

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



Кваліфікаційна робота бакалавра

Сценарії мережевого «Penetration Testing» у віртуалізованому середовищі кіберполігону

Виконав: **Заремба Богдан Вадимович**

Київ · 2026



АКТУАЛЬНІСТЬ

Чому це потрібно

4,8 млн

Світовий дефіцит фахівців з кібербезпеки (ISC2)

90%

організацій головною проблемою називають розрив у практичних навичках

Опанувати пентест за підручником неможливо.

Потрібне ізольоване середовище з навмисно вразливими цілями, де студент безпечно відпрацьовує реальні атаки.

Практичні навички, а не теорія є вузьким місцем у підготовці фахівців.

МЕТА ТА ЗАВДАННЯ

Мета і завдання роботи



Розробити навчальні сценарії мережевого пентесту та програмний тренажер для їх виконання — придатний до інтеграції в навчальний процес кафедри.

П'ять задач — кожна розкрита далі окремим блоком доповіді:

- 1 Проаналізувати наявні рішення й обґрунтувати потребу
- 2 Спроекувати віртуалізоване середовище із сегментами та знімками стану
- 3 Розробити 5 сценаріїв (55 кроків) трьох рівнів складності
- 4 Реалізувати тренажер: автоматична перевірка, звіти, розширюваність
- 5 Провести апробацію за п'ятьма напрямками

Наявні рішення не закривають потребу



Комерційні платформи

HackTheBox, TryHackMe

- Англomовні
- 14–18 \$/міс за студента
- Потрібен інтернет
- Немає контролю викладача



Академічні полігони

КУРО

- 64+ ГБ ОЗП, 16 ядер
- Окремий адміністратор
- Складне розгортання



Безкоштовні мішені

Metasploitable, DVWA

- Лише мішені
- Без мережі та сценаріїв
- Без перевірки результату
- Без оцінювання

Розрив: немає безкоштовного українського засобу з готовими покроковими сценаріями, перевіркою відповідей і контролем викладача.

ЗАДАЧА 2 · СЕРЕДОВИЩЕ

Віртуалізоване середовище та знімки стану

Сегментоване середовище (Kali · pfSense · Metasploitable 2 · DC-1). Кожна VM має знімок `clean_state` — той самий набір машин постає в різній топології залежно від сценарію.

Сценарій 3 · pivot



MS2 з двома адаптерами працює мостом DMZ → Internal — можливий pivot до ізольованого DC-1.

Сценарій 5 · обхід фаєрвола



MS2 лише за pfSense (один адаптер). Фаєрвол інлайн з правилами — обхід має реальний ефект.

Той самий хост грає дві ролі — завдяки знімкам стану, без ручного переналаштування мережі.

ЗАДАЧА 3 · СЦЕНАРІЇ

Стандарти й методології в основі сценаріїв

Кожен сценарій — структурований ланцюг атаки, побудований на визнаних галузевих стандартах:



PTES

Penetration Testing Execution Standard

Задає послідовність процесу пентесту — 7 фаз від розвідки до звітування.



MITRE ATT&CK

Adversarial Tactics, Techniques & Common Knowledge

Матриця технік реальних атак; кожен крок має код (напр. T1190).



Cyber Kill Chain

Модель Lockheed Martin

7 етапів логіки атакувальника — від розвідки до дій над ціллю.

Також застосовано у роботі:

NIST SP 800-115

методика тестування ІБ (4 фази)

П'ять сценаріїв — прогресія складності

№	Сценарій	Рівень	Кроки	Ключові техніки та інструменти
1	Базовий пентест Metasploitable 2	Початковий	10	Nmap · vsftpd (CVE-2011-2523) · John the Ripper
2	Пентест додатку DVWA	Середній	10	SQL Injection · Command Injection · Hydra
3	Багатоетапна атака з pivot (DMZ → Internal)	Просунутий	15	Drupalgeddon2 · proxychains · SUID · збір кред.
4	Глибока мережева розвідка та enumeration	Середній	10	SYN/FIN/Xmas · NSE · enum4linux · NFS
5	Обхід stateful-фаєрвола	Просунутий	10	fragmentation · decoy · idle-scan · ACK-scan

Прогресія: експлуатація одного сервісу → веб-рівень → багатоетапна атака крізь кілька сегментів мережі.

Базовий пентест Metasploitable 2

Повний цикл атаки на окремий хост — від розвідки до зламу облікових даних.

Інструменти: Nmap · Metasploit Framework · John the Ripper

1

Розвідка

Nmap: хости й порти

T1046

2

Пошук CVE

версія vsftpd

T1190

3

Експлуатація

бекдор vsftpd → shell

T1190

4

Облікові дані

хеш з /etc/shadow

T1003

5

Злам пароля

John (режим single)

T1110.002

Сценарій 1: Базовий пентест Metasploitable 2

BEGINNER

90 хв

10 кроків

У цьому сценарії ви виконаєте базовий пентест проти **Metasploitable 2** — навмисно вразливої віртуальної машини на Ubuntu 8.04.

Пройдете перші фази методології PTES: розвідка → аналіз вразливостей → експлуатація → постексплуатація (аж до відновлення пароля з хешу).

Мережа:

- Атакуюча машина — Kali Linux (192.168.1.10)
- Шлюз DMZ — pfSense (192.168.1.1)
- Ціль — десь у мережі 192.168.1.0/24, її треба знайти

Як це працює: кожне поле відповіді — це результат конкретної команди в Kali. Команди в кожному кроці можна скопіювати кнопкою «Копіювати». Білі поля показано приклад очікуваного формату відповіді.

Навчальні цілі

- Засвоєння базових технік мережевої розвідки (host discovery, port scanning)
- Робота з Nmap для виявлення сервісів та їх версій
- Самостійний пошук CVE за виявленою версією ПЗ
- Використання Metasploit Framework для експлуатації відомих вразливостей
- Розуміння послідовності фаз методології PTES
- Базові навички постексплуатації Linux
- Відновлення паролів за хешами (offline cracking) за допомогою John the Ripper

Техніки MITRE ATT&CK

T1018 · Remote System Discovery T1046 · Network Service Discovery T1190 · Exploit Public-Facing Application
T1059 · Command and Scripting Interpreter T1082 · System Information Discovery T1003 · OS Credential Dumping
T1110.002 · Password Cracking

► Розпочати сценарій

Пентест додатку DVWA

Веб-застосунок як мережевий сервіс на порту 80 — типові вразливості OWASP.

Інструменти: Браузер · SQLmap · Hydra

1

Веб-сервер

Nmap, порт 80

T1046

2

Command Exec

RCE + файлова система

T1059

3

SQL Injection

Boolean + UNION SELECT

T1190

4

Витяг хешів

SQLi / SQLmap

T1555

5

XSS + Brute

Hydra на форму входу

T1110

Сценарій 2: Пентест веб-додатку DVWA

MEDIUM

150 хв

10 кроків

DVWA (Damn Vulnerable Web Application) — навмисно вразливий PHP/MySQL-додаток для навчання веб-пентесту. У цьому сценарії DVWA розгорнуто на Metasploitable 2 за адресою `http://192.168.1.100/dvwa/`. Ви попрацюєте з типовими веб-вразливостями: Command Injection, SQL Injection, XSS та Brute Force, проходячи фази розвідки, експлуатації та постексплуатації.

Облікові дані для входу в DVWA: `admin / password`. Після входу обов'язково відкрийте **DVWA Security** і встановіть рівень **Low**.

Підказка: кожне поле відповіді — це результат конкретної дії чи команди. Біля поля показано приклад очікуваного формату відповіді — орієнтуйтеся на нього.

Навчальні цілі

- Виявлення та аналіз веб-додатків з вразливостями
- Експлуатація SQL Injection вручну та через SQLmap
- Експлуатація Command Injection для віддаленого виконання коду
- Перевірка XSS-вразливостей (Reflected, Stored)
- Використання Burp Suite для перехоплення та модифікації HTTP-запитів
- Розуміння класифікації OWASP Top 10

Техніки MITRE ATT&CK

T1046 · Network Service Discovery T1595 · Active Scanning T1059 · Command and Scripting Interpreter
T1003 · File and Directory Discovery T1190 · Exploit Public-Facing Application
T1555 · Credentials from Password Stores T1189 · Drive-by Compromise T1110 · Brute Force

► Розпочати сценарій

Багатоетапна атака з pivot (DMZ → Internal)

Латеральний рух: компрометація DMZ → транзит → атака ізольованого DC-1.

Інструменти: Metasploit · proxychains · Nmap

1

Розвідка DMZ та Internal

Internal недоступний прямо

T1018

2

Initial Access

Samba на Metasploitable

T1190

3

Pivot

autoroute + SOCKS-проксі

T1090

4

Drupalgeddon2

DC-1 · CVE-2018-7600

T1190

5

Privesc + флаг

SUID find -exec

T1548.001

Сценарій 3: Багатоетапна атака з pivot через DMZ до Internal

ADVANCED

240 хв

15 кроків

Цей сценарій моделює реалістичну багатоетапну атаку проти корпоративної мережі. Завдання — пройти від зовнішнього сегменту до внутрішнього з privilege escalation на цільовому сервері.

Цільова інфраструктура:

- DMZ (192.168.1.0/24): Metasploitable 2 — публічний сервер; Kali Linux — ваша атакуюча машина (192.168.1.10)
 - Internal (10.10.10.0/24): DC-1 — внутрішній веб-сервер з вразливою CMS
 - pfSense (192.168.1.1 / 10.10.10.1) — маршрутизатор, що блокує прямий доступ DMZ → Internal
- Metasploit отримає root-доступ на DC-1, який недоступний напряму з Kali. Потрібно скомпрометувати Metasploitable 2 та використати його як pivot-точку для атак на Internal. Сценарій покриває всі 7 фаз PTES: Pre-engagement → Intelligence Gathering → Threat Modeling → Vulnerability Analysis → Exploitation → Post-Exploitation → Reporting.

Навчальні цілі

- Комплексне виконання усіх 7 фаз методології PTES
- Експлуатація мережевих сервісів для початкового доступу (Initial Access)
- Налаштування pivot та латерального руху (Lateral Movement)
- Експлуатація CMS Drupal через критичну вразливість Drupalgeddon2
- Privilege escalation через SUID-bit (find -exec)
- Збір облікових даних з конфігураційних файлів та БД
- Розуміння концепції захисту в глибину (Defense in Depth)

Техніки MITRE ATT&CK

T1046 · Network Service Discovery	T1190 · Exploit Public-Facing Application	T1059.004 · Unix Shell	T1090 · Proxy
T1018 · Remote System Discovery	T1003 · File and Directory Discovery	T1548.001 · Setuid and Setgid	
T1052.001 · Credentials in Files	T1003 · OS Credential Dumping	T1005 · Data from Local System	

▶ Розпочати сценарій

Глибока мережева розвідка та enumeration

Глибока розвідка й enumeration — фундамент будь-якої подальшої атаки.

Інструменти: Nmap (NSE) · enum4linux · Nikto · dirb

1

SYN / UDP

сканування портів

T1046

2

OS fingerprint

TCP/IP стек

T1082

3

NSE-скрипти

SMB-вразливості

T1595.002

4

enum4linux

SMB-облікові + NFS

T1087.001

5

Nikto / dirb

HTTP, приховані шляхи

T1595.001

Сценарій 4: Глибока мережева розвідка та enumeration

MEDIUM

120 хв

10 кроків

Розвідка (Reconnaissance) — найважливіша фаза будь-якого пентесту. Чим більше інформації про ціль зібрано пасивно та активно, тим точнішими будуть наступні фази атаки. У цьому сценарії ви виконаєте систематичну, багаторівневу розвідку проти навмисно вразливого сервера у DMZ — від мережевого рівня до рівня окремих сервісів.

Методологія: рух від загального до конкретного — спочатку host discovery, потім сканування портів різних типів, далі визначення версій сервісів, NSE-скрипти для глибокого аналізу та, нарешті, специфічна для протоколів enumeration (SMB, NFS, HTTP).

Мережеве оточення:

- Калі (192.168.1.10) — атакуюча машина
- Цільова машина (192.168.1.100) — об'єкт розвідки
- Шлюз pfSense (192.168.1.1)

Усі команди виконуються у Калі. Тримайте окремий термінал для запису результатів — наприкінці сценарію ви матимете повну fingerprint-карту цілі.

Навчальні цілі

- Опанування різних типів TCP-сканування (SYN, Connect, FIN, NULL, Xmas) та розуміння їх tradeoff'ів
- Сканування UDP-сервісів та особливості UDP-розвідки
- Використання Nmap NSE-скриптів для автоматизованого аналізу вразливостей
- Активне визначення версій сервісів та OS fingerprinting
- Розширена розвідка SMB-сервісів через enum4linux та nmap NSE
- Розвідка мережевих ресурсів NFS та небезпека відкритих експортів (world-readable shares)
- Брутфорс директорій веб-сервера через dirb/gobuster
- Інтеграція результатів розвідки у єдину картину для подальшої атаки

Техніки MITRE ATT&CK

- | | | |
|--------------------------------------|-------------------------------------|--------------------------------------|
| T1595 - Active Scanning | T1595.001 - Scanning IP Blocks | T1595.002 - Vulnerability Scanning |
| T1018 - Remote System Discovery | T1046 - Network Service Discovery | T1135 - Network Share Discovery |
| T1002 - System Information Discovery | T1007.001 - Local Account Discovery | T1003 - File and Directory Discovery |

► Розпочати сценарій

Обхід stateful-фаєрвола

Інструменти: Nmap · proxychains · tshark

1

Filtered/closed

розвідка крізь pfSense

T1046

2

Фрагментація

-f проти scrub

T1027

3

Decoy / spoof

підставні IP та порт

T1090

4

Idle scan

-sl через zombie

T1090

5

ACK-скан

мапа правил фаєрвола

T1595

Сценарій 5: Обхід stateful-фаєрвола та просунуте сканування

ADVANCED

150 хв

10 кроків

Цей сценарій — про зіткнення класичних технік ухилення Nmap із реальним stateful-фаєрволом (pfSense). Ви на власному стилі переконаєтесь, що проти правильно налаштованого фаєрвола більшість «трюків» (фрагментація, decoy, підміна порту-джерела, idle scan) не відкривають закриті порти — і це головний практичний урок для пентестера.

Топологія:

- Kali (атакувальник) — 192.168.1.10, шлюз 192.168.1.1
- pfSense — em0/LAN 192.168.1.1 (бік Kali), em1/LAN 10.10.10.1 (бік цілі)
- Ціль Metasploitable 2 — 10.10.10.50 (за фаєрволом, DMZ-карта вимкнена)

Політика фаєрвола: з мережі Kali до цілі дозволено лише `ssh/tcp` та `ICMP`; до решти портів (21, 22, 139, 445, 3306) трафік не доходить — pfSense мовчки відкидає пакети. Фаєрвол stateful, з увімкненим `scrub` (реасемблює IP-фрагменти) та `antispoof` на WAN.

Дві точки спостереження, `tcpdump/tshark` на Kali бачить усе, що ви відправляєте (до фаєрвола); до цілі ж доходить лише дозволене. Саме контраст між цими двома картинками пояснює, що насправді дає кожна техніка.

Етичне зауваження: усі техніки описано виключно для авторизованого тестування та навчання зазвичай. Застосування проти чужих систем без письмового дозволу — кримінальне правопорушення (ст. 361 КК України).

Навчальні цілі

- Виявлення фаєрвола за реакцією портів (filtered vs closed)
- Перевірка дієвості класичних evasion-технік Nmap (fragmentation, decoys, timing, source-port spoofing) проти stateful-фаєрвола
- Розуміння, чому `scrub`, `antispoof` і stateful-інспекція нейтралізують ці техніки
- Оцінка придатності хоста як zombie для `idle-scan (-sl)` за класом генерації IP ID
- Фінгерпринтинг типу фаєрвола через ACK-скан (`-sA`)
- Аналіз трафіку сканування з двох точок спостереження (сегмент атакуюльника vs за фаєрволом)

Техніки MITRE ATT&CK

T1595 - Active Scanning T1595.001 - Scanning IP Blocks T1046 - Network Service Discovery T1090 - Proxy
T1090.001 - Internal Proxy T1562.004 T1027 - Obfuscated Files or Information

► Розпочати сценарій

ЗАДАЧА 4 · ТРЕНАЖЕР

Як тренажер перевіряє відповіді



Кожен крок прив'язаний до техніки MITRE ATT&CK



Підказка трохи знижує бали за крок



Контрольне теоретичне питання на розуміння

5 типів валідаторів: точний збіг · регулярний вираз · числовий діапазон · підрядок · вибір з варіантів

КРОК 2 з 15 **+10 балів**

Спроба прямого доступу до Internal

Спробуйте сканувати внутрішню підмережу 10.10.10.0/24 на адресу з Kali:

КОМАНДА

`ncmap -sn 10.10.10.0/24 --max-retries 1 -t4`

Прапорці команд:

- sn — ping-scan: лише виявлення «живих» хостів (host discovery), без сканування портів;
- max-retries 1 — максимум одна повторна спроба на зонді, щоб скан не «висів» довго на недоступній мережі;
- t4 — швидкий timing-шаблон (T0 — найповільніший/найдовший, T5 — найшвидший/найкучніший).

Подивіться, що відповість Nmap і скільки хостів виявить. Це покаже, чи має взагалі сенс шукати pivot.

Питання для самоперевірки:

Чому міжмережний екран ефективно блокує прямі атаки з DMZ на Internal та які варіанти обходу є у атакуючого?

Скільки хостів виявлено на адресу з Kali у мережі 10.10.10.0/24 (число):

Введіть, формат: число

Спроба: 1 з 3

Прогрес

1 з 15 кроків

Кроки сценарію

- ✓ 1. Розвідка мережі DMZ
- ➡ 2. Спроба прямого доступу до Internal
- 3. Сканування Metasploitable 2
- 4. Ідентифікація Samba (Initial Access)
- 5. Формування інфраструктури сесії для pivot
- 6. Навантаження pivot через smbexec
- 7. Сканування Internal через pivot
- 8. SOCKS-проксі для доступу через pivot
- 9. Розвідка веб-додатку DC-1
- 10. Експлуатація OpenRedirect CVE-2016-7680
- 11. Пошук облікових даних у конфігурації Drupal
- 12. Витяг нових креденціалів Drupal
- 13. Пошук SUDO-файлів для pivot
- 14. Privilege Escalation через SUDO-fixer
- 15. Збір фінального флага

Поточний бал

0 / 250

Час: 00:23

Автоматичний PDF-звіт про проходження

ЗВІТ ПРО ВИКОНАННЯ СЦЕНАРІЮ ПЕНТЕСТУ

PortSec Trainer v1.0 | KDUVA, спеціальність 125

Інформація про виконавця

ІМ'Я студента:

Зареба Богдан Владислав

Група:

БКС-22

Дата виконання:

2026-06-23 22:54

Інформація про сценарій

Сценарій:

Сценарій 3: Інтеграція атака з pivot через DMZ до Internal

Початок:

2026-06-23 22:54

Завершення:

2026-06-23 22:58

Виконані кроки

№	Крок	ATT&CK	Бали	Час	Статус
2	Спроба прямого доступу до Internal	T1018	10	0хх 37с	☐
3	Скачування Metasploitable 2	T1046	9	0хх 22с	☐
4	Експлуатація Samba (Initial Access)	T1190	20	0хх 4с	☐
5	Отримання інтерактивної сесії для piv0t	T1059.004	15	0хх 8с	☐
6	Навстановлення pivot через nat0x0x	T1090	20	0хх 7с	☐
7	Скачування Internal через pivot	T1046	15	0хх 3с	☐
8	SOCKS-прокси для доступу через pivot	T1090	15	0хх 6с	☐
9	Результат веб-камери (DC-1)	T1195	12	0хх 13с	☐
10	Експлуатація DoS (CVE-2016-7601) 190		25	0хх 6с	☐
11	Попули об'єктів даних у конфігурації	DB1552.001	20	0хх 4с	☐
12	Витяг шкелу адміністратора DoS	T1003	15	0хх 4с	☐
13	Попули SUDO-файла для ретеве	T1063	15	0хх 5с	☐
14	Privilege Escalation через SUDO find	T1548.001	25	0хх 5с	☐
15	Збір фінального флажа	T1005	25	0хх 5с	☐

Підсумкова оцінка

Набрано балів:

241 з 250

Відсоток:

96.4%

Оцінка CKTC:

A (відмінно)

Звіт містить:

- Бали за кожен крок — і підсумкову суму
- Підсумкова оцінка — переведена у шкалу ЄКТС
- Загальний час — проходження сценарію
- Використані підказки — кількість і вплив на бали

Студент отримує об'єктивну автоматичну оцінку, викладач — готовий звіт без ручної перевірки.

Модульність і розширюваність



Формат JSON

Новий додається без зміни коду



CLI-інструменти

Створення та валідація сценаріїв із командного рядка



Веб-редактор

Візуальне створення з заповненням технік ATT&CK

Новий сценарій — 8 хвилин
проти 52 хв ручним JSON

Новий сценарій

Валідувати

Скасувати

Зберегти

Метадані

ID *

Рівень *

а-1, 0-9, _ (3-64 символів) Стислий файл

medium

Назва *

Наприклад: Глибока мережева розвідка

Тривалість, хв

Спроб на крок

Мережева топологія

120

3

— оберіть —

Потрібні VM *

оберіть зі списку доступних профілів

DC-1 (act)

Kali Linux (full)

Metasploitable2 (metasploitd2)

p5Sense (p5sense)

Snapshot для кожної VM

кожен snapshot відновить стан запуску (становай clean state)

Навчальні цілі

Перелічіть 3-7 ключових навичок, які студент набуває.

Додати ціль

MITRE ATT&CK — техніки на рівні сценарію

Почніть друкувати ID (наприклад, T1018) або назву техніки для пошуку.

T1018 / Remote System / Discovery...

Теоретичний вступ

Показувати студенту перед стартом. Підтримуються теги: `<p>`, `<ul>`, `<li>`, `<code>`, `<pre>`, `<strong>`.

<p>У цьому сценарії ви виконаєте...</p>

ПРАКТИЧНИЙ ВНЕСОК

Що дає робота на практиці



Безкоштовне, україномовне, автономне рішення з готовими сценаріями — придатне до впровадження в навчальний процес без комерційних ліцензій і без доступу до інтернету.

Рішення побудоване за модульним принципом — розширюється без зміни коду:

1

Модульні сценарії

Опис у форматі JSON — новий сценарій додають без зміни коду

`scenario_loader.py`

2

Додавання VM з вебінтерфейсу

Нові віртуальні машини реєструють і запускають через панель

`vm_manager.py`

3

Знімки стану й топологія

Відкат до еталона перед стартом; знімок задає топологію сценарію

`clean_state`

4

Гнучка перевірка

П'ять типів валідаторів, стійких до змінного стану цілі

`5 валідаторів`

Викладач розширює середовище — нові сценарії та машини — без програмування

Апробація за п'ятьма напрямками

1

Вимірювання середовища

старт VM 43–87 с · RAM ~1,2 ГБ · диск ~30 ГБ → працює на ПК з 8 ГБ

2

Самотестування сценаріїв

усі 55 кроків прийняв валідатор · 160 хв проти 290 планових (–44,8%)

3

Розширюваність

новий сценарій 8 хв через веб-редактор проти 52 хв ручним JSON

4

Порівняння з аналогами

україномовність · безкоштовність · автономність

5

Покриття стандартів

36 технік ATT&CK · 7 фаз PTES · 7/8 підфаз NIST 800-115

ЗАДАЧА 5 · ПОКРИТТЯ

Покриття MITRE ATT&CK

Сценарії покривають 9 із 12 ключових тактик — загалом 36 технік:



Детальне покриття PTES і NIST SP 800-115 — на наступному слайді.

Покриття PTES та NIST SP 800-115

PTES 7 / 7 фаз

- ✓ Pre-engagement
- ✓ Intelligence Gathering
- ✓ Threat Modeling
- ✓ Vulnerability Analysis
- ✓ Exploitation
- ✓ Post-Exploitation
- ✓ Reporting

NIST SP 800-115 7 / 8 підфаз

- ✓ Planning
- ✓ Discovery: Network Discovery
- ✓ Discovery: Vulnerability ID
- ✓ Attack: Gaining Access
- ✓ Attack: Escalating Privileges
- ✓ Attack: System Browsing
- Attack: Install Add. Tools
- ✓ Reporting

ВИСНОВКИ

Мету досягнуто — усі 5 задач виконано

- ✓ Проаналізовано наявні рішення й обґрунтовано потребу
- ✓ Побудовано віртуалізоване середовище зі знімками стану
- ✓ Розроблено 5 сценаріїв (55 кроків, 3 рівні складності)
- ✓ Реалізовано тренажер: автоматична перевірка, звіти, розширюваність
- ✓ Проведено апробацію за 5 напрямками з підтвердженням покриття стандартів



Безкоштовний україномовний інструмент, готовий до впровадження в навчальний процес кафедри.



Дякую за увагу!

Готовий відповісти на запитання

Заремба Богдан Вадимович · КНУБА · 2026

