КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
БУДІВНИЦТВА І АРХІТЕКТУРИ

Факультет автоматизації та інформаційних технологій · Кафедра кібербезпеки та комп'ютерної інженерії

КВАЛІФІКАЦІЙНА РОБОТА · СТУПІНЬ ВИЩОЇ ОСВІТИ «БАКАЛАВР»

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

Здобувач: **Тарасов Максим Ілліч**
Спеціальність 125 «Кібербезпека» · Група БІКС-22

Науковий керівник: к.т.н., доц. Делембовський М. М.

Київ, 2026

АКТУАЛЬНІСТЬ · ПОСТАНОВКА ПРОБЛЕМИ

Атаки на привілейовані акаунти організацій

Привілейовані облікові записи — головна ціль

Компрометація адмінських акаунтів дає атакувальнику повний контроль над інфраструктурою — від банків до критичної інфраструктури.

В умовах гібридної агресії проти України атаки на критичну інфраструктуру через PAM-системи набувають стратегічного значення.

Традиційні лекції та ізольовані лабораторії не формують реального досвіду роботи з enterprise-системами захисту.

27%

інцидентів в Україні — атаки на привілейований доступ і PAM-системи

CERT-UA, 2024

49%

порушень безпеки у світі пов’язані з компрометацією привілейованих даних

Verizon DBIR

+63%

зростання кіберінцидентів в Україні; понад 4 500 випадків за рік

CERT-UA, 2024

43%

роботодавців вимагають знань PAM-систем від випускників

ринок праці

НАПРЯМ ДОСЛІДЖЕННЯ

Мета, об’єкт та завдання роботи

МЕТА

Розробити та обґрунтувати модель CTF-кіберполігону на базі системи привілейованого доступу PAM CyberArk як ефективного інструменту практичної підготовки здобувачів спеціальності 125 «Кібербезпека».

Об’єкт

Процес практичної підготовки здобувачів вищої освіти спеціальності 125 «Кібербезпека».

Предмет

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

Основні завдання

1. Дослідити теоретичні основи та класифікацію CTF-кіберполігонів
2. Проаналізувати нормативно-правову базу й педагогічні аспекти їх застосування
3. Оцінити стан практичної підготовки за спеціальністю 125
4. Провести порівняльний аналіз існуючих платформ і кіберполігонів
5. Розробити та апробувати модель кіберполігону на базі PAM CyberArk

ЗАПРОПОНОВАНЕ РІШЕННЯ

Ідея: CTF-кіберполігон на базі PAM CyberArk

Навчати на справжній enterprise-системі захисту, а не на симуляції. Студенти працюють із реальною промисловою PAM-системою CyberArk Self-Hosted, розгорнутою у виробничому середовищі компанії ВАКОТЕСН, виконуючи завдання у форматі «захоплення прапора» (CTF).

Реальна PAM-система

CyberArk Self-Hosted v14.x: Vault, PVWA, PSM, CPM, PTA у єдиному середовищі.

Формат CTF

9 завдань трьох рівнів складності з прапорами та 100-бальною системою оцінювання.

Принцип least privilege

Ролі студента, аудитора й адміна; сейфи та акаунти як у справжній організації.

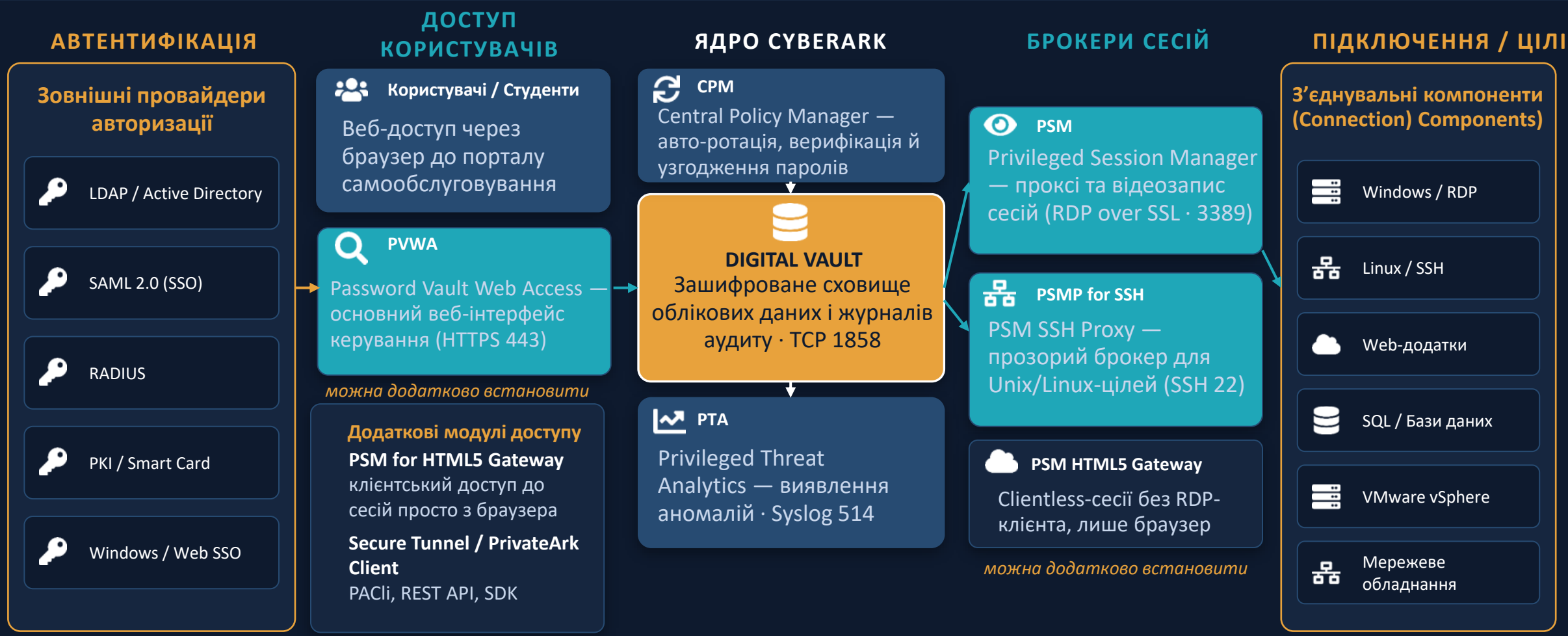
Прив'язка до ПРН

Завдання прямо формують програмні результати навчання Стандарту 125.

Вхід студента › Запит / ротація пароля › PSM-сесія до цілі › Пошук прапора › Аудит та аналітика PTA

ПОВНА АРХІТЕКТУРА PAM CYBERARK

Базові компоненти, додаткові модулі, підключення та авторизація



Базове ядро та сховище

Базові компоненти доступу та сесій

Додаткові модулі / підключення (опційно)

РОЗГОРТАННЯ ТА КОНФІГУРАЦІЯ

Компоненти CyberArk PAM та їх ролі

Vault	Зашифроване сховище облікових даних, паролів і журналів аудиту — єдина точка контролю.	TCP 1858
PVWA	Веб-портал керування сховищем: акаунти, політики, звіти, провіжинг користувачів.	HTTPS 443
CPM	Автоматична ротація, верифікація й узгодження паролів (Discovery → Analyze → Provision).	TCP 443
PSM	Брокер привілейованих сесій із повним відеозаписом; працює як проксі, не розкриваючи паролів.	RDP 3389
PTA	Аналітика загроз: виявлення підозрілої активності та аномалій у реальному часі.	Syslog 514

Принципи розгортання

- **Єдиний порт**
  Усі компоненти звертаються до Vault через захищений TCP 1858 — спрощене правило firewall за принципом мінімальних привілеїв.
- **Дворівневий доступ**
  Контроль на рівні Vault (Admins, Auditors, Users) і на рівні Сейфів (гранулярні права на групи акаунтів).
- **Mandatory Access Control**
  Мережеві зони за IP-діапазонами та часові вікна доступу до сейфів.
- **Self-Hosted v14.x**
  Primary-DR архітектура; Vault — вручну, інші компоненти — автоматизовано (скрипти в додатках).

СТРУКТУРА НАВЧАЛЬНОГО СЕРЕДОВИЩА

Сейфи, облікові записи та ролі (least privilege)

4 сейфи: Training-Windows, -Linux, -Audit, -Flags

7 цільових облікових записів (зокрема прихований backup_admin)

3 ролі: cyberark_admin ·student_user · auditor_user

Облікові записи у навчальних сейфах

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

Роль Junior PAM Analyst

Права student_user точно відтворюють реальну посаду:

Дозволено: List, Use (PSM), Retrieve (masked)

Заборонено: Add, Delete, Modify, Rename, Manage Safe

Прапори зберігаються у трьох місцях:

- поля Properties акаунтів у PVWA
- файли на цільових хостах (через PSM)
- журнали сесій та коментарі алертів PTA

ЗАСТОСУВАННЯ · ОБОРОНА

Сценарії Blue Team на кіберполігоні

Полігон навчає захисників виявляти, моніторити, розслідувати та реагувати — використовуючи штатні засоби PAM як інструмент Blue Team.

Моніторинг сесій

Перегляд та відеозапис привілейованих сесій через PSM; контроль активних підключень і перехоплення підозрілих сесій без квитка.

PSM · PVWA Active Sessions

Виявлення аномалій

Аналіз алертів CyberArk PTA: незвичні IP, аномальна поведінка, ескалація привілеїв у реальному часі.

PTA · Security Events

Forensics та аудит

Робота auditor_user із сейфом Training-Audit: розслідування інцидентів за журналами й артефактами сесій.

Auditor · Training-Audit

Контроль облікових даних

Аудит керованих і некерованих акаунтів, перевірка ротації CPM, виявлення прихованих акаунтів (Pending).

CPM · Pending Accounts

ГНУЧКІСТЬ ПЛАТФОРМИ

Можливості застосування в інших сценаріях

Red Team / наступальні сценарії

- Ескалація привілеїв та виконання CTF-сценарію в ролі студента
- Експлуатація некерованого акаунту (service_account поза CPM)
- Виявлення прихованого backup_admin через Pending Accounts
- Attack-Defense та King of the Hill між командами

Інші формати CTF за векторами загроз

- Email forensics — аналіз фішингу та аномалій (PTA)
- Ransomware forensics — аналіз артефактів шкідливого ПЗ
- Supply chain — reverse engineering, мережева forensics
- Web CTF (Jeopardy) — OWASP, безпека веб-додатків

Розширюваність середовища

Нові підключення

Web, SQL, VMware, мережеве обладнання як цілі через Connection Components

Інтеграція авторизації

LDAP/AD, SAML SSO, RADIUS, PKI — гнучка автентифікація учасників

Хмарне розгортання

Дистанційна версія полігону; масштабування під потоки студентів

Інтеграція з SIEM

Передача журналів у Splunk / Sentinel / QRadar для SOC-сценаріїв

ПРОРОБЛЕНА РОБОТА

Практична реалізація: CTF-завдання

9	практичних завдань
3	рівні складності
100	балів максимум
5	компонентів задіяно

Рівень 1 — Знайомство з PVWA

- 1 · Перший вхід: опис акаунту
- 2 · Платформа: кастомне поле
- 3 · Ротація паролів (CPM)
- 4 · Некерований акаунт

Рівень 2 — Робота з PSM

- 5 · Підключення через PSM (RDP)
- 6 · SSH без пароля (PSM)
- 7 · Перехоплення активної сесії

Рівень 3 — Реагування

- 8 · PTA-алерт: аномальний IP
- 9 · Підсумковий рапорт ризиків

Персональний md5-флаг (анти-списування)

Розгорнуто реальну CyberArk PAM Self-Hosted v14.x у середовищі BAKOTECH · структура сейфів і акаунтів · методика заняття (3–4 год) · Картка учасника · 100-бальна система оцінювання.

ОСВІТНЯ ЦІННІСТЬ

Відповідність ПРН Стандарту 125 «Кібербезпека»

Модель прямо забезпечує програмні результати навчання **Стандарту вищої освіти 125 «Кібербезпека» (наказ МОН України № 1547 від 29.10.2024).**

ПРН-3	**Виявляти та аналізувати вразливості інформаційних систем**	→	Пошук вразливостей у завданнях Jeopardy та Attack-Defense
ПРН-7	**Реагувати на кіберінциденти та розслідувати їх**	→	Forensics-сценарії, аналіз журналів аудиту CyberArk PTA
ПРН-9	**Здійснювати моніторинг та аудит безпеки**	→	Робота з PVWA, перегляд сесій PSM, аналіз подій CPM
ПРН-11	**Застосовувати сучасні інструменти захисту інформації**	→	Безпосередня робота з enterprise PAM — лідером ринку за Gartner
ПРН-14	**Приймати рішення в умовах невизначеності та часового тиску**	→	Змагальний CTF-формат із таймером формує швидкість реакції

ПІДСУМКИ

Висновки та перспективи

Виконано в роботі

- Розроблено та апробовано модель CTF-кіберполігону на реальній enterprise-системі CyberArk PAM Self-Hosted у середовищі ВАКОТЕСН
- Описано архітектуру й покроково розгорнуто 5 компонентів (Vault, PVWA, CPM, PSM, PTA), 4 сейфи та 7 акаунтів за принципом least privilege
- Створено 9 практичних CTF-завдань трьох рівнів, систему прапорів і 100-бальне оцінювання
- Обґрунтовано вибір PAM як бази: 27 % інцидентів в Україні — атаки на привілейований доступ

Стандарт спеціальності 125

Модель забезпечує ПРН-3, 7, 9, 11, 14 Стандарту вищої освіти 125 «Кібербезпека» — наказ МОН України № 1547 від 29.10.2024.

Подальші перспективи

- інтеграція з SIEM-системами
- автоматизація перевірки прапорів
- інноваційна версія полігону
- CTF-змагання

Мету роботи досягнуто: enterprise-PAM CyberArk підтверджено як ефективний інструмент практичної підготовки фахівців з кібербезпеки, що наближає навчання до реальних вимог ринку праці.