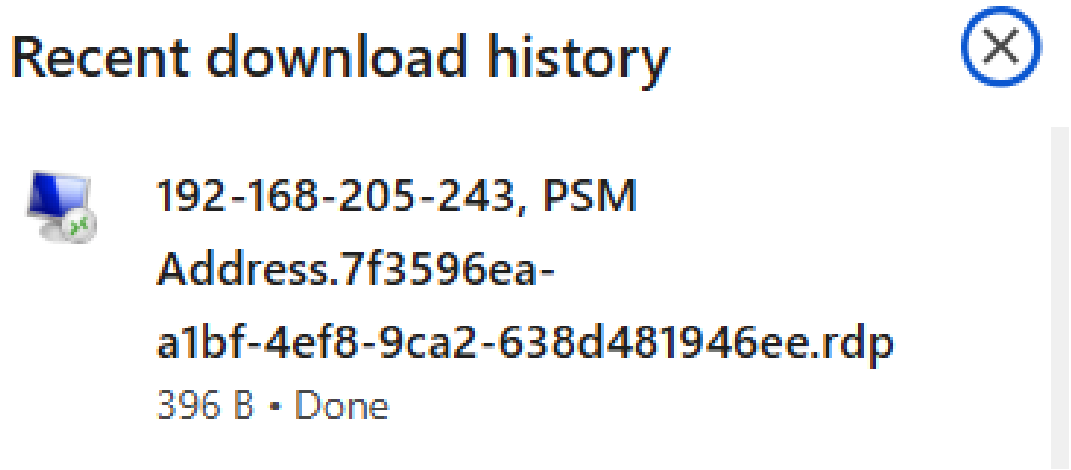


Рисунок Г.11 – Завантаження RDP-файлу активної PSM-сесії без розкриття пароля (завдання 5)

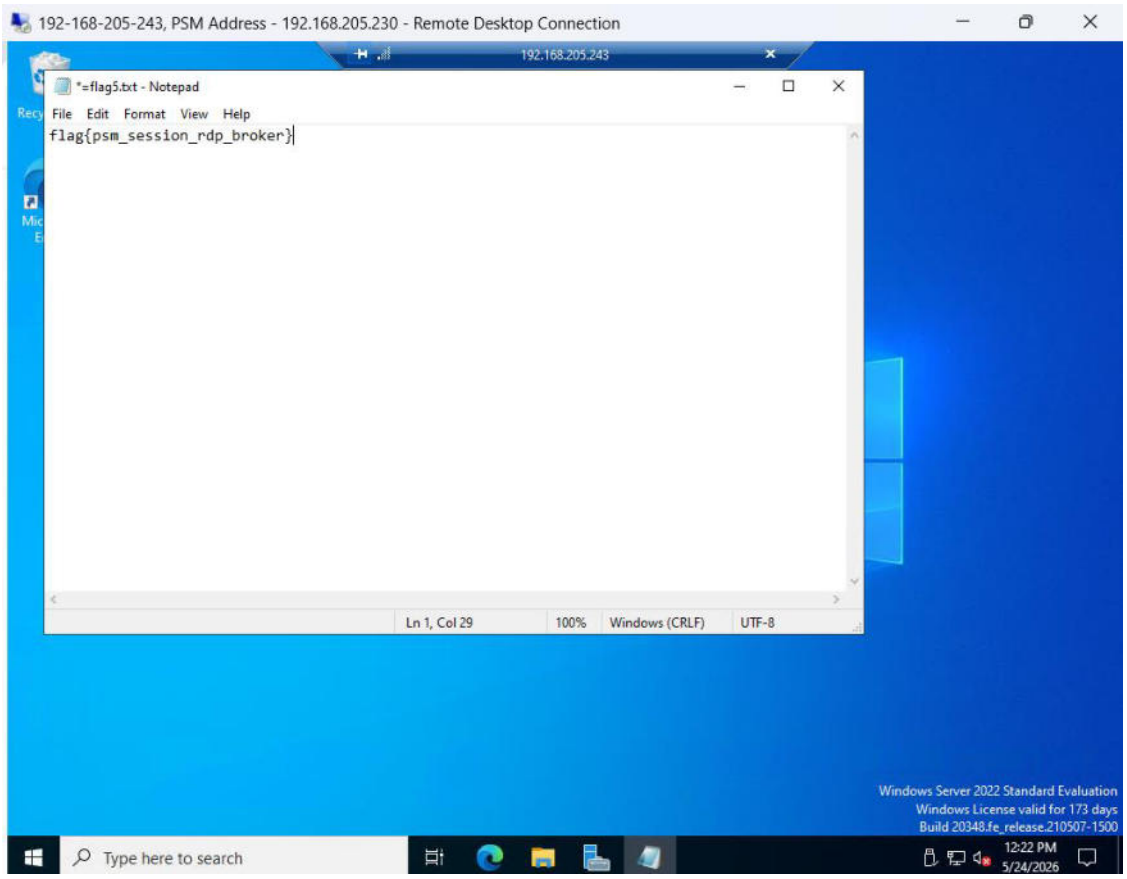


Рисунок Г.12 – Файл C:\flags\flag5.txt з флагом завдання 5 на цільовому хості

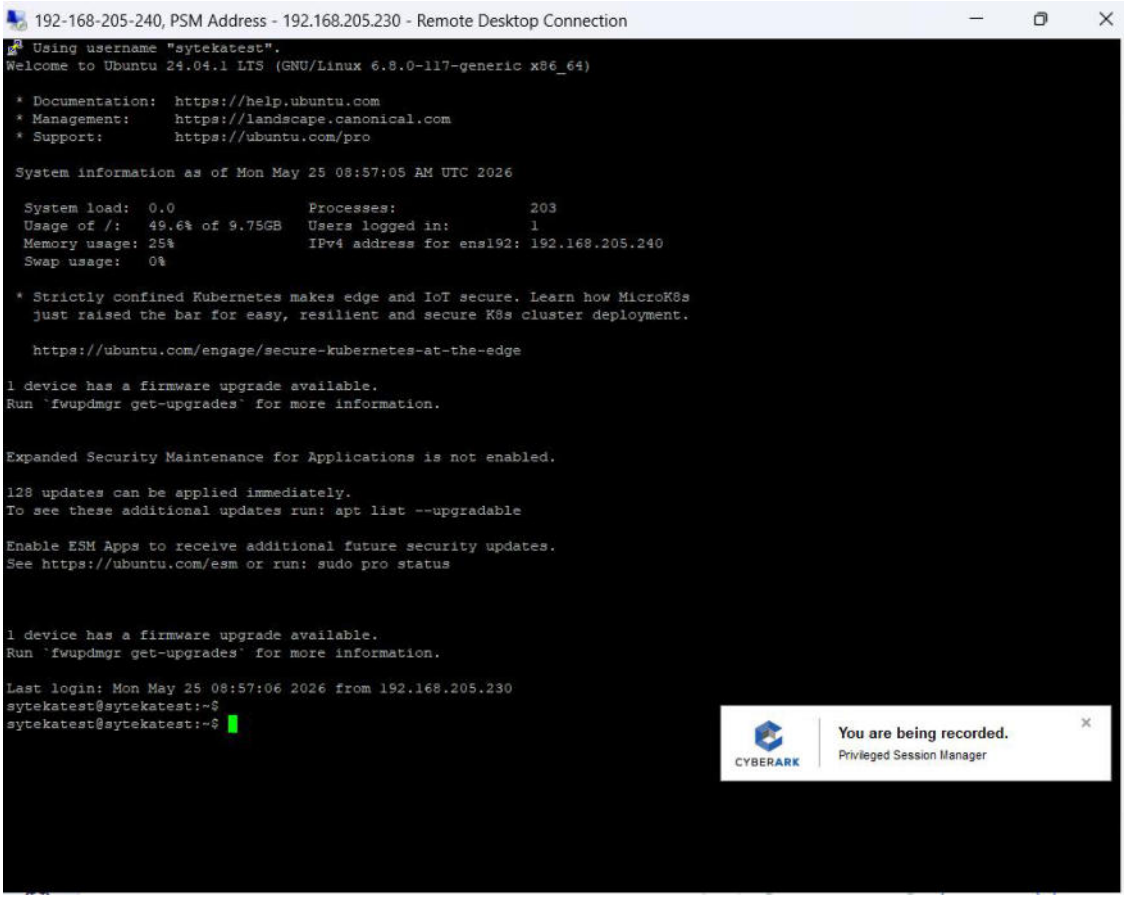


Рисунок Г.13 – PSM-SSH-сесія до Linux-сервера під обліковим записом root (завдання 6)

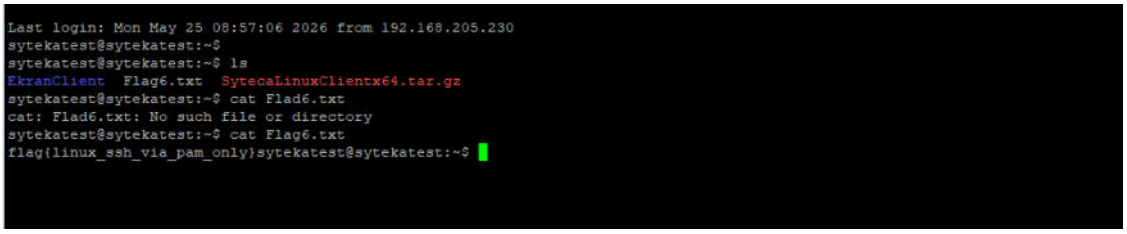


Рисунок Г.14 – Виконання команди cat /opt/flags/flag6.txt у PSM-SSH-терміналі (завдання 6)

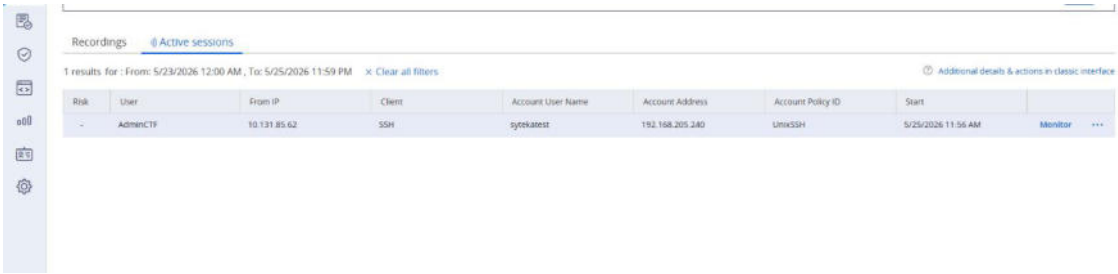


Рисунок Г.15 – Список активних сесій у PVWA: сесія domain_admin без тікету (завдання 7)

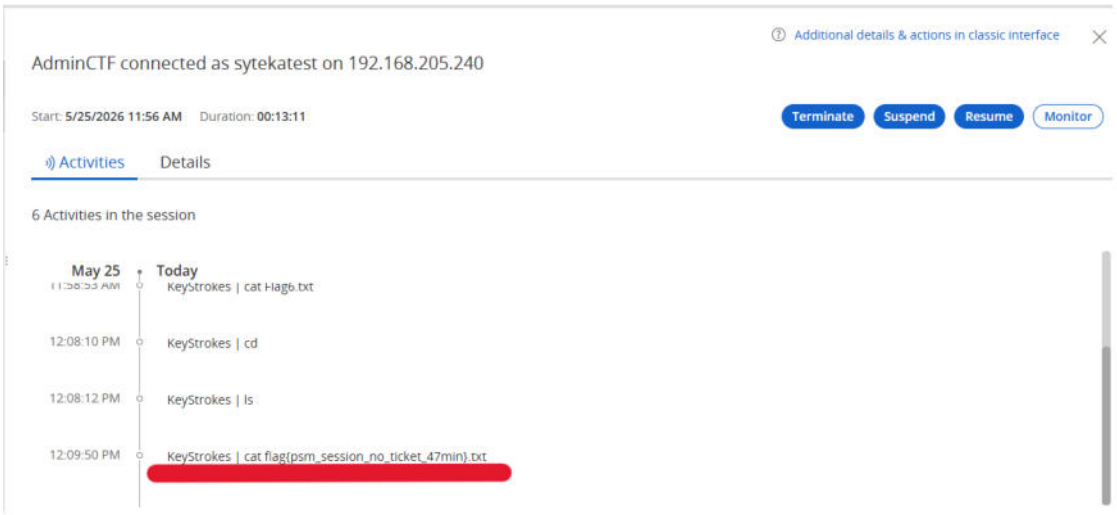


Рисунок Г.16 – Деталі підозрілої PSM-сесії: поле Session Note з флагом завдання 7

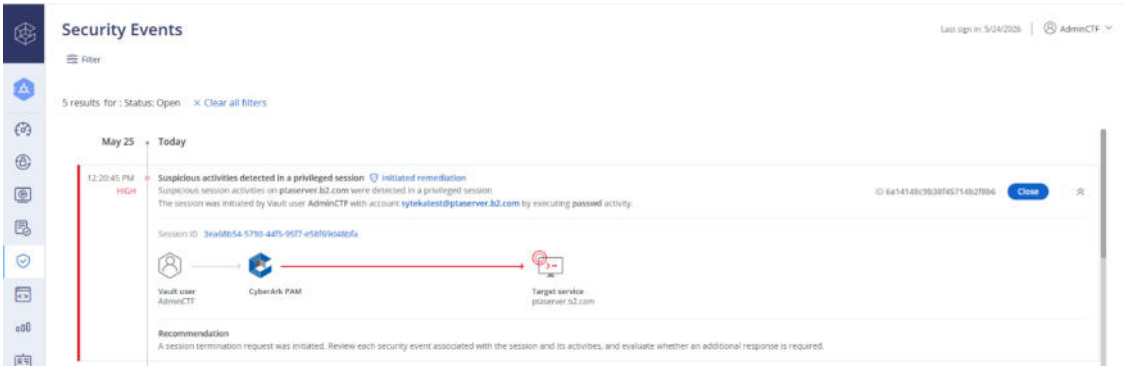


Рисунок Г.17 – PTA Security Events: алерт типу Suspicious Connection Source (завдання 8)

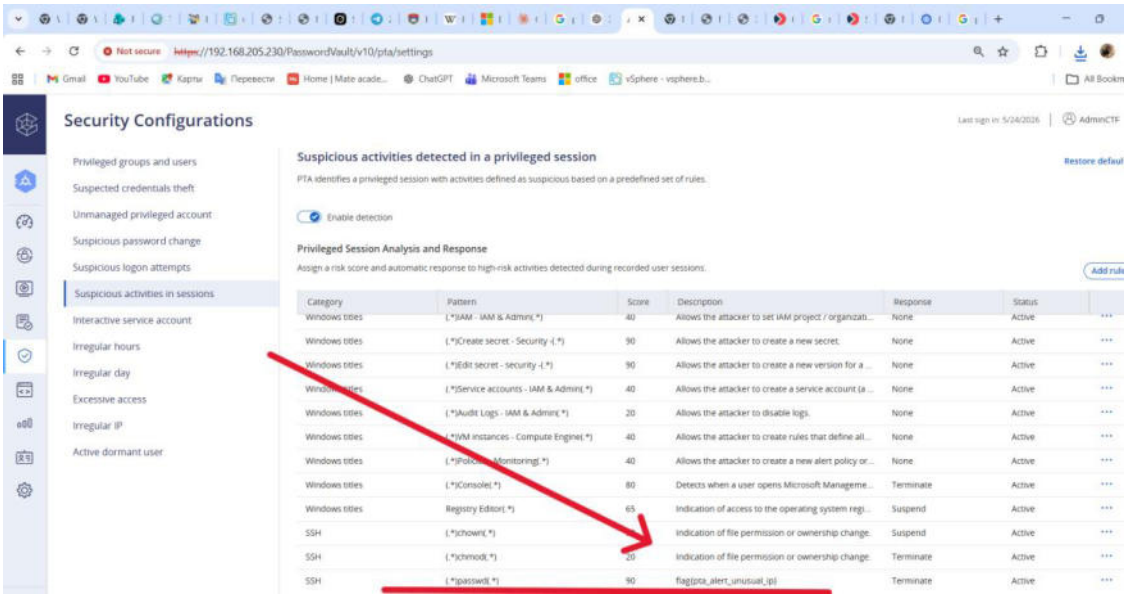


Рисунок Г.18 – Деталі PTA-алерту з полем Comment, що містить флаг завдання 8