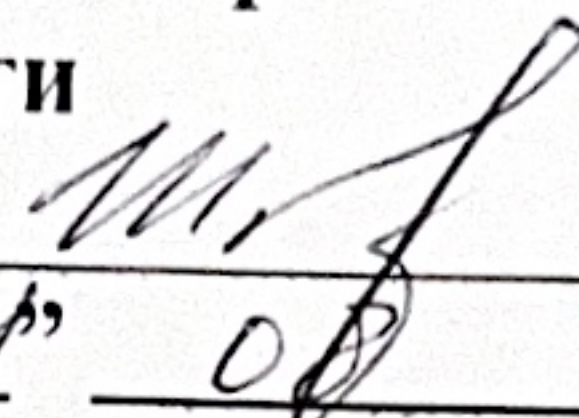


ЗАКЛАД ВИЩОЇ ОСВІТИ
«УНІВЕРСИТЕТ КОРОЛЯ ДАНИЛА»
Факультет суспільних і прикладних наук
Кафедра інформаційних технологій

ЗАТВЕРДЖУЮ

Проректор з навчально-методичної
роботи

 Ярослав ШТАНЬКО
“31” 08 2026 р.

Learn Ethical Hacking from Scratch

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Галузь знань:	12 Інформаційні технології
Спеціальність	121 Інженерія програмного забезпечення
Освітньо-професійна (освітньо-наукова) програма	Розробка та тестування програмного забезпечення
Освітній рівень:	перший (бакалаврський)
Статус дисципліни:	вибіркова
Мова викладання, навчання та оцінювання:	українська та англійська
Семестр викладання	VII

Івано-Франківськ

2026

РОЗРОБНИК:

викладач кафедри



Павло ЗАГОРОДЬКО

ЗАТВЕРДЖЕНО:

на засіданні кафедри інформаційних технологій, протокол № 1 від 27.08.2026 р.

PhD, завідувач кафедри

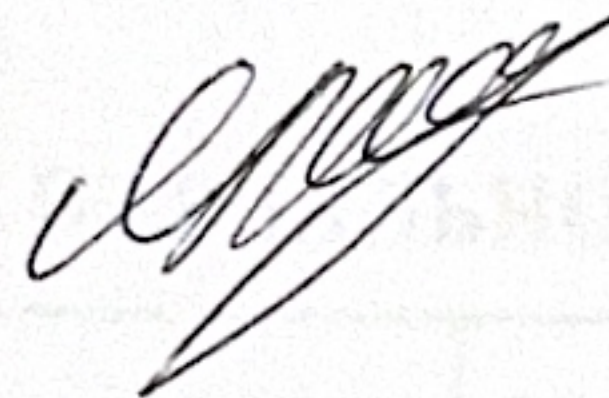


Олександр ІВАНОВ

УЗГОДЖЕНО:

Гарант ОП

к. ф-м.н., доцент кафедри



Володимир МАКОВИШИН

СХВАЛЕНО:

на засіданні Науково-методичної ради, протокол № 1 від 31 серпня 2026 року

e-mail	pavlo.zagorodko@ukd.edu.ua
Номер аудиторії чи кафедри	Кафедра інформаційних технологій
Посилання на сайт УКД	https://ukd.edu.ua
Сторінка курсу в СДО	

ВСТУП

Анотація навчальної дисципліни

Навчальна дисципліна “Learn Ethical Hacking from Scratch” навчає знаходити вразливості вебзастосунків з позиції атакувальника, щоб уміти їх закривати з позиції розробника. Впродовж курсу ви навчитеся перехоплювати й змінювати HTTP-трафік у Burp Suite, самостійно експлуатувати основні класи веб-вразливостей та пояснювати, який дефект коду чи архітектури стоїть за кожним із них. Усі практичні завдання виконуються на навмисно вразливих навчальних застосунках PortSwigger Web Security Academy, атакувати які дозволено.

Під кінець курсу студенти вмітимуть провести розвідку вебзастосунку, виявити й підтвердити SQL-ін'єкцію, XSS, CSRF, порушений контроль доступу, дефекти автентифікації, помилки бізнес-логіки, розкриття інформації, небезпечне завантаження файлів та ін'єкцію промπτу в LLM-інтеграціях, а також запропонувати коректний захист для кожного випадку. Окремо розглядаються соціальна інженерія, кримінальна відповідальність за несанкціонований доступ за законодавством України та правила безпечної практики — межі дозволеного, письмовий дозвіл і rules of engagement.

Метою навчальної дисципліни є набуття компетентностей з виявлення, експлуатації та усунення вразливостей вебзастосунків у межах правового поля.

Завданнями курсу встановлено:

- Оволодіння поняттями етичного хакінгу, моделі загроз та меж дозволеного, а також інструментарієм перехоплення й модифікації HTTP-трафіку на базі Burp Suite.

- Опанування основних класів вебвразливостей за OWASP Top 10: ін'єкції, міжсайтовий скриптинг, підробка міжсайтових запитів, порушений контроль доступу, дефекти автентифікації, розкриття інформації.
- Опанування дефектів бізнес-логіки, небезпечного завантаження файлів та атак на вебзастосунки з інтегрованими великими мовними моделями.
- Набуття навичок обґрунтування та документування захисних заходів, а також розуміння юридичних ризиків і вимог ринку праці у сфері кібербезпеки.

Компетентності та результати навчання, яких набувають здобувачі освіти внаслідок вивчення навчальної дисципліни (шифри та зміст компетентностей та програмних результатів навчання вказані відповідно до ОПП «Розробка та тестування програмного забезпечення», введеної в дію ЗВО «Університет Короля Данила» 29 травня 2026 року, наказом № 33/од).

Шифр та назва компетентності	Шифр та назва програмних результатів навчання
ЗК 2. Здатність застосовувати знання у практичних ситуаціях. ЗК 8. Здатність діяти на основі етичних міркувань.	ПРН 2. Знати кодекс професійної етики, розуміти соціальну значимість та культурні аспекти інженерії програмного забезпечення і дотримуватись їх в професійній діяльності. ПРН 14. Застосовувати на практиці
СК 6. Здатність аналізувати, вибирати і застосовувати методи і засоби для забезпечення	

інформаційної безпеки (в тому числі кібербезпеки). СК 13. Здатність обґрунтовано обирати та освоювати інструментарій з розробки та супроводження програмного забезпечення.	інструментальні програмні засоби доменного аналізу, проектування, тестування, візуалізації, вимірювань та документування програмного забезпечення. ПРН 21. Знати, аналізувати, вибирати, кваліфіковано застосовувати засоби забезпечення інформаційної безпеки (в тому числі кібербезпеки) і цілісності даних відповідно до розв’язуваних прикладних завдань та створюваних програмних систем.
---	---

ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Курс	четвертий (4)			
Семестр	сьомий (7)			
Кількість кредитів ЄКТС	3			
		Всього:	денна форма	заочна форма
Аудиторні навчальні	лекції	24	20 (в годинах)	4 (в годинах)

заняття	практичні	26	22 (в годинах)	4 (в годинах)
Самостійна робота		130	48 (в годинах)	82 (в годинах)
Форма підсумкового контролю	Іспит			

ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Перелік тем лекційного матеріалу та практичних занять

Тема 1. Вступ до етичного хакінгу та платформа PortSwigger

Що таке етичний хакінг і чим він відрізняється від несанкціонованого доступу. Правила гри: письмовий дозвіл, межі тестування, відповідальне розкриття. Платформа PortSwigger Web Security Academy як навчальне середовище. Основи SQL-ін'єкції та оглядовий перелік класів атак, які розглядатиме курс.

Тема 2. Burp Suite та SQL-ін'єкції

Burp Suite як робочий інструмент: проксі, перехоплення та модифікація запитів, Repeater, Intruder, налаштування CA-сертифіката. SQL-ін'єкція поглиблено: обхід автентифікації, UNION-атаки, витяг даних з інших таблиць, сліпа ін'єкція за умовними відповідями та за часом затримки. Захист: параметризовані запити.

Тема 3. XSS та CSRF

Міжсайтовий скриптинг: три типи — відображений, збережений і на основі DOM. Контексти вставки та експлуатація: викрадення сесії,

перехоплення облікових даних. Захист від XSS: екранування за контекстом, Content Security Policy. Підробка міжсайтових запитів: умови можливості атаки, обхід перевірки токена, обхід обмежень SameSite і захисту на основі Referer, коректний захист.

Тема 4. Контроль доступу та автентифікація

Вертикальне й горизонтальне підвищення привілеїв, IDOR, обхід контролю доступу за URL, методом запиту та заголовком Referer; методика пошуку таких дефектів. Автентифікація: перелічення користувачів, атаки на вхід за паролем, обхід багатофакторної автентифікації, дефекти скидання пароля та отруєння посилання для скидання, вразливості механізму «запам'ятати мене» і сесії після входу.

Тема 5. Бізнес-логіка та розкриття інформації

Дефекти бізнес-логіки як наслідок хибних припущень: надмірна довіра до клієнтської частини й до вводу, припущення про послідовність дій користувача, неузгоджені засоби контролю, недостатня валідація робочого процесу. Розкриття інформації: повідомлення про помилки, сторінки налагодження, резервні файли, історія системи контролю версій; інструменти пошуку в Burp Suite.

Тема 6. Вразливості завантаження файлів

Веб-шелл і віддалене виконання коду як найгірший наслідок. Як сервер вирішує виконати файл: розширення, обробник, конфігурація. Обхід перевірок: підміна Content-Type, обхід чорного списку розширень, обфускація розширення, обхід через traversal шляху, поліглотні файли та стан гонитви. Захист: білий список, перейменування, зберігання поза кореневим каталогом.

Тема 7. Атаки на вебзастосунки з LLM

LLM-інтеграція як поверхня атаки; аналогія із SSRF. Картування поверхні атаки: які API та дані доступні моделі. Зловживання API через модель за надмірних повноважень. Непряма ін'єкція промпту через дані,

які модель читає. Небезпечне оброблення виводу моделі. Вразливості AI-сканерів. Захист: обмеження повноважень, ізоляція даних від інструкцій, перевірка виводу.

Тема 8. Соціальна інженерія, юридичні ризики та професія

Людина як поверхня атаки: психологічні важелі, життєвий цикл атаки, канали й техніки; фішинг з обходом багатofакторної автентифікації, clickjacking, вплив генеративного штучного інтелекту на переконливість атак і захист від них. Кримінальна відповідальність за статтями 361–362 Кримінального кодексу України та у інших юрисдикціях. Безпечна практика: письмовий дозвіл, rules of engagement, safe harbour. Професія, ринок праці України та Європи.

Зміст самостійної роботи здобувачів

Розподіл годин виділених на вивчення дисципліни:

Найменування видів робіт	Розподіл годин	
	денна форма	заочна форма
Самостійна робота, год. у т.ч.:	48	82
Опрацювання матеріалу, викладеного на лекціях	12	20
Підготовка до практичних занять та контрольних заходів	12	18
Підготовка звітів з практичних робіт	12	18

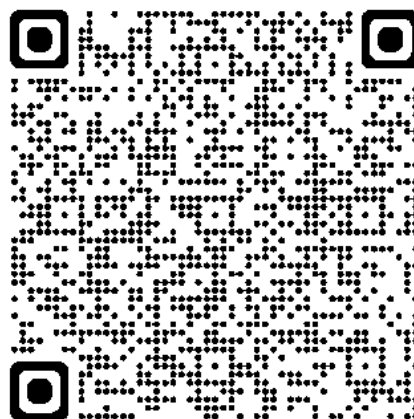
Підготовка до поточного контролю	4	6
Опрацювання матеріалу, винесеного на самостійне вивчення	8	20

ПОЛІТИКА КУРСУ

Коротко, з посиланням на відповідну нормативну базу УКД, висвітити питання:

1) щодо системи поточного і підсумкового контролю

Організація поточного та підсумкового семестрового контролю знань студентів, проведення практик та атестації, переведення показників академічної успішності за 100-бальною шкалою в систему оцінок за національною шкалою здійснюються згідно з “Положенням про систему поточного і підсумкового контролю, оцінювання знань та визначення рейтингу здобувачів освіти”. Ознайомитись з документом можна за [посиланням](#).



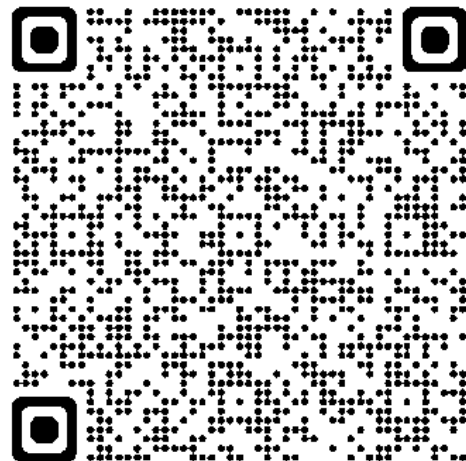
2) щодо оскарження результатів контрольних заходів

Здобувачі вищої освіти мають право на оскарження оцінки з дисципліни, отриманої під час контрольних заходів. Апеляція здійснюється відповідно до «Положення про політику та врегулювання конфліктних ситуацій». Ознайомитись з документом можна за [посиланням](#).



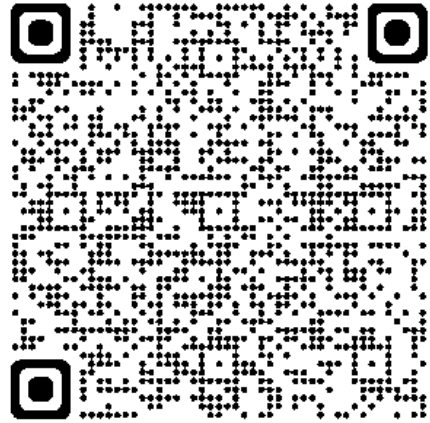
3) щодо відпрацювання пропущених занять

Згідно “Положення про організацію освітнього процесу” здобувач допускається до семестрового контролю з конкретної навчальної дисципліни (семестрового екзамену, диференційованого заліку), якщо він виконав усі види робіт, передбачені на семестр навчальним планом та силабусом/робочою програмою навчальної дисципліни, підтвердив опанування на мінімальному рівні результатів навчання (отримав ≥ 35 бали), відпрацював визначені індивідуальним навчальним планом всі лекційні, практичні, семінарські та лабораторні заняття, на яких він був відсутній. Ознайомитись з документом можна за [посиланням](#).



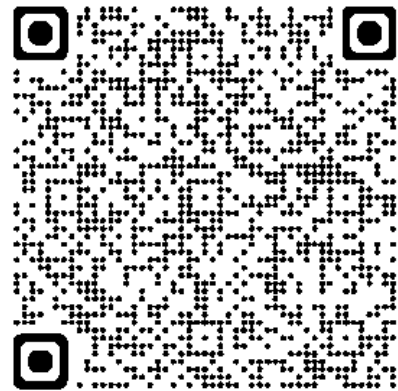
4) щодо дотримання академічної доброчесності

“Положення про академічну доброчесність” закріплює моральні принципи, норми та правила етичної поведінки, позитивного, сприятливого, доброчесного освітнього і наукового середовища, професійної діяльності та професійного спілкування спільноти Університету, викладання та провадження наукової (творчої) діяльності з метою забезпечення довіри до результатів навчання. Ознайомитись з документом можна за [посиланням](#).



5) щодо використання штучного інтелекту

“Положення про академічну доброчесність” визначає політику щодо використання технічних засобів на основі штучного інтелекту в освітньому процесі. Ознайомитись з документом можна за [посиланням](#). “Положення про систему запобігання та виявлення академічного плагіату, самоплагіату, фабрикації та фальсифікації академічних творів” містить рекомендації щодо використання в академічних текстах генераторів на основі штучного інтелекту. Ознайомитись з документом можна за [посиланням](#).



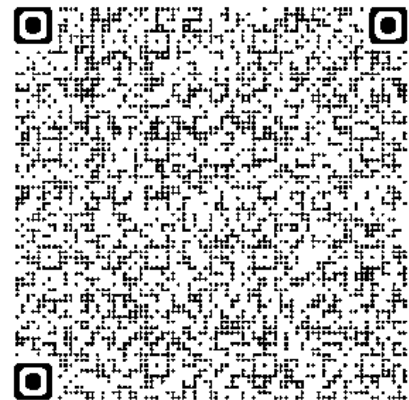
6) щодо використання технічних засобів в аудиторії та правила комунікації

Використання мобільних телефонів, планшетів та інших гаджетів під час лекційних та практичних занять дозволяється виключно у навчальних цілях (для уточнення певних даних, перевірки правопису, отримання довідкової інформації тощо). На гаджетах повинен бути активований режим «без звуку» до початку заняття. Під час занять заборонено надсилання текстових повідомлень, прослуховування музики, перевірка електронної пошти, соціальних мереж тощо. Під час виконання заходів контролю використання гаджетів заборонено (за винятком, коли це передбачено умовами його проведення). У разі порушення цієї заборони результат анулюється без права перескладання.

Комунікація відбувається через електронну пошту і сторінку дисципліни в Moodle.

7) щодо зарахування результатів навчання, здобутих шляхом формальної/інформальної освіти

Процедури визнання результатів навчання, здобутих шляхом формальної/інформальної освіти, визначаються «Положенням про порядок визнання результатів навчання, здобутих шляхом неформальної та/або інформальної освіти». Ознайомитись з документом можна за [ПОСИЛАННЯМ](#).



МЕТОДИ НАВЧАННЯ

При вивченні дисципліни застосовується комплекс методів для організації навчання студентів з метою розвитку їх логічного та

абстрактного мислення, творчих здібностей, підвищення мотивації до навчання та формування особистості майбутнього фахівця.

Програмний результат навчання	<u>Метод навчання</u>	<u>Метод оцінювання</u>
ПРН 2. Знати кодекс професійної етики, розуміти соціальну значимість та культурні аспекти інженерії програмного забезпечення і дотримуватись їх в професійній діяльності.	Словесні методи: лекція, бесіда. Наочні методи: ілюстрування, комп'ютерні і мультимедійні методи. Практичні методи: вправи, практичні роботи. Творчий метод, методи самостійної роботи вдома, робота під керівництвом викладача. Інтерактивний метод: кейс-метод.	МФО 4 - поточний контроль, МФО 5 - усний контроль, МФО 6 - письмовий контроль, МФО 8 - тестовий контроль.
ПРН 14. Застосовувати на практиці інструментальні програмні засоби доменного аналізу, проектування, тестування, візуалізації, вимірювань та документування програмного забезпечення.	Словесні методи: лекція. Наочні методи: ілюстрування, комп'ютерні і мультимедійні методи. Практичні методи: практичні роботи. Творчий метод, робота під керівництвом викладача. Інтерактивний метод: мозковий штурм.	МФО 4 - поточний контроль, МФО 5 - усний контроль, МФО 6 - письмовий контроль, МФО 8 - тестовий контроль.
ПРН 21. Знати, аналізувати, вибирати, кваліфіковано застосовувати засоби забезпечення інформаційної безпеки (в тому числі	Словесні методи: лекція. Наочні методи: ілюстрування, комп'ютерні і мультимедійні методи. Практичні методи: вправи, практичні	МФО 4 - поточний контроль, МФО 5 - усний контроль, МФО 6 - письмовий контроль, МФО 8 - тестовий контроль.

кібербезпеки) і цілісності даних відповідно до розв’язуваних прикладних завдань та створюваних програмних систем.	роботи. Творчий метод, методи самостійної роботи вдома, робота під керівництвом викладача.	
---	--	--

ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ

Контрольні заходи

Вид	Зміст	% від загальної оцінки	Бал	
			min	max
Поточні контрольні заходи	всього	50	35	50
Підсумкові контрольні заходи	письмові роботи	50	25	50
Всього:		100	60	100

Процедура проведення контрольних заходів, а саме поточного контролю знань протягом семестру та підсумкового семестрового контролю, регулюється «Положенням про систему поточного та підсумкового контролю оцінювання знань та визначення рейтингу студентів».

Фіксація поточного контролю здійснюється в “Електронному журналі обліку успішності академічної групи” на підставі чотирибальної шкали - “2”; “3”; “4”; “5”. У разі відсутності студента на занятті виставляється “н”. За результатами поточного контролю у Журналі,

автоматично визначається підсумкова оцінка, здійснюється підрахунок пропущених занять.

Усі пропущені заняття, а також негативні оцінки студенти зобов'язані відпрацювати впродовж трьох наступних тижнів. У випадку недотримання цієї норми, замість “н” в журналі буде виставлено “0” (нуль балів), без права перездачі. Відпрацьоване лекційне заняття в електронному журналі позначається літерою «в».

Критерії оцінювання (за необхідності, поточного та/або підсумкового контролю)

“незадовільно”	володіє навчальним матеріалом на рівні елементарного розпізнавання і відтворення окремих фактів, елементів, об’єктів, що позначаються окремими словами чи реченнями; володіє матеріалом на елементарному рівні засвоєння, викладає його уривчастими реченнями, виявляє здатність висловити думку на елементарному рівні; володіє матеріалом на рівні окремих фрагментів, що становлять незначну частину навчального матеріалу;
“задовільно”	володіє матеріалом на початковому рівні, значну частину матеріалу відтворює на репродуктивному рівні; володіє матеріалом на рівні, вищому за початковий, здатний за допомогою викладача логічно відтворити значну його частину; може відтворити значну частину теоретичного матеріалу, виявляє знання і розуміння основних положень, за допомогою викладача може аналізувати навчальний матеріал, порівнювати та робити висновки, виправляти допущені помилки;
“добре”	здатний застосовувати вивчений матеріал на рівні стандартних ситуацій, частково контролювати власні навчальні дії, наводити окремі власні приклади на підтвердження певних тверджень: вміє порівнювати, узагальнювати, систематизувати інформацію під керівництвом викладача, в цілому

	самостійно застосовувати її на практиці, контролювати власну діяльність, виправляти помилки і добирати аргументи на підтвердження певних думок під керівництвом викладача; вільно володіє вивченим обсягом матеріалу, та вміє застосовувати його на практиці; вільно розв'язує задачі в стандартних ситуаціях, самостійно виправляє допущені помилки, добирає переконливі аргументи на підтвердження вивченого матеріалу;
“відмінно”	виявляє початкові творчі здібності, самостійно визначає окремі цілі власної навчальної діяльності, оцінює окремі нові факти, явища, ідеї; знаходить джерела інформації та самостійно використовує їх відповідно до цілей, поставлених викладачем; вільно висловлює власні думки і відчуття, визначає програму особистої пізнавальної діяльності, самостійно оцінює різноманітні життєві явища і факти, виявляючи особисту позицію щодо них; без допомоги викладача знаходить джерела інформації і використовує одержані відомості відповідно до мети та завдань власної пізнавальної діяльності; використовує набуті знання і вміння в нестандартних ситуаціях; виявляє особливі творчі здібності, самостійно розвиває власні обдарування і нахили, вміє самостійно здобувати знання.

До підсумкового контролю допускаються студенти, які за результатами поточного контролю отримали не менше 35 балів. Усі студенти, що отримали 34 бали і менше, не допускаються до складання підсумкового контролю і на підставі укладення додаткового договору, здійснюють повторне вивчення дисципліни впродовж наступного навчального семестру. За результатами підсумкового контролю (диференційований залік/екзамен) студент може отримати 40 балів. Студенти, які під час підсумкового контролю отримали 24 бали і менше, вважаються такими, що не здали екзамен/диференційований залік і повинні йти на перездачу.

Загальна семестрова оцінка з дисципліни, яка виставляється в екзаменаційних відомостях, оцінюється в балах (згідно з **Шкалою оцінювання знань за ECTS**) і є сумою балів, отриманих під час поточного та підсумкового контролю. Підсумковий контроль проводиться у вигляді письмових робіт.

Шкала оцінювання знань за ECTS

Оцінка за національною шкалою	Рівень досягнень, %	Шкала ECTS
Національна диференційована шкала		
Відмінно	90-100	A
Добре	83-89	B
	75-82	C
Задовільно	67-74	D
	60-66	E
Незадовільно	35-59	FX
	0-34	F
Національна недиференційована шкала		
Зараховано	60-100	-
Не зараховано	0-59	-

Студенти, які не з'явилися на заліки/екзамени без поважних причин, вважаються такими, що одержали незадовільну оцінку.

РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

Основна література

1. Stuttard, D., & Pinto, M. (2011). *The web application hacker's handbook: Finding and exploiting security flaws* (2nd ed.). Wiley.
2. Li, V. (2021). *Bug bounty bootcamp: The guide to finding and reporting web vulnerabilities*. No Starch Press.
3. Yaworski, P. (2019). *Real-world bug hunting: A field guide to web hacking*. No Starch Press.

Електронні інформаційні ресурси

1. PortSwigger. (n.d.). *Web Security Academy*. Retrieved from <https://portswigger.net/web-security>
2. PortSwigger. (n.d.). *Burp Suite documentation*. Retrieved from <https://portswigger.net/burp/documentation>
3. OWASP. (2025). *OWASP Top 10:2025*. Retrieved from <https://owasp.org/Top10/2025/>
4. Кримінальний кодекс України, № 2341-III. (2001). Retrieved from <https://zakon.rada.gov.ua/laws/show/2341-14>