МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

ЗАТВЕРДЖУЮ

Декан факультету комп'ютерних інформаційних технологій
Ігор ЯКИМЕНКО
_____
«29» 08 2025 р.

ЗАТВЕРДЖУЮ

Проректор з науково-педагогічної роботи
Віктор ОСТРОВЕРХОВ
_____
«29» 08 2025 р.

ЗАТВЕРДЖУЮ:

Директор Навчально-наукового інституту новітніх освітніх технологій
_____ Святослав ПИТЕЛЬ
«29» 08 2025 р.

РОБОЧА ПРОГРАМА

з дисципліни «Тестування комп'ютерних систем на проникнення»
ступінь вищої освіти – магістр
галузь знань – F Інформаційні технології
спеціальність – F5 Кібербезпека та захист інформації
освітньо-професійна програма – Кібербезпека

Кафедра кібербезпеки

Форма навчання	Курс	Семестр	Лекції (год.)	Лабор. заняття (год.)	Інд. роб. (год.)	Тренінг (год.)	Самост. робота (год.)	Разом (год.)	Залік / екзамен (семестр)
Денна	1	1	32	14	5	6	93	150	Екзамен (1)
Заочна	1	1	8	4	-	-	138	150	Екзамен (1)

29.08.2025 р.

Тернопіль – 2025 р.

Робоча програма розроблена на основі освітньо-професійної програми підготовки магістра галузі знань F «Інформаційні технології» спеціальності F5 «Кібербезпеки та захист інформації», затвердженої Вченою радою ЗУНУ (протокол №8 від 26.06.2025 р.).

Робочу програму склав завідувач кафедри кібербезпеки, д.т.н., професор Василь Яцків Василь

Робоча програма затверджена на засіданні кафедри кібербезпеки, протокол № 1 від 26.08.2025 р.

Завідувач кафедри Василь ЯЦКІВ

Гарант освітньо-професійної програми Василь ЯЦКІВ

СТРУКТУРА РОБОЧОЇ ПРОГРАМИ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

1. Опис дисципліни «Тестування комп'ютерних систем на проникнення»

Дисципліна «Тестування комп'ютерних систем на проникнення»	**Галузь знань, спеціальність, СВО**	**Характеристика навчальної дисципліни**
Кількість кредитів ECTS – 5	Галузь знань – F Інформаційні технології	**Статус дисципліни** - обов'язкова **Мова навчання** – українська
Кількість залікових модулів – 4	Спеціальність F5 – Кібербезпека та захист інформації	Рік підготовки: *Денна – 1* *Заочна – 1* Семестр: *Денна – 1* *Заочна – 1*
Кількість змістових модулів – 2	Ступінь вищої освіти – магістр	Лекції (год.): *Денна – 32* *Заочна – 8* Лабораторні роботи (год.): *Денна – 14* *Заочна – 4*
Загальна кількість годин – 150		Самостійна робота (год.): *Денна – 93* *Заочна – 138* Тренінг (год.): *денна – 6* Індивідуальна робота (год.): *Денна – 5*
Тижневих годин – 10 з них аудиторних – 3		Вид підсумкового контролю – екзамен

2. Мета і завдання дисципліни «Тестування комп'ютерних систем на проникнення»

2.1. Мета вивчення дисципліни

Метою дисципліни «Тестування комп'ютерних систем на проникнення» є - отримання знань та умінь, які необхідні для проведення тестування комп'ютерних систем на проникнення.

2.2. Завдання вивчення дисципліни

Основне завдання дисципліни дати здобувачам теоретичну та практичну підготовку з виконання тестів на проникнення.

2.3. Найменування та опис компетентностей, формування котрих забезпечує вивчення дисципліни

КЗ1. Здатність застосовувати знання у практичних ситуаціях.

КЗ3. Здатність до абстрактного мислення, аналізу та синтезу.

КЗ4. Здатність оцінювати та забезпечувати якість виконуваних робіт.

КФ3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.

КФ5. Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

КФ6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

КФ8. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

2.4. Передумови для вивчення дисципліни

Вивчення курсу «Тестування комп'ютерних систем на проникнення» передбачає наявність систематичних та ґрунтовних знань із суміжних курсів («Аналіз шкідливого програмного забезпечення», «Моніторинг та управління інформаційною безпекою»), а також цілеспрямованої роботи на лекційних та лабораторних заняттях, самостійної роботи здобувачів ОПП.

2.5. Результати навчання

РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.

РН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.

РН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

РН13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури.

РН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.

РН22. Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.

РН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.

3. Програма навчальної дисципліни: «Тестування комп'ютерних систем на проникнення»

Змістовий модуль 1. Види тестування на проникнення

Тема 1. Вступ до тестування на проникнення

Мета та завдання тестування на проникнення. Види тестування на проникнення (чорна скринька, біла скринька, сіра скринька). Етичні та юридичні аспекти тестування на проникнення

Тема 2. Методологія тестування на проникнення OSSTMM

Принципи OSSTMM. Структура OSSTMM. Процес тестування за OSSTMM. Аналіз метрик RAV у OSSTMM

Тема 3. Методології тестування PTES та NIST

Особливості методології PTES. Структура PTES. Особливості методології NIST. Структура процесу тестування за NIST.

Тема 4. Планування та підготовка до тестування на проникнення

Етапи тестування на проникнення. Збір вимог та визначення цілей. Укладання угоди про проведення тестування (Rules of Engagement). Побудова тестового середовища. Інструменти для планування тестування

Тема 5. Види розвідки

Розвідка у тестуванні на проникнення. Види розвідки. Інструменти для проведення розвідки. Соціальні мережі. Реєстраційні дані

Тема 6. Активна розвідка

Сканування мережі. Основні можливості Nmap. Типовий сценарій використання Nmap при тестуванні. Інструменти та методи захоплення банерів.

Тема 7. Аналіз результатів сканування при тестуванні на проникнення.

Основні етапи аналізу результатів сканування. Інструменти для аналізу результатів. Визначення вразливостей при тестуванні на проникнення. Інструменти для визначення вразливостей.

Тема 8. Експлуатація вразливостей

Експлуатація вразливостей при тестуванні на проникнення. Вибір вразливостей для експлуатації. Інструменти для експлуатації.

Змістовий модуль 2. Атаки на протоколи та програми

Тема 9. Атаки на паролі

Методи отримання доступу через злом паролів/автентифікацію. Техніки злому паролі. Архітектура автентифікації та зберігання паролів. Інструменти. Рекомендації із захисту

Тема 10. Тестування безпеки бездротових мереж

Загрози й вразливості бездротових технологій. Протоколи Wi-Fi (802.11): WEP, WPA2, WPA3 та атаки. Протоколи Bluetooth/BLE. ZigBee та LoRaWAN. RFID/NFC. SDR-атаки (ADS-B, ACARS, GPS). Захист бездротових мереж.

Тема 11. Використання фреймворку MITRE ATT&CK у тестуванні на проникнення

Використання ATT&CK пентестером. Основні поняття та навігація. ATT&CK у циклі пентесту. Приклади використання фреймворку Atomic Red Team у тестуванні на проникнення.

Тема 12. Соціальна інженерія в тестуванні на проникнення

Основні види атак соціальної інженерії. Приклади реальних кейсів соціальної інженерії. Інструменти для симуляції атак соціальної інженерії. Методи захисту від соціально-інженерних атак

Тема 13. Тестування безпеки IoT-пристроїв

Методи аналізу безпеки IoT-пристроїв. Типові вразливості IoT. Атаки через мережеві протоколи

Тема 14. Юридичні питання тестування на проникнення

Юридичні причини тестування на проникнення. Правові рамки тестування на проникнення. Умови договору між тестером на проникнення та клієнтом. Нормативні акти України, які безпосередньо або опосередковано стосуються тестування на проникнення. Шаблон договору на проведення тестування на проникнення

Тема 15. Звітність та рекомендації.

Етапи написання звітів. Основні елементи звіту. Значення звітності. Основні принципи створення звіту. Формат представлення вразливостей і ризиків. Побудова дорожньої карти для усунення вразливостей

4. Структура залікового кредиту з дисципліни "Тестування комп'ютерних систем на проникнення"

4.1 Структура залікового кредиту дисципліни (денна форма навчання)

	Кількість годин					
	Лекції	Лабор. заняття (год.)	Інд. роб. (год.)	Тренінг	Самост. робота (год.)	Контрольні заходи
Змістовий модуль 1. *Види тестування на проникнення*						
Тема 1. Вступ до тестування на проникнення	2	-	2	2	3	Поточне опитування
Тема 2. Методологія тестування на проникнення OSSTMM	2	-			6	
Тема 3. Методології тестування PTES та NIST	2	-			6	
Тема 4. Планування та підготовка до тестування на проникнення	2	2			6	
Тема 5. Види розвідки	2	-			6	
Тема 6. Активна розвідка	2	-			6	
Тема 7. Аналіз результатів сканування при тестуванні на проникнення	4	4			4	
Тема 8. Експлуатація вразливостей	2	-			4	
Змістовий модуль 2. *Атаки на протоколи та програми*						

Тема 9. Атаки на паролі	2	-	3	4	6	Поточне опитування
Тема 10. Тестування безпеки бездротових мереж	2	2			6	
Тема 11. Використання фреймворку MITRE ATT&CK у тестуванні на проникнення	2	2			8	
Тема 12. Соціальна інженерія в тестуванні на проникнення	2	-			8	
Тема 13. Тестування безпеки IoT-пристроїв	2	2			8	
Тема 14. Юридичні питання тестування на проникнення	2	-			8	
Тема 15. Звітність та рекомендації	2	2			8	
Разом	32	14	5	6	93	

4.2 Структура залікового кредиту (заочна форма навчання)

	Кількість годин		
	Лекції	Лабор. заняття (год.)	Самост. робота (год.)
Змістовий модуль 1. ***Види тестування на проникнення***			
Тема 1. Вступ до тестування на проникнення	2	2	8
Тема 2. Методологія тестування на проникнення OSSTMM			8
Тема 3 Методології тестування PTES та NIST			8
Тема 4. Планування та підготовка до тестування на проникнення			8
Тема 5. Види розвідки	2		8
Тема 6. Активна розвідка			10
Тема 7. Аналіз результатів сканування при тестуванні на проникнення			10
Тема 8. Експлуатація вразливостей			10
Змістовий модуль 2. ***Атаки на протоколи та програми***			
Тема 9. Атаки на паролі	2	2	10
Тема 10. Тестування безпеки бездротових мереж			10
Тема 11. Використання фреймворку MITRE ATT&CK у тестуванні на проникнення			10
Тема 12. Соціальна інженерія в тестуванні на проникнення	2		10
Тема 13. Тестування безпеки IoT-пристроїв			10
Тема 14. Юридичні питання тестування на проникнення			10
Тема 15. Звітність та рекомендації			8
Разом	**8**	**4**	**138**

5. Тематика лабораторних робіт

Лабораторна робота №1

Тема: тестування безпеки віртуальної машини Kioptrix Level 1

Мета: здобути практичні навички повного циклу пентесту на прикладі машини *Kioptrix: Level 1*: від мережевої розвідки до отримання root та підготовки рекомендацій.

Завдання:

– підготовка середовища;
– виявлення цілі;
– повне сканування портів і сервісів;
– веб-розвідка;
– SMB-розвідка (альтернативний вектор);
– експлуатація;
– пост-експлуатація;
– збір доказів та оформлення звіту.

Лабораторна робота №2

Тема: проходження машини Damn Vulnerable Web App (DVWA)

Мета: відпрацювати цикл веб-пентесту на прикладі DVWA: від розвідки до експлуатації класичних вразливостей (SQLi, XSS, Command Injection, File Upload, LFI/RFI, CSRF) і підготувати рекомендації.

Завдання:

– підготовка середовища;
– початкова розвідка;
– аутентифікація та рівень безпеки DVWA;
– Brute force; – збір доказів та оформлення звіту.

Лабораторна робота №3

Тема: проходження машини FristiLeaks 1.3 (VulnHub)

Мета: відпрацювати повний цикл пентесту CTF-типу: веб-розвідка → експлуатація (file upload bypass) → первинний доступ → горизонтальний/вертикальний перехід прав (cron-трик, розшифрування «паролів») → привілей-ескалація до root → збір доказів і рекомендації.

Завдання:

– підготовка середовища;
– розвідка;
– початкова пост-експлуатація;
– реверс алгоритму «шифрування» паролів;
– ескалація привілеїв;
– отримання прапора і артефактків;
– збір доказів та оформлення звіту.

Лабораторна робота №4

Тема: віртуальна машина LazySysAdmin

Мета: відпрацювати повний цикл пентесту (Discovery → Scanning → Enumeration → Exploitation → Priv-Esc) з акцентом на помилкові налаштування, опанувати енумерацію веб-

сервісів і SMB, виконати підвищення привілеїв у Linux та задокументувати робочий шлях до root.

Завдання:

– підготовка середовища;
– розвідка та сканування;
– енумерація сервісів;
– експлуатація;
– підвищення привілеїв;
– пост-експлуатація;
– збір доказів та оформлення звіту.

Лабораторна робота №5

Тема: підвищення привілеїв у ОС Linux: Lin.Security

Мета: виконати повний цикл: Discovery → Scanning → Enumeration → Exploitation → Privilege Escalation (Linux) → Post-Ex → Звіт.

Завдання:

– підготовка та сканування;
– надійний доступ до цільової системи з виконанням команд;
– підвищення привілеїв у ОС Linux;
– пост-експлуатація;
– збір доказів та оформлення звіту.

Лабораторна робота №6

Тема: віртуальна машина SickOS 1.1

Мета: виконати повний цикл: Discovery → Scanning → Web-Enumeration → Exploitation (до RCE) → Privilege Escalation (Linux) → Звіт.

Завдання:

– підготовка та пошук цілі;
– сканування;
– веб-енумерація;
– експлуатація до RCE;
– підвищення привілеїв (Linux);
– збір доказів та оформлення звіту.

6. Організація та проведення тренінгу з дисципліни «Тестування комп'ютерних систем на проникнення»

№ п/п	Вид роботи	Порядок проведення тренінгу
1	Налаштувати інфраструктуру для виконання завдання.	Для виконання завдання необхідні: 1. Засіб віртуалізації - VirtualBox; 2. Образ віртуальної машини для дослідження - Metasploitable2; Образ віртуальної машини атакуючого - Kali Linux.
2	Визначити доступні сервіси на досліджуваній машині.	Для визначення запущених на досліджуваній машині мережевих сервісів з машини «атакуючого» необхідно провести сканування за допомогою утиліти nmap.

3	Отримати віддалений доступ, шляхом експлуатації вразливостей чотирьох різних сервісів.	Вибрати чотири різних сервісів, які мають вразливості. Запустити Metasploit. Отримати доступ до вибраних сервісів використовуючи знайдені вразливості.

7. Самостійна робота

Для самостійної роботи кожному здобувачу пропонується виконання наскрізного проєкту **«Виконання тесту на проникнення»**, який складається із шести завдань**:**

1. Вибір цілі (віртуальна машина із заданими вразливостями).
2. Збір інформації та пошук цілей.
3. Пошук вразливостей.
4. Експлуатація та проведення атак.
5. Розширення зони впливу і ескалація привілеїв.
6. Написання звіту.

8. Методи навчання

У освітньому процесі застосовуються: лекції, в тому числі з використання мультимедійного проектора та інших ТЗН; лабораторні роботи, індивідуальні заняття; самостійна робота здобувачів, робота в Інтернет.

9. Засоби оцінювання та методи демонстрування результатів навчання

У процесі вивчення дисципліни «**Тестування комп'ютерних систем на проникнення**» використовуються наступні засоби оцінювання та методи демонстрування результатів навчання:

– поточне опитування;
– оцінювання виконання лабораторних робіт;
– підсумковий модульний контроль за кожним змістовним модулем;
– оцінювання тренінгу;
– оцінювання результатів самостійної роботи;
– підсумковий екзамен.

10. Політика оцінювання

Політика щодо дедлайнів і перескладання. Для виконання усіх видів завдань здобувачами і проведення контрольних заходів встановлюються конкретні терміни. Перескладання модулів проводиться в установленому порядку.

Політика щодо академічної доброчесності. Списування під час проведення контрольних заходів заборонені. Під час контрольного заходу здобувач може користуватися лише дозволеними допоміжними матеріалами або засобами, йому забороняється в будь-якій формі обмінюватися інформацією з іншими здобувачами, використовувати, розповсюджувати, збирати варіанти контрольних завдань.

Політика щодо відвідування. За об'єктивних причин (наприклад, карантин, воєнний стан, хвороба, закордонне стажування) навчання може відбуватись в дистанційній формі за погодженням із керівником курсу з дозволу дирекції факультету.

11. Критерії, форми поточного та підсумкового контролю

Підсумковий бал (за 100-бальною шкалою) з дисципліни «**Тестування комп'ютерних систем на проникнення**» визначається як середньозважена величина, залежно від питомої ваги кожної складової залікового кредиту:

Модуль 1		Модуль 2	Модуль 3	Модуль 4
20 %	20 %	5 %	15 %	40 %
Поточне оцінювання	Модульний контроль	Тренінги	Самостійна робота	Екзамен
Оцінка за даний модуль визначається як середнє арифметичне за захист лабораторних робіт № 1-6.	Підсумкове тестування за темами №1-15.	Визначається як середнє арифметичне з оцінок за виконання трьох завдань тренінгу.	Оцінка за даний модуль виставляється за виконання наскрізного завдання.	1. Теоретичні питання: 2 питання по 30 балів - max 60 балів. 2. Практичне завдання - max 40 балів

Виконання лабораторних робіт:

90 – 100 балів: здобувач глибоко розуміє повний цикл пентесту, самостійно планує дії; аргументовано обирає підходи; надає надійні докази (відтворювані етапи/логи/скріншоти); пише чіткий, структурований звіт із практичними рекомендаціями; суворо дотримується етики та меж обсягу;

75 – 89 балів: здобувач розуміє й у цілому коректно застосовує етапи пентесту з незначними неточностями; демонструє достатні докази; звіт повний, але місцями потребує уточнень; етика та дотримані меж;

60 – 74 бали: знає базові кроки та виконує їх переважно за інструкцією; докази часткові/неповні; звіт мінімально достатній; етика/межі у цілому дотримані, але потрібен супровід;

1 – 59 балів: фрагментарне розуміння процесу; відсутні або ненадійні докази; звіт неповний/неструктурований; можливі порушення етики чи меж обсягу.

Підсумкове модульне тестування - вид контролю, при якому засвоєний здобувачем теоретичний та практичний матеріал оцінюється у форматі тестування. Тестування містить 25 запитань кожна правильна відповідь дає 4 бали, максимум 100 балів.

Тренінг:

90-100 балів: здобувач самостійно, без помилок, виконав усі етапи завдання, правильно задокументував усі етапи роботи, та вільно оперує поняттями та принципами тестування на проникнення;

75-89 балів: здобувач виконав завдання, але з кількома дрібними помилками, які не вплинули на кінцевий результат (наприклад, неточна послідовність дій), виникали питання під час роботи;

60-74 балів: здобувач виконав завдання, але з суттєвими помилками, наприклад, не з першого разу. Розуміння поставлених завдань є поверхневим;

1-59 балів: здобувач не зміг виконати завдання або результати були повністю невірними. Не продемонстрував базових навичок роботи з наданим програмним забезпеченням.

Самостійна робота:

1. Збір інформації та пошук цілей – 15 балів:

14 – 15 повна карта поверхні атаки; коректно визначені сервіси/версії; підтверджена валідність знахідок; дані структуровані та відтворювані;

12 – 13: виявлено основні сервіси/версії; незначні прогалини або часткова валідація; структура даних переважно коректна;

9 – 11: базове виявлення без глибини та валідації; поодинокі неточності; часткова відтворюваність;

0 – 8: неповні/неточні результати; відсутня валідація або хаотичні дані; неможливо відтворити.

2. Пошук вразливостей – 20 балів**:**

18 – 20: релевантні вразливості зіставлені з активами; мінімізовано фолс-позитиви; зроблена первинна пріоритизація ризиків із посиланнями (CVE/CWE/CVSS); доказова база повна;

14 – 17: якісний список вразливостей із базовою перевіркою та пріоритизацією; поодинокі фолс-позитиви;

10 – 13: перелік є, але неповний/частково нерелевантний; слабка пріоритизація; обмежена доказовість;

0 – 9: критично неповний або хибний пошук; відсутні докази або системність.

3. Експлуатація та проведення атак – 25 балів**:**

23 – 25: стабільний, відтворюваний PoC/експлойт (власний або коректно адаптований); чіткий доказ; контроль впливу/безпеки; описані обхідні прийоми за потреби;

19 – 22: успішна експлуатація з незначними недоліками у стабільності/оформленні; докази достатні; вплив контрольований;

13 – 18: частковий або нестабільний результат; доказовість обмежена; є прогалини у безпечному виконанні;

0 – 12: немає переконливого PoC/доказів; порушення межі або невиправданий вплив.

4. Розширення зони впливу й ескалація привілеїв – 20 балів:

18 – 20: логічний ланцюжок від первинного доступу до підвищення привілеїв/бічного руху в дозволених межах; чіткі артефакти та відтворюваність; мінімізований вплив.

14 – 17: досягнуто ескалації або часткового бічного руху; докази достатні; незначні прогалини в методиці.

10 – 13: описано підхід і спроби, але результат частковий/сумнівний; доказів недостатньо.

0 – 9: відсутні робочі спроби/докази або порушено межі тестування.

5. Написання звіту – 20 балів:

18 – 20: структурований звіт для технічної й управлінської аудиторій; чіткі висновки, пріоритизація та практичні рекомендації з дорожньою картою; докази й артефакти повні, відтворювані;

14 – 17: повний звіт із мінорними недоліками в ясності/єдності стилю; рекомендації здебільшого практичні;

10 – 13: основні розділи є, але бракує глибини/узгодженості/доказовості; рекомендації загальні;

0 – 9: неповний або нечіткий звіт; відсутні рекомендації; недостатня доказова база.

Екзамен - вид підсумкового контролю, який проводиться з метою оцінювання засвоєння здобувачем вищої освіти теоретичного та практичного матеріалу. Екзаменаційний білет складається з двох блоків.

Перший блок містить два теоретичних запитань, за кожне з яких можна отримати від 0 до 30 балів, що в підсумку дає максимально 60 балів. За відповідь на питання здобувач отримує 16–30 балів, якщо у повному обсязі володіє навчальним матеріалом, всебічно, самостійно та аргументовано відповідає на питання білету і 1–15 балів – якщо володіє навчальним матеріалом не в повному обсязі, викладає його фрагментарно, допускаючи при цьому суттєві неточності.

Другий блок містить практичне завдання:

31 –40 балів - доповідь охоплює всі основні аспекти обраної теми, демонструючи глибоке розуміння предмету дисципліни. Здобувач вільно володіє матеріалом, відповідає впевнено на всі запитання.

21–30 балів - доповідь розкриває основні питання теми, але може бути недостатньо деталізованою; є аналітичні елементи, але вони можуть бути не достатньо глибокими. Здобувач демонструє знання матеріалу, але має незначні труднощі з відповідями на додаткові питання.

11–20 балів - відповідь охоплює лише основні аспекти теми, бути пропущені важливі деталі. Здобувач не завжди впевнено відповідає на запитання.

1–10 балів - відповідь містить значні помилки або не зовсім відповідає завданню.

Шкала оцінювання:

За шкалою ЗУНУ	**За національною шкалою**	**За шкалою ECTS**
90–100	відмінно	A (відмінно)
85–89	добре	B (дуже добре)
75-84		C (добре)
65-74	задовільно	D (задовільно)
60-64		E (достатньо)
35-59	незадовільно	FX (незадовільно з можливістю повторного складання)
1-34		F (незадовільно з обов’язковим повторним курсом)

12. Інструменти, обладнання та програмне забезпечення, використання яких передбачає навчальна дисципліна

№	**Найменування**	**Номер теми**
1.	Мультимедійний проектор	1 - 15
2.	Комп’ютерна лабораторія (Кіберполігон). Доступ до Інтернету.	1 - 15
3.	Програмне забезпечення: Oracle VM VirtualBox, Kali Linux віртуальні машини із заданими вразливостями.	1 - 15

Рекомендовані джерела інформації

1. Опорний конспект лекцій з курсу «Тестування комп'ютерних систем на проникнення» для здобувачів освітньо-професійної програми «Кібербезпека» другого (магістерського) рівня вищої освіти спеціальності «Кібербезпека та захист інформації» / Укл. В. Яцків. Тернопіль: ЗУНУ, 2025. – 132 с.
2. Тестування на проникнення: навч. посіб. Ч.1 / [Є.О. Живило]; за ред. Є.О. Живило. – П.: ПНТУ "Полтавська політехніка ім. Юрія Кондратюка", 2024. – 134 с.
3. Тестування на проникнення: навч. посіб. Ч.2 / [Є.О. Живило]; за ред. Є.О. Живило. – П.: ПНТУ "Полтавська політехніка ім. Юрія Кондратюка", 2024. – 239 с.
4. Яцків В.В., Яцків Н.Г., Возняк С.І., Кондратюк В.М. Методика виконання тестів на проникнення з використання MITRE ATT&CK. Інформатика та математичні методи в моделюванні. 2025. Том 15, № 2. – С. 288-297. DOI 10.15276/imms.v15.no2.288
5. OSSTMM 3 – The Open Source Security Testing Methodology Manual. https://www.isecom.org/OSSTMM.3.pdf
6. BSI - Study A Penetration Testing Model. Federal Office for Information Security, 111p. Режим доступу: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/Penetration/penetration_pdf.html
7. Vulnerability Scanning Tools. Режим доступу: https://www.owasp.org/index.php/Category:Vulnerability_Scanning_Tools
8. PTES Technical Guidelines. http://www.pentest-standard.org/index.php/Exploitation
9. MITRE ATT&CK Documentation. https://attack.mitre.org
10. Isozaki, I., Shrestha, M., Console, R., & Kim, E. (2025, June). Towards automated penetration testing: Introducing llm benchmark, analysis, and improvements. In Adjunct Proceedings of the 33rd ACM Conference on User Modeling, Adaptation and Personalization, pp. 404-419.
11. 12 Types of social engineering attacks. Режим доступу: https://www.trendmicro.com/en_no/what-is/social-engineering/types-of-social-engineering-attacks.html
12. Що таке соціальна інженерія в кібербезпеці? Реальні приклади та методи запобігання. Режим доступу: https://hideez.com/uk-ua/blogs/news/social-engineering?srsltid=AfmBOooW2bDba7-SY8L7kkJavAw09QkjtAQs9jvt6QlAr1KGFSU3l_Dl
13. Hashcat. Режим доступу: https://hashcat.net/wiki/doku.php?id=hashcat
14. Hydra. Режим доступу: https://hackviser.com/tactics/tools/hydra
15. Akhilesh, R.; Bills, O.; Chilamkurti, N.; Chowdhury, M.J.M. Automated Penetration Testing Framework for Smart-Home-Based IoT Devices. Future Internet 2022, 14, 276. https://doi.org/10.3390/fi14100276
16. Zigbee Security 101 (Architecture And Security Issues). Режим доступу: https://payatu.com/blog/zigbee-security-101-architecture-and-security-issues/
17. Barrera, D., Bellman, C., & Van Oorschot, P. (2023). Security best practices: a critical analysis using IoT as a case study. ACM Transactions on Privacy and Security, 26(2), 1-30.
18. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах». Режим доступу: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text
19. Закон України «Про інформацію». Режим доступу: https://zakon.rada.gov.ua/laws/show/2657-12#Text
20. Закон України «Про захист персональних даних». Режим доступу: https://zakon.rada.gov.ua/laws/show/2297-17#Text