МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

МІЖНАРОДНИЙ ГУМАНІТАРНИЙ УНІВЕРСИТЕТ

Кафедра комп'ютерної інженерії та інноваційних технологій

«ЗАТВЕРДЖУЮ»

Ректор Міжнародного гуманітарного університету д.ю.н., професор

_____ Костянтин ГРОМОВЕНКО

«29» серпня 2025 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ЕТИЧНИЙ ХАКІНГ ТА ТЕСТУВАННЯ НА ПРОНИКНЕННЯ

Галузь знань	12 «Інформаційні технології»
Спеціальність	125 «Кібербезпека та захист інформації»
Назва освітньої програми	Кібербезпека
Рівень вищої освіти	перший (бакалаврський) рівень

Одеса - 2025 рік

Робоча програма затверджена на засіданні кафедри комп'ютерної інженерії та інноваційних технологій протокол № 1 від 28 серпня 2025 року.

Розробники і викладачі	**Контактний тел.**	**E-mail**
професор кафедри комп'ютерної інженерії та інноваційних технологій, д.т.н., професор **Соколов Артем Вікторович**	050-492-32-57	radiosquid@gmail.com

Завідувач кафедри комп'ютерної інженерії та інноваційних технологій
к.т.н., доцент _____ Лариса ЙОНА

Гарант освітньої програми
к.т.н., доцент _____ Лариса ЙОНА

Узгоджено
Начальник навчального відділу _____ Лілія САЄНКО

1. ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

<table>
<tr><th rowspan="2">Найменування показників</th><th rowspan="2">Галузь знань, напрям підготовки, освітньо-кваліфікаційний рівень</th><th colspan="2">Характеристика навчальної дисципліни</th></tr>
<tr><th>денна форма навчання</th><th>заочна форма навчання</th></tr>
<tr><td rowspan="2">Кількість кредитів – 6

Загальна кількість годин – 180</td><td>Галузь - 12 «Інформаційні технології»</td><td colspan="2">обов’язкова</td></tr>
<tr><td rowspan="10">Спеціальність – 125 «Кібербезпека та захист інформації»</td><td colspan="2">Рік підготовки:</td></tr>
<tr><td colspan="2">4-й</td></tr>
<tr><td colspan="2">Семестр</td></tr>
<tr><td>8-й</td><td>8-й</td></tr>
<tr><td colspan="2">Лекції</td></tr>
<tr><td rowspan="9">Мова навчання – українська</td><td>26 год.</td><td>6 год.</td></tr>
<tr><td colspan="2">Практичні, семінарські</td></tr>
<tr><td>20 год.</td><td>4 год.</td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td>20 год.</td><td>4 год.</td></tr>
<tr><td colspan="2">Самостійна робота та індивідуальні завдання</td></tr>
<tr><td>114 год.</td><td>166 год.</td></tr>
<tr><td colspan="2">Вид контролю:</td></tr>
<tr><td>екзамен</td><td>екзамен</td></tr>
</table>

Етичний хакінг та тестування на проникнення – це дисципліна, яка присвячена вивченню принципів етичного хакінгу та методологій тестування на проникнення з метою забезпечення кібербезпеки комп’ютерних систем, мережевої інфраструктури та вебзастосунків. Здобувачі отримують знання про сучасні підходи до пошуку вразливостей, аналіз безпеки мережевих протоколів, операційних систем, сервісів і веб-ресурсів.

У межах курсу розглядаються практичні сценарії атак відповідно до міжнародних методологій, зокрема OWASP, а також досліджуються поширені класи вразливостей – від мережевих і системних атак до веб-ін’єкцій (SQLi, XSS, CSRF), Command Injection, File Inclusion та атак на механізми автентифікації й авторизації.

Практична частина реалізується на основі безпечних навчальних платформ, таких як DVWA, Metasploitable, що дозволяє здобувачам відпрацювати техніки експлуатації вразливостей, аналіз ризиків та розроблення рекомендацій щодо підвищення рівня захищеності інформаційних систем.

Метою навчальної дисципліни є формування у здобувачів системного розуміння принципів етичного хакингу та сучасних методологій тестування на проникнення, а також набуття практичних навичок виявлення, аналізу та експлуатації вразливостей у комп’ютерних системах, мережевих інфраструктурах і вебзастосунках.

ПРЕРЕКВІЗИТИ: дисципліни циклу професійної підготовки – «Основи програмування» (ОК 8), «Захист інформації в інфокомунікаційних системах та мережах» (ОК 12), «Комп'ютерні мережі» (ОК 13), «Web-технології» (ОК 14), «Безпека програм та даних» (ОК 16), «Криптографія та криптоаналіз» (ОК 23), знання з яких є необхідною базою для опанування освітнього компонента.

ПОСТРЕКВІЗИТИ: результати навчання за дисципліною інтегрують та узагальнюють

компетентності, сформовані протягом освітньої програми, та застосовуються під час підготовки і захисту кваліфікаційної роботи, а також у професійній діяльності за спеціальністю.

2. ОЧІКУВАНІ КОМПЕТЕНТНОСТІ, ЯКІ ПЛАНУЄТЬСЯ СФОРМУВАТИ ТА ДОСЯГНЕННЯ ПРОГРАМНИХ РЕЗУЛЬТАТІВ

У процесі реалізації програми дисципліни «Етичний хакінг та тестування на проникнення» формуються наступні компетентності із передбачених освітньою програмою:

Інтегральна компетентність

Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі кібербезпеки та захисту інформації.

Загальні компетентності (ЗК)

ЗК1. Здатність застосовувати знання у практичних ситуаціях.

ЗК 2 Знання та розуміння предметної області та розуміння професійної діяльності

Спеціальні (фахові) компетентності

СК 2. Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації

СК 4. Здатність забезпечувати захист інформації в інформаційних та інформаційно-комунікаційних системах згідно встановленої політики кібербезпеки й захисту інформації.

СК 10. Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.

СК 11. Здатність здійснювати проєктування, адміністрування та керування інформаційно-комунікаційними системами, забезпечуючи їхню надійність, безпеку та ефективність функціонування.

Навчальна дисципліна «Етичний хакінг та тестування на проникнення» забезпечує досягнення програмних результатів навчання (РН), передбачених освітньою програмою:

РН 4. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність

РН 10. Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.

РН 15. Збирати, обробляти зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводили аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи.

РН 18. Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.

РН 19. Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів.

РН 20. Визначати загрози створення технічних каналів витоку інформації на об'єктах інформаційної діяльності; впроваджувати засоби і заходи технічного захисту інформації від витоку технічними каналами, проводити обслуговування і контроль стану апаратних засобів захисту інформації та комплексів технічною захисту інформації.

РН 21. Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору й інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.

РН 22. Вміти застосовувати методи та інструменти проєктування й адміністрування мереж і систем, виконувати налаштування, моніторинг та підтримку їхньої працездатності з урахуванням вимог інформаційної безпеки.

Заплановані результати навчання за навчальною дисципліною

Знання:

1. На понятійному рівні – системно розуміти основні категорії, поняття та їх визначення у сфері етичного хакінгу та тестування на проникнення, структуру та зміст дисципліни, а також принципи, підходи й етапи проведення тестування на проникнення відповідно до міжнародних стандартів і методологій (OWASP, PTES, NIST), включаючи ризик-орієнтований підхід до оцінювання безпеки.
2. Описувати сучасний ландшафт кіберзагроз (threat landscape), типові та критичні вразливості інформаційних систем, мережевих інфраструктур і вебзастосунків (зокрема відповідно до OWASP Top 10), а також сучасні методи їх виявлення, аналізу, класифікації та усунення з урахуванням практик забезпечення кіберстійкості.

Уміння:

3. Розуміти процеси проведення тестування на проникнення та якісні зміни у сфері кібербезпеки, пов'язані з розвитком інформаційних технологій.
4. Визначати вразливості інформаційних систем, мережевих сервісів та вебзастосунків із застосуванням сучасних інструментів аналізу безпеки.
5. Пояснювати механізми реалізації атак (зокрема ін'єкційних, клієнтських, мережевих) та принципи їх запобігання.
6. Застосовувати знання:
   a. на рівні відтворення – виконувати базові етапи тестування на проникнення, аналізувати результати сканування та оцінювати ризики;
   b. на творчому рівні – розробляти сценарії тестування, проводити комплексний аналіз захищеності систем, формувати рекомендації щодо підвищення рівня кібербезпеки.

Навички:

7. Використовувати спеціалізовані інструменти етичного хакінгу (зокрема Kali Linux, Nmap, Metasploit, Burp Suite, DVWA) для виявлення та аналізу вразливостей.
8. Аргументовано обговорювати та пояснювати результати тестування на проникнення, формувати звіти (penetration testing report) та обґрунтовувати рекомендації щодо усунення вразливостей і підвищення захищеності інформаційних систем.

3. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Тема 1. Вступ до етичного хакінгу та тестування на проникнення

У межах теми розглядаються теоретичні засади етичного хакінгу та тестування на проникнення як складових сучасної кібербезпеки. Визначаються основні поняття, категорії та підходи до оцінювання захищеності інформаційних систем, а також місце тестування на приникнення у загальній системі забезпечення інформаційної безпеки. Особлива увага приділяється розмежуванню понять тестування на проникнення, оцінки вразливостей та етичного хакінгу.

Окремо аналізуються міжнародні стандарти та методології проведення тестування на проникнення (OWASP, PTES, NIST), а також етапи життєвого циклу тестування на приникнення. Розглядаються правові та етичні аспекти діяльності фахівців з кібербезпеки, включаючи питання визначення меж тестування (scope), відповідальності та дотримання принципів академічної та професійної доброчесності.

Тема 2. Розвідка та збір інформації

Тема присвячена дослідженню процесів збору та аналізу інформації про ціль тестування, які є критично важливими для подальших етапів тестування на проникнення. Розглядаються підходи до проведення пасивної та активної розвідки, а також методи отримання відкритої інформації (OSINT), що дозволяють сформувати початкову модель досліджуваної системи.

Особлива увага приділяється методам сканування мережевої інфраструктури, виявлення активних хостів, відкритих портів та сервісів, а також технікам ідентифікації операційних систем і програмного забезпечення (fingerprinting). Аналізуються способи інтерпретації отриманих даних

для побудови подальшої стратегії тестування на проникнення.

Тема 3. Аналіз вразливостей

У межах теми розглядаються підходи до виявлення, класифікації та оцінювання вразливостей інформаційних систем. Аналізуються сучасні моделі класифікації, зокрема OWASP Top 10, а також принципи функціонування автоматизованих сканерів вразливостей.

Окрему увагу приділено оцінюванню ризиків за допомогою стандартизованих методик, таких як CVSS, що дозволяє визначати критичність виявлених вразливостей. Розглядаються підходи до пріоритезації ризиків та планування подальших дій у процесі тестування на проникнення.

Тема 4. Веб-вразливості: ін'єкційні атаки

Тема охоплює дослідження ін'єкційних вразливостей як одного з найбільш критичних класів загроз для вебзастосунків. Розглядаються механізми виникнення та реалізації атак типу SQL Injection, Command Injection, LDAP Injection та інших форм ін'єкційного впливу.

Особлива увага приділяється аналізу способів обходу механізмів фільтрації та валідації вхідних даних, а також інтерпретації відповідей сервера. Досліджуються сучасні підходи до виявлення та запобігання ін'єкційним атакам у контексті безпечної розробки вебзастосунків.

Тема 5. Веб-вразливості: клієнтські атаки

У межах теми розглядаються клієнтські вразливості вебзастосунків, які пов'язані з обробкою даних на стороні користувача. Аналізуються основні типи атак, зокрема Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), а також вразливості включення файлів (LFI/RFI).

Окрема увага приділяється механізмам управління сесіями, автентифікації та авторизації, включаючи загрози захоплення сесій (session hijacking) та маніпуляцій з cookies. Розглядаються сучасні методи виявлення та запобігання клієнтським атакам.

Тема 6. Експлуатація, підвищення привілеїв та постексплуатація

Тема присвячена практичним аспектам реалізації атак після виявлення вразливостей. Розглядаються основні підходи до експлуатації вразливостей, а також методи отримання несанкціонованого доступу до системи.

Особлива увага приділяється технікам підвищення привілеїв, переміщення всередині мережі (pivoting) та закріплення доступу. Аналізуються принципи постексплуатаційної діяльності, включаючи збір інформації, оцінювання стійкості системи та використання спеціалізованих інструментів, таких як Metasploit Framework.

Тема 7. Звітність, виправлення вразливостей та побудова захисту

У межах теми розглядаються підходи до документування результатів тестування на проникнення та формування звітності. Визначаються структура та зміст звіту з тестування на проникнення, а також принципи представлення результатів аналізу вразливостей.

Окремо досліджуються методи оцінювання ризиків та пріоритезації вразливостей, що дозволяє ефективно планувати заходи з їх усунення. Розглядаються підходи до виправлення вразливостей та інтеграції принципів безпеки у життєвий цикл розробки програмного забезпечення (Secure SDLC), а також методи перевірки ефективності впроваджених заходів захисту.

4. СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Назви змістових модулів і тем	Кількість годин									
	денна форма					Заочна форма				
	усього	у тому числі				усього	у тому числі			
		лекц.	лаб.	практ.	сам. роб.		лекц.	лаб.	практ.	сам. роб.
Тема 1. Вступ до етичного хакінгу та пентесту	26	4	3	3	16	23	-	-	-	23
Тема 2. Розвідка та збір інформації	26	4	3	3	16	27	2	-	2	23
Тема 3. Аналіз вразливостей	26	4	3	3	16	25	-	2	-	23
Тема 4. Веб-вразливості: ін’єкційні атаки	26	4	3	3	16	27	2	-	2	23
Тема 5. Веб-вразливості: клієнтські атаки	26	4	3	3	16	27	2	2	-	23
Тема 6. Експлуатація, підвищення привілеїв та постексплуатація	25	3	3	3	16	25	-	-	-	25
Тема 7. Звітність, виправлення вразливостей та побудова захисту	25	3	2	2	18	26	-	-	-	26
Усього годин	**180**	**26**	**20**	**20**	**114**	***180***	***6***	***4***	***4***	***166***
ПІДСУМКОВИЙ КОНТРОЛЬ - ЕКЗАМЕН										

5. ПИТАННЯ ДО ПРАКТИЧНИХ ЗАНЯТЬ

№ з/п	Назва теми	Кількість годин	
		денна форма	заочна форма
1	**Тема 1. Вступ до етичного хакінгу та тестування на проникнення** 1. Аналіз понять етичний хакінг, тестування на проникнення та оцінка вразливості. 2. Моделі взаємодії Red Team, Blue Team та Purple Team. 3. Етапи проведення тестування на проникнення за стандартами OWASP та PTES. 4. Правові та етичні аспекти проведення тестування на проникнення. 5. Формування мети та правил проведення тестування.	2	-
2	**Тема 2. Розвідка та збір інформації** 1. Пасивна та активна розвідка в процесі тестування на проникнення. 2. Використання OSINT для збору інформації про ціль. 3. Сканування мережі та виявлення хостів. 4. Аналіз відкритих портів і сервісів. 5. Ідентифікація операційних систем та версій програмного забезпечення.	2	-
3	**Тема 3. Аналіз вразливостей** 1. Класифікація вразливостей (OWASP Top 10). 2. Використання автоматизованих сканерів вразливостей. 3. Інтерпретація результатів сканування. 4. Оцінювання ризиків за методикою CVSS. 5. Пріоритезація вразливостей для подальшої експлуатації.	2	2
4	**Тема 4. Веб-вразливості: ін'єкційні атаки** 1. Механізми реалізації SQL Injection. 2. Аналіз та експлуатація Command Injection. 3. LDAP Injection та інші типи ін'єкцій. 4. Методи обходу фільтрації введених даних. 5. Методи виявлення та запобігання ін'єкційним атакам.	2	-
5	**Тема 5. Веб-вразливості: клієнтські атаки** 1. Аналіз XSS (збережений та відображений). 2. Механізми реалізації CSRF-атак. 3. Вразливості типу LFI/RFI. 4. Захоплення сесій та маніпуляції з cookies. 5. Методи захисту від клієнтських атак.	4	-
6	**Тема 6. Експлуатація, підвищення привілеїв та постексплуатація** 1. Основні підходи до експлуатації вразливостей. 2. Методи підвищення привілеїв у системах. 3. Переміщення в мережі (pivoting). 4. Використання Metasploit Framework. 5. Закріплення доступу та постексплуатаційні дії.	4	2
7	**Тема 7. Звітність, виправлення вразливостей та побудова захисту** 1. Структура звіту з тестування на проникнення.	4	-

	2. Аналіз та оцінювання ризиків. 3. Пріоритезація вразливостей. 4. Розробка рекомендацій щодо усунення вразливостей. 5. Інтеграція принципів Secure SDLC.		
	Всього	**20**	**4**

5. ЛАБОРАТОРНІ РОБОТИ

№ з/п	Назва теми	Кількість годин	
		денна форма	заочна форма
1	**Дослідження структури мережі із застосуванням утиліти nmap та пошук вразливостей** Мета роботи — закріпити теоретичні знання по застосуванню утиліти nmap для дослідження структури мережі. Отримати практичні навички із дослідження структури мережі та пошуку вразливостей.	2	-
2	**Дослідження атак SQLi проти вразливих веб-застосунків і шляхів захисту від таких атак** Мета роботи — закріпити теоретичні знання по атакам SQLi, отримати практичні навички по тестуванню можливості проведення таких атак і захисту проти них на прикладі DVWA.	2	-
3	**Дослідження атак Brute Force проти вразливих веб-застосунків і шляхів захисту від таких атак** Мета роботи — ознайомитися з методами проведення атак Brute Force на веб-додатки, дослідити механізми захисту від таких атак та навчитися їх обходити. Використати утиліти Burp Suite та Hydra для проведення атак на DVWA при різних рівнях складності безпеки.	2	2
4	**Дослідження атак Command Injection проти вразливих веб-застосунків і шляхів захисту від таких атак** Мета роботи — ознайомитися з методами проведення атак Command Injection на веб-додатки, дослідити механізми захисту від таких атак та навчитися їх обходити. Набути навички створення та використання Reverse Shell.	2	-
5	**Дослідження атак CSRF проти вразливих веб-застосунків і шляхів захисту від таких атак** Мета роботи — закріпити теоретичні відомості про атаки CSRF, набути практичні навички виконання даного виду атак та захисту від них.	2	-
6	**Дослідження атак Local та Remote File Inclusion проти вразливих веб-застосунків і шляхів захисту від таких атак** Мета роботи — навчитись експлуатувати вразливості Local та Remote File Inclusion у DVWA, включаючи отримання Reverse Shell для демонстрації повноцінного компрометування системи.	2	2
7	**Дослідження атак XSS проти вразливих веб-застосунків і шляхів захисту від таких атак** Мета роботи – дослідити різні типи XSS-атак (DOM-based, Reflected, Stored) за допомогою вразливого веб-додатку DVWA (Damn Vulnerable Web Application). Навчитися ідентифікувати, експлуатувати та запобігати XSS-вразливостям.	2	-
8	**Дослідження контролю доступу та уразливостей Authorisation Bypass** Мета роботи — дослідити механізми контролю доступу у веб-додатках, вивчити уразливість Authorisation Bypass та способи її використання на прикладі DVWA (Damn Vulnerable Web Application).	2	-
9	**Open HTTP Redirect: вивчення вразливості та практичне тестування на DVWA** Мета роботи — дослідити, як виникає вразливість Open Redirect, навчитися експлуатувати її на різних рівнях складності у DVWA, та ознайомитися із способами її запобігання.	2	-
10	**Клієнтські атаки через браузерні інструменти** Мета роботи — ознайомлення з можливостями користувача втручатися у виконання JavaScript-коду в браузері та вивчення потенційних ризиків для безпеки веб-застосунків.	2	-
	Всього	**20**	**4**

6. САМОСТІЙНА РОБОТА

До самостійної роботи студентів щодо вивчення дисципліни «Етичний хакінг та тестування на проникнення» включаються:

1. Знайомство з науковою та навчальною літературою відповідно зазначених у програмі тем.
2. Опрацювання лекційного матеріалу.
3. Підготовка до практичних занять.
4. Консультації з викладачем протягом семестру.
5. Самостійне опрацювання окремих питань навчальної дисципліни.
6. Підготовка та виконання індивідуальних завдань.
7. Підготовка до підсумкового контролю.

Тематика та питання до самостійної підготовки та індивідуальних завдань

№ з/п	Назва теми	Кількість годин	
		денна форма	заочна форма
1	**Тема 1. Вступ до етичного хакінгу та тестування на проникнення** Поняття етичного хакінгу та тестування на проникнення. Мета, завдання та сфери застосування тестування на проникнення. Співвідношення аналізу вразливостей і тестування на проникнення. Типологія хакерської діяльності: black hat, white hat, grey hat. Командні моделі протиборства: Red Team, Blue Team, Purple Team. Правові та етичні засади проведення тестування. Договірні межі та правила виконання робіт. Стандарти й методології тестування (OWASP, Penetration Testing Execution Standard, National Institute of Standards and Technology). Етапи життєвого циклу тестування на проникнення: планування, збір інформації, виявлення вразливостей, експлуатація, післяексплуатаційний аналіз, підготовка звіту.	16	23
2	**Тема 2. Розвідка та збір інформації** Пасивна та активна розвідка. Методи збору відкритої інформації (OSINT). Сканування мережі та виявлення хостів. Визначення відкритих сервісів та їхніх версій. Техніки ідентифікації операційних систем та fingerprinting. Використання інструментів автоматизації сканування, зокрема Nmap. Аналіз отриманих даних для подальшого планування тестування на проникнення.	16	23
3	**Тема 3. Аналіз вразливостей** Класифікація вразливостей інформаційних систем. Основні категорії та приклади OWASP Top 10. Використання автоматизованих сканерів для виявлення вразливостей. Оцінювання ризиків та їхніх наслідків за методикою CVSS. Підготовка до експлуатації виявлених вразливостей. Аналіз пріоритетності та планування подальших дій у пентесті.	16	23
4	**Тема 4. Веб-вразливості: ін’єкційні атаки** Поняття ін’єкційних атак та механізми їх реалізації. SQL Injection (класична та «сліпа»). Command Injection. LDAP Injection. Методи обходу механізмів фільтрації та валідації введених даних. Аналіз відповідей сервера та інтерпретація результатів ін’єкційних впливів. Виявлення та запобігання ін’єкційним вразливостям.	16	23
5	**Тема 5. Веб-вразливості: клієнтські атаки** Cross-Site Scripting (збережене та відображене). Cross-Site Request Forgery (CSRF). Local та Remote File Inclusion (LFI/RFI). Захоплення сесій (Session Hijacking). Маніпуляції з cookies та механізмами автентифікації. Методи виявлення та запобігання клієнтським веб-аткам.	16	23

6	**Тема 6. Експлуатація, підвищення привілеїв та постексплуатація** Етапи експлуатації вразливостей. Методи закріплення доступу в системі. Підвищення привілеїв (Privilege Escalation) у середовищах різного типу. Переміщення всередині мережі (Pivoting). Теоретичні основи аналізу стійкості паролів та підходи до їх перевірки. Загальні принципи роботи фреймворку Metasploit.	16	23
7	**Тема 7. Звітність, виправлення вразливостей та побудова захисту** Структура звіту з тестування на проникнення (penetration testing report). Оцінка ризиків (Risk Assessment) та пріоритезація вразливостей. Рекомендації щодо усунення виявлених вразливостей. Інтеграція принципів безпечного життєвого циклу розробки програмного забезпечення (Secure SDLC). Практичні підходи до захисту від атак на прикладі лабораторного середовища DVWA. Контроль та перевірка ефективності впроваджених заходів.	18	28
	Всього	**114**	**166**

7. ВИДИ ТА МЕТОДИ КОНТРОЛЮ

Види контролю	Складові оцінювання
поточний контроль, який здійснюється у ході: проведення практичних (лабораторних) занять, виконання самостійної роботи, індивідуальних завдань, дослідна робота здобувача тощо.	**50%**
підсумковий контроль	**50%**

Методи діагностики знань (контролю)	**фронтальне опитування; наукова доповідь, реферати, усне повідомлення, індивідуальне опитування; робота у групах; ділова гра, розв`язання ситуаційних завдань, кейсів, практичних завдань, екзамен**

Питання до екзамену

1. Розкрийте сутність етичного хакінгу як складової сучасної системи кібербезпеки. Обґрунтуйте його роль у забезпеченні захисту інформаційних систем.
2. Порівняйте тестування на проникнення та оцінку вразливостей: визначте їх спільні риси, відмінності та сфери застосування.
3. Охарактеризуйте основні цілі, завдання та очікувані результати тестування на проникнення в контексті управління кіберризиками.
4. Проаналізуйте класифікацію хакерської діяльності (white hat, black hat, grey hat) та визначте етичні межі професійної діяльності фахівця.
5. Розкрийте сутність моделей Red Team, Blue Team та Purple Team, поясніть їхню взаємодію у процесі забезпечення кібербезпеки.
6. Детально охарактеризуйте етапи проведення тестування на проникнення та їх взаємозв’язок.
7. Проаналізуйте міжнародні стандарти та методології (OWASP, PTES, NIST) у контексті організації тестування на проникнення.
8. Поясніть значення визначення меж тестування (scope) та проаналізуйте ризики його некоректного формування.
9. Обґрунтуйте роль етапу розвідки у процесі тестування на проникнення та його вплив на ефективність подальших атак.
10. Порівняйте пасивну та активну розвідку, визначте їх переваги, недоліки та сфери застосування.
11. Розкрийте сутність OSINT та проаналізуйте його можливості для збору інформації про ціль.
12. Охарактеризуйте методи сканування мережі та поясніть їх значення для виявлення потенційних точок входу.
13. Поясніть принципи виявлення активних хостів і відкритих портів та їх значення для аналізу безпеки.
14. Розкрийте методи fingerprinting операційних систем і сервісів та оцініть їхню точність і обмеження.
15. Проаналізуйте, як результати розвідки використовуються для формування стратегії тестування на проникнення.
16. Оцініть ризики та обмеження, пов’язані зі збором інформації в умовах реальних систем.
17. Розкрийте поняття вразливості інформаційної системи та її роль у формуванні кіберзагроз.
18. Проаналізуйте класифікацію OWASP Top 10 та її значення для сучасної практики кібербезпеки.
19. Охарактеризуйте принципи роботи автоматизованих сканерів вразливостей та їх обмеження.
20. Поясніть поняття false positive та false negative і проаналізуйте їх вплив на результати тестування.

21. Розкрийте методику CVSS та поясніть її застосування для оцінювання ризиків.
22. Проаналізуйте підходи до визначення критичності вразливостей у різних системах.
23. Обґрунтуйте необхідність пріоритезації вразливостей та запропонуйте критерії її здійснення.
24. Розкрийте взаємозв'язок між вразливостями, загрозами та ризиками у кібербезпеці.
25. Розкрийте природу ін'єкційних атак та поясніть причини їх виникнення у вебзастосунках.
26. Детально проаналізуйте механізм SQL Injection та можливі наслідки його реалізації.
27. Порівняйте різні типи SQL Injection (in-band, blind) та їх особливості.
28. Охарактеризуйте Command Injection та поясніть принципи його експлуатації.
29. Проаналізуйте інші типи ін'єкцій (LDAP, XPath тощо) та їх специфіку.
30. Розкрийте методи обходу фільтрації та валідації введених даних.
31. Поясніть, як аналіз відповідей сервера дозволяє виявляти ін'єкційні вразливості.
32. Обґрунтуйте сучасні підходи до захисту від ін'єкційних атак.
33. Розкрийте сутність клієнтських атак та їх місце у структурі веб-загроз.
34. Детально проаналізуйте механізм Cross-Site Scripting (XSS) та його види.
35. Порівняйте stored та reflected XSS з точки зору ризиків та складності реалізації.
36. Поясніть механізм CSRF-атак та умови їх успішної реалізації.
37. Охарактеризуйте вразливості LFI та RFI та їх потенційні наслідки.
38. Проаналізуйте механізми session hijacking та їх вплив на безпеку системи.
39. Розкрийте роль cookies у забезпеченні безпеки та можливості їх компрометації.
40. Обґрунтуйте методи захисту від клієнтських атак.
41. Розкрийте сутність експлуатації вразливостей та її роль у тестуванні на проникнення.
42. Охарактеризуйте основні етапи процесу експлуатації та їх взаємозв'язок.
43. Поясніть поняття ескалації привілеїв та його значення для компрометації системи.
44. Порівняйте вертикальне та горизонтальне підвищення привілеїв.
45. Розкрийте сутність переміщення всередині мережі (pivoting) та поясніть його роль у розширенні атаки.
46. Охарактеризуйте методи закріплення доступу (persistence) у системі.
47. Поясніть принципи роботи Metasploit Framework у контексті експлуатації.
48. Проаналізуйте завдання та методи постексплуатаційної діяльності.
49. Розкрийте значення звітності у процесі тестування на проникнення.
50. Охарактеризуйте структуру звіту про тестування на проникнення та його основні розділи.
51. Поясніть підходи до оцінювання ризиків у звіті.
52. Проаналізуйте принципи пріоритезації вразливостей у звітності.
53. Розкрийте сутність виправлення вразливостей та її роль у підвищенні безпеки.
54. Обґрунтуйте підходи до формування рекомендацій щодо усунення вразливостей.
55. Поясніть принципи Secure SDLC та їх значення для запобігання вразливостям.
56. Охарактеризуйте методи контролю ефективності впроваджених заходів захисту.
57. Обґрунтуйте роль етичного хакінгу в сучасній системі управління кібербезпекою.
58. Проаналізуйте взаємозв'язок між тестуванням на проникнення та управлінням ризиками.
59. Розкрийте етичні та правові аспекти діяльності фахівця з кібербезпеки.
60. Оцініть сучасні тенденції розвитку тестування на проникнення (автоматизація, AI, DevSecOps).

8. ОЦІНЮВАННЯ ЗДОБУВАЧІВ ВИЩОЇ ТА ФАХОВОЇ ПЕРДВИЩОЇ ОСВІТИ ЗА НАВЧАЛЬНУ ДИСЦИПЛІНУ У МІЖНАРОДНОМУ ГУМАНІТАРНОМУ УНІВЕРСИТЕТІ

(*поточний контроль, підсумковий контроль, загальний результат оцінювання)*

ЕКЗАМЕН

Поточний контроль			
Види роботи	**Планові терміни виконання**	**Форми контролю та звітності**	**Максимальний відсоток оцінювання**
Систематичність і активність роботи на практичних (лабораторних) заняттях			
1.1. Підготовка до практичних, лабораторних занять	Відповідно до робочої програми та розкладу занять	Перевірка обсягу та якості засвоєного матеріалу під час практичних (лабораторних) занять	**30**
Виконання завдань для самостійного опрацювання			
1.2. Індивідуальне тестування, завдання за заданою тематикою	Відповідно до робочої програми та розкладу занять	Розгляд відповідного матеріалу під час аудиторних занять або ІКР[1], перевірка конспектів навчальних текстів тощо	**10**
Виконання індивідуальних завдань, дослідна робота здобувача			
1.3. Інші види індивідуальних завдань, в т.ч.підготовка наукових публікацій, участь у роботі круглих столів, конференцій тощо.	Відповідно до робочої програми та розкладу занять	Обговорення результатів проведеної роботи під час аудиторних занять, наукових конференцій та круглих столів.	**10**
Разом балів за поточний контроль			**50**
Підсумковий контроль екзамен			**50**
Загальний результат оцінювання			**100**

Поточний контроль знань здобувачів освіти при формі контролю **екзамен** (максимум 50 балів) оцінюється за шкалою *(«2», «3», «4», «5»)*, з обов'язковим переведенням балів за кожний вид роботи таким чином:

- за підготовку до аудиторних занять (максимум 30 балів) здобувачу освіти необхідно мати не менше 1/2 оцінок від загальної кількості практичних (лабораторних) занять, для переводу балів за підготовку до аудиторних занять середньоарифметична оцінка множиться на коефіцієнт 6;
- за виконання завдань для самостійного опрацювання (тестування, завдання, підготовка реферату (есе) за заданою тематикою) (максимум 10 балів) здобувачу освіти необхідно мати не менше 1/2 оцінок від загальної кількості програмного матеріалу, що виноситься на самостійне вивчення, для переводу зазначених балів середньоарифметична оцінка множиться на коефіцієнт 2;
- за інші види індивідуальних завдань, в т.ч. підготовку наукових публікацій, участь у роботі круглих столів, конференцій тощо (максимум 10- балів) здобувачу освіти необхідно мати не менше 1/2 оцінок від загальної кількості інших видів індивідуальних завдань, для переводу

[1] Індивідуально-консультативна робота викладача зі здобувачами

балів за підготовку до аудиторних занять середньоарифметична оцінка множиться на коефіцієнт 2.

КРИТЕРІЇ ОЦІНЮВАННЯ ЗА ПОТОЧНИЙ КОНТРОЛЬ

- «2»- виставляється за неправильну відповідь (письмову роботу), яка не відповідає змісту теми та свідчить про нерозуміння її основних положень;
- «3» -виставляється за відповідь (письмову роботу), яка відповідає змісту теми, але є неповною і неточною у визначенні понять, свідчить про неповне розуміння основних положень навчального матеріалу, свідчить про те, що знання студента мають фрагментарний, поверховий характер;
- «4» - оцінюється правильна і обґрунтована відповідь (письмова робота), з якої видно, що студент знає й розуміє теоретичний матеріал в обсязі навчальної теми, володіє необхідними навичками, не допускає суттєвих помилок.
- «5» - оцінюється повна, правильна, ґрунтовна відповідь (письмова робота) на запитання теми, що передбачає логічність і послідовність викладу матеріалу, володіння термінологією, показує вміння повно й глибоко використовувати теоретичні знання в практичній площині.

КРИТЕРІЇ ОЦІНЮВАННЯ ПІДСУМКОВОГО КОНТРОЛЮ ЗНАНЬ ЗДОБУВАЧІВ ЗА ЕКЗАМЕН
(максимум 50 балів)

Рівень знань оцінюється:

- від 40 до 50 балів - студент виявляє особливі творчі здібності, вміє самостійно знаходити та опрацьовувати необхідну інформацію, демонструє знання матеріалу, проводить узагальнення і висновки;
- 30 до 40 балів - студент володіє знаннями матеріалу, але допускає незначні помилки у формуванні термінів, категорій, проте за допомогою викладача швидко орієнтується і знаходить правильні відповіді;
- 20 - 30 балів - студент відтворює значну частину теоретичного матеріалу, виявляє знання і розуміння основних положень, з допомогою викладача може аналізувати навчальний матеріал, але дає недостатньо обґрунтовані, невичерпні відповіді, допускає помилки.
- 10 - 20 балів - володіє навчальним матеріалом на середньому рівні, допускає помилки, серед яких є значна кількість суттєвих;
- 0 10 балів - володіє навчальним матеріалом на рівні, вищому за початковий, значну частину його відтворює на репродуктивному рівні, на всі запитання дає необґрунтовані, невичерпні відповіді, допускає помилки.

Поточний контроль знань здобувачів освіти оцінюється за шкалою *(«2», «3», «4», «5»)*, з обов'язковим переведенням балів за кожний вид роботи таким чином:

- за підготовку до аудиторних занять (максимум 60 балів) здобувачу освіти необхідно мати не менше 1/2 оцінок від загальної кількості практичних (лабораторних) занять, для переводу балів за підготовку до аудиторних занять середньоарифметична оцінка множиться на коефіцієнт 12;
- за виконання завдань для самостійного опрацювання (тестування, завдання, підготовка реферату (есе) за заданою тематикою) (максимум 20 балів) здобувачу освіти необхідно мати не менше 1/2 оцінок від загальної кількості програмного матеріалу, що виноситься на самостійне вивчення, для переводу зазначених балів середньоарифметична оцінка множиться на коефіцієнт 4;
- за інші види індивідуальних завдань, в т.ч. підготовку наукових публікацій, участь у роботі круглих столів, конференцій тощо (максимум 20- балів) здобувачу освіти необхідно мати не менше 1/2 оцінок від загальної кількості інших видів індивідуальних завдань, для переводу балів за підготовку до аудиторних занять середньоарифметична оцінка множиться на коефіцієнт 4.

9. КРИТЕРІЇ ЗАГАЛЬНИХ РЕЗУЛЬТАТІВ ОЦІНЮВАННЯ ЗНАНЬ ЗДОБУВАЧІВ

Рівень знань оцінюється:

- «відмінно» / «зараховано» A - від 90 до 100 балів. Студент виявляє особливі творчі здібності, вміє самостійно знаходити та опрацьовувати необхідну інформацію, демонструє знання матеріалу, проводить узагальнення і висновки. Був присутній на лекціях та семінарських заняттях, під час яких давав вичерпні, обґрунтовані, теоретично і практично правильні відповіді, має конспект з виконаними завданнями до самостійної роботи, презентував реферат (есе) за заданою тематикою, проявляє активність і творчість у науково-дослідній роботі;
- «добре» / «зараховано» B - від 82 до 89 балів. Студент володіє знаннями матеріалу, але допускає незначні помилки у формуванні термінів, категорій, проте за допомогою викладача швидко орієнтується і знаходить правильні відповіді. Був присутній на лекціях та семінарських заняттях, має конспект з виконаними завданнями до самостійної роботи, презентував реферат (есе) за заданою тематикою, проявляє активність і творчість у науково-дослідній роботі;
- «добре» / «зараховано» C - від 74 до 81 балів. Студент відтворює значну частину теоретичного матеріалу, виявляє знання і розуміння основних положень, з допомогою викладача може аналізувати навчальний матеріал, але дає недостатньо обґрунтовані, невичерпні відповіді, допускає помилки. При цьому враховується наявність конспекту з виконаними завданнями до самостійної роботи, реферату та активність у науково-дослідній роботі;
- «задовільно» / «зараховано» D - від 64 до 73 балів. Студент був присутній не на всіх лекціях та семінарських заняттях, володіє навчальним матеріалом на середньому рівні, допускає помилки, серед яких є значна кількість суттєвих. При цьому враховується наявність конспекту з виконаними завданнями до самостійної роботи, рефератів (есе);
- «задовільно» / «зараховано» E - від 60 до 63 балів. Студент був присутній не на всіх лекціях та семінарських заняттях, володіє навчальним матеріалом на рівні, вищому за початковий, значну частину його відтворює на репродуктивному рівні, на всі запитання дає необґрунтовані, невичерпні відповіді, допускає помилки, має неповний конспект з завданнями до самостійної роботи.
- «незадовільно з можливістю повторного складання» / «не зараховано» FX – від 35 до 59 балів. Студент володіє матеріалом на рівні окремих фрагментів, що становлять незначну частину навчального матеріалу.
- «незадовільно з обов'язковим повторним вивченням дисципліни» / «не зараховано» F – від 0 до 34 балів. Студент не володіє навчальним матеріалом.

ТАБЛИЦЯ ВІДПОВІДНОСТІ ЗАГАЛЬНИХ РЕЗУЛЬТАТІВ ОЦІНЮВАННЯ ЗНАНЬ ЗА РІЗНИМИ ШКАЛАМИ

100-бальною шкалою	Шкала за ECTS	За національною шкалою	
		екзамен	залік
90-100	A	Відмінно	Зараховано
82-89	B	Добре	
74-81	C		
64-73	D	Задовільно	
60-63	E		
35-59	Fx	Незадовільно	Не зараховано
1-34	F		

10. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

1. Harper A. Gray Hat Hacking: The Ethical Hacker's Handbook, 6th Edition. McGraw Hill, 2022. 704 p.
2. Brooks-Kempler M. Scams, Hacking, and Cybersecurity: The Ultimate Guide to Online Safety and Privacy. Authority Publishing, 2024. 219 p.
3. Graham D. Ethical Hacking: A Hands-on Introduction to Breaking In. No Starch Press, 2021. 376 p.
4. Singh G.D. et al. The Ultimate Kali Linux Book: Perform Advanced Penetration Testing Using Nmap, Metasploit, Aircrack-Ng, and Empire, 2nd Edition.
5. Dangi R. OWASP for Secure Web Applications. B0DBNRRTNJ, 2024. 204 p.

Допоміжна

6. Alhamed M., Rahman M. M. H. A systematic literature review on penetration testing in networks: future research directions. Applied Sciences. 2023. Vol. 13, No. 12. P. 6986.
7. Garg D., Bansal N. A systematic review on penetration testing. 2nd Global Conference for Advancement in Technology (GCAT), IEEE, 2021. P. 1-4.
8. Krishnama S. et al. A process of penetration testing using various tools. Mesopotamian Journal of CyberSecurity. 2023. Vol. 2023. P. 93-103.
9. Lazarov W. et al. Penterep: Comprehensive penetration testing with adaptable interactive checklists. Computers & Security. 2025. Vol. 154. P. 104399.
10. Confido A., Ntagiou E. V., Wallum M. Reinforcing penetration testing using ai. IEEE Aerospace Conference (AERO). IEEE, 2022. P. 1-15.

Інформаційні ресурси

11. Національна бібліотека України ім. В.І. Вернадського : веб-сайт. URL: http://www.nbuv.gov.ua.
12. Он-лайн бібліотека. URL: http://www.lib.com.ua
13. http://www.info-library.com.ua/books-book-149.html
14. https://owasp.org – OWASP
15. https://portswigger.net – Portswigger