Міжнародний гуманітарний університет
Факультет кібербезпеки, програмної інженерії
та комп'ютерних наук
Кафедра комп'ютерної інженерії та інноваційних технологій

СИЛАБУС 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

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

1. АНОТАЦІЯ ДО КУРСУ

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. Передумовами є знання, уміння та навички, отримані при вивченні «Комп'ютерних мереж» (ОК 13), «Захисту інформації в інфокомунікаційних системах та мережах» (ОК 12), «Безпеки програм та даних» (ОК 16), «Операційних систем» (ОК 20), «Основ Web-безпеки» (ОК 22), «Комплексних систем захисту інформації» (ОК 24) та «Управління інформаційною та кібербезпекою» (ОК 30).

ПОСТРЕКВІЗИТИ. Практичні навички тестування на проникнення та виявлення вразливостей завершують фахову підготовку й є безпосередньою базою для проходження переддипломної практики (ОК 35) і підготовки та захисту кваліфікаційної роботи (ОК 36).

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.

3. ОБСЯГ ТА ОЗНАКИ КУРСУ

Загалом		**Вид заняття** (денне відділення / заочне відділення)				**Ознаки курсу**		
ЄКТС	**годин**	**Лекційні заняття**	**Лабораторні заняття**	**Практичні заняття**	**Самостійна робота**	**Курс, (рік навчання)**	**Семестр**	**Обов’язкова / вибіркова**
6	180	26/6	20/4	20/4	114/166	4	8	Обов’язкова

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, ремедіація 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. ТЕХНІЧНЕ Й ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ / ОБЛАДНАННЯ

Студенти отримують теми та питання курсу, методичні рекомендації, перелік основної й додаткової літератури, індивідуальні та практичні завдання, а також результати оцінювання як традиційним шляхом, так і з використанням університетської платформи дистанційного навчання на базі Moodle.

Для формування практичних компетентностей з етичного хакінгу та тестування на проникнення використовується спеціалізоване лабораторне середовище, розгорнуте у віртуалізованій інфраструктурі. Практичні заняття проводяться із застосуванням операційних систем для тестування безпеки (наприклад, Kali Linux), інструментів сканування, аналізу вразливостей та експлуатації, а також навчального веб-додатку Damn Vulnerable Web Application (DVWA) для відпрацювання атак на різних рівнях складності.

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 в рамках лабораторних робіт.
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	25
7	**Тема 7. Звітність, ремедіація 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	26
	Всього	**114**	**166**

7. ВИДИ ТА МЕТОДИ КОНТРОЛЮ

Види контролю	**Складові оцінювання**	
	Для екзамену	**Для заліку**
поточний контроль, який здійснюється у ході: проведення практичних та лабораторних занять, виконання самостійної роботи, індивідуальних завдань, дослідна робота здобувача тощо.	**50%**	**100%**
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

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, підготовка реферату (есе) 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:

[1] Індивідуально-консультативна робота викладача зі здобувачами

- 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 балів за пдготовку 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 ІСПИТ
(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 при формі контролю **залік** (максимум 100 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 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.

КРИТЕРІЇ ЗАГАЛЬНИХ РЕЗУЛЬТАТІВ ОЦІНЮВАННЯ ЗНАНЬ ЗДОБУВАЧІВ
(для екзамену / заліку)

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. ДОТРИМАННЯ ВИМОГ АКАДЕМІЧНОЇ ДОБРОЧЕСНОСТІ

Викладання та засвоєння навчальної дисципліни передбачає неухильне дотримання вимог академічної доброчесності, яка регулюється Законом України "Про освіту" (Відомості Верховної Ради (ВВР), 2014, № 37-38, ст.2004), «Методичними рекомендаціями для закладів вищої освіти з підтримки принципів академічної доброчесності» (Лист МОН № 1/9-650 від 23.10.18 року), іншими нормативними документами. Зокрема, основні засади дотримання академічної доброчесності визначено у «Положенні про академічну доброчесність у Міжнародному гуманітарному університеті», «Кодексі академічної доброчесності Міжнародного гуманітарного університету» та «Інструкції щодо процедури технічної перевірки на наявність текстових запозичень (академічного плагіату)», затвердженої наказом МГУ від 03.05.2024 р., № 708а.

Відповідно до ст.42 Закону України "Про освіту" академічна доброчесність - це сукупність етичних принципів та визначених законом правил, якими мають керуватися учасники освітнього процесу під час навчання, викладання та провадження наукової (творчої) діяльності з метою забезпечення довіри до результатів навчання та/або наукових (творчих) досягнень.

Дотримання академічної доброчесності передбачає:

- самостійне виконання навчальних завдань, завдань поточного та підсумкового контролю результатів навчання (для осіб з особливими освітніми потребами ця вимога застосовується з урахуванням їхніх індивідуальних потреб і можливостей);
- посилання на джерела інформації у разі використання ідей, розробок, тверджень, відомостей;
- дотримання норм законодавства про авторське право і суміжні права;
- надання достовірної інформації про результати власної навчальної (наукової, творчої) діяльності, використані методики досліджень і джерела інформації.

11. 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