ЗАТВЕРДЖЕНО

Вченою радою факультету інформаційно-комп'ютерних технологій

28 серпня 2024 р., протокол №8

Голова Вченої ради

_____ Тетяна НІКІТЧУК

РОБОЧА ПРОГРАМА
вибіркової навчальної дисципліни фахової підготовки
«Безпека web-додатків»

факультет інформаційно-комп'ютерних технологій

для здобувачів вищої освіти освітнього ступеня «бакалавр»

Схвалено на засіданні кафедри комп'ютерної інженерії та кібербезпеки
26 серпня 2024 р., протокол №6

Завідувач кафедри

_____ Андрій ЄФІМЕНКО

Розробник: к.т.н., доцент кафедри комп'ютерної інженерії та кібербезпеки
Олександр ПІРОГ

Житомир
2024 – 2025 н.р.

Робоча програма навчальної дисципліни «Безпека web-додатків» для здобувачів вищої освіти освітнього ступеня «бакалавр» спеціальності 125 «Кібербезпека та захист інформації» освітньо-професійна програма «Кібербезпека» затверджена Вченою радою факультету інформаційно-комп'ютерних технологій від 28 серпня 2024 р., протокол № 8.

1. Опис навчальної дисципліни

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, напрям підготовки, освітній ступінь</td><td colspan="2">Характеристика навчальної дисципліни</td></tr>
<tr><td>денна форма навчання</td><td>заочна форма навчання</td></tr>
<tr><td>Кількість кредитів 4</td><td>Галузь знань
12 «Інформаційні технології»</td><td colspan="2">за вибором</td></tr>
<tr><td>Модулів – 1</td><td rowspan="5">Спеціальність
125 «Кібербезпека та захист інформації»</td><td colspan="2">Рік підготовки:</td></tr>
<tr><td rowspan="2">Змістових модулів – 1</td><td>3</td><td>–</td></tr>
<tr><td colspan="2">Семестр</td></tr>
<tr><td rowspan="2">Загальна кількість годин - 120</td><td>1</td><td>–</td></tr>
<tr><td colspan="2">Лекції</td></tr>
<tr><td rowspan="10">Тижневих годин для денної форми навчання:
аудиторних 4
самостійної роботи – 3,5</td><td rowspan="10">Освітній ступінь «бакалавр»</td><td>32 год.</td><td>–</td></tr>
<tr><td colspan="2">Практичні</td></tr>
<tr><td>–</td><td>–</td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td>32 год.</td><td>–</td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td>56 год.</td><td>–</td></tr>
<tr><td colspan="2"></td></tr>
<tr><td colspan="2">Вид контролю: залік</td></tr>
</table>

Співвідношення кількості годин аудиторних занять до самостійної та індивідуальної роботи становить:
для денної форми навчання – 53 % аудиторних занять, 47 % самостійної та індивідуальної роботи.

2. Мета та завдання навчальної дисципліни

Метою вивчення навчальної дисципліни є формування у студентів знань, умінь, необхідних для вирішення задач захисту web-систем.
Завданнями навчальної дисципліни є формування теоретичних знань та практичних умінь у сфері забезпечення безпеки web-ресурсів, в тому числі:
– знати основні вразливості web-систем;
– вміти аналізувати, виявляти та оцінювати можливі загрози, вразливості web-систем;
– вміти розробляти політики безпеки web-систем;
– вміти забезпечувати захист програм, баз даних та інформації, що обробляється у web-системах;
– вміти забезпечувати безперервну працездатність web-систем;
– вміти вирішувати задачі забезпечення та супроводу, в тому числі: огляд, тестування web-систем на вразливості;
– вміти управляти процедурами ідентифікації, аутентифікації, авторизації користувачів у web-системах;
– вміти реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформації у web-системах.
Під час вивчення навчальної дисципліни здобувачі вищої освіти зможуть отримати наступні Soft skills:
- *комунікативні навички*: письмове, вербальне й невербальне спілкування; уміння грамотно спілкуватися в електронному листуванні; вести дискусію і відстоювати свою позицію;
- *керування часом:* уміння справлятися із завданнями вчасно;
- *гнучкість і адаптивність:* гнучкість, адаптивність і здатність змінюватися; уміння аналізувати ситуацію, орієнтування на вирішення проблеми;
- *лідерські якості*: уміння спокійно працювати в напруженому середовищі; уміння ухвалювати рішення; уміння ставити мету, планувати діяльність;
- *особисті якості:* креативне й критичне мислення; етичність, чесність, терпіння, повага до оточуючих.

3. Програма навчальної дисципліни

Тема 1. Вступ до безпеки web-систем.
Клієнт-серверна архітектура. Модель OSI. Протоколи та порти. Структура URL. HTTP протокол, запити та відповіді сервера. HTML. JavaScript. Методи кодування, шифрування, хешування. Вимоги до безпеки в контексті вимог до додатків. OWASP Top Ten. Схема атаки. Методи злому. Структура фішингової атаки. Ознаки фішингової атаки. Методи боротьби. Поняття web-додатку, web-системи. Види веб-додатків. Основні вразливості. Поняття web-безпеки.

Стандартизація вхідного контенту. Модель безпеки браузерів – політика однакового походження (same-origin policy). HTTP заголовки безпеки. Що необхідно знати пентестеру, дерево скілів.

Тема 2. Контроль доступу.

Ідентифікація, аутентифікація, контроль доступу. Паролі. Хеш-шифрування. Метод перебору (brute-force атаки). Rainbow tables. Інструменти злому паролів: John the Ripper, Hydra, Medusa. «Соління» паролів (salt). Протокол «виклик/відповідь» (challenge/response protocol). Обмеження числа спроб вгадування пароля (antihammer). Перебір за словником (dictionary attack). Методи кодування та шифрування. Оцінка ефективності схем аутентифікації. Біометрична аутентифікація. Багатофакторна аутентифікація (MFA). Управління сесіями (Sniffing, Hijack). Токени, JSON, JWT, JWK. Контроль доступу. Незахищені прямі посилання на об’єкти (IDOR). Необмежене завантаження файлів (Unrestricted File Upload). Адміністрування прав доступу в web-системах. Відповіді сервера. Адміністрування Apache та MySQL. Права програм на сервері та їх обмеження. Права доступу. Розмежування прав, ролі користувачів.

Тема 3. Вразливості web-додатків.

Нульовий байт, символи рівня директорій. Web-форми. Методи GET/POST. Обробка вхідних даних. Міжсайтовий скріптинг (XSS). Контексти XSS атак. Запобігання XSS. Підробка міжсайтових запитів (CSRF). Класифікація CSRF. Захист від CSRF. SQL ін'єкції (SQL injection). Паттерни SQL ін'єкцій. UNION SQL ін'єкції. Сліпі SQL ін'єкції. Інформаційна схема БД. Ін’єкції NoSQL. Запобігання атакам SQL. Введення зовнішньої сутності XML (XXE). Запобігання атакам XXE. Введення команд ОС (OS command injection). Сліпе введення команди ОС. Запобігання атакам введення команд ОС. Небезпечна десеріалізація (Insecure Deserialization). Запобігання атакам небезпечної десеріалізації. Підробка запитів на стороні сервера (SSRF). Запобігання атакам SSRF.

Тема 4. DoS-атаки.

DoS/DDoS атаки. Ботнет. ICMP-флуд прямий (Ping) і обернений (Smurf). Переповнення буферу. Teardrop. UDP-флуд. HTTP-флуд. Атака посилення (Amplification Attack). DNS-флуд. SYN-флуд. Атака додатку. Slowloris. ReDoS. Посилення NTP. Атаки нульового дня. Серверні та клієнтські вразливості. Захист від DoS вразливостей.

Тема 5. Розкриття інформації.

Класифікація даних. Витоки даних. Класи вразливостей web-сервера. Розкриття інформації в web-системах. Відбитки пальців web-сервера / програми (Web Server/Application Fingerprinting). Індексація каталогів (Directory Indexing). Витік інформації (Information Leakage). Розкриття чутливої інформації (Sensitive Data Exposure). Обхід шляху (Path Traversal). Витік повного шляху (Full path disclosure). Розкриття структури БД (SQL DB Structure Extraction). Передбачуване місцезнаходження ресурсу (Predictable Resource Location). Захист від Full path

disclosure вразливостей. Методологія хакінгу. Розвідка інфраструктури web-вузлу, web-додатку, ПЕОМ адміністраторів та користувачів. Тестування компонентів системи. Методи протидії розкриттю інформації.

Тема 6. Тестування web-додатків.

Принципи, склад та види тестування безпеки ПЗ. Вимоги до безпеки. Тестова документація. Тестування на проникнення (Pentesting). Види тестів на проникнення. Фази тестування. Визначення області тестування (Scope). Технічне завдання. Угода про нерозголошення (NDA). Збір інформації: пасивний/активний. Whois, Shodan, TheHarvester, Google dorking, Gophish. Типи сканування. Типи, причини, тактики підвищення привілеїв (Privilege Escalation). Nikto, Greenbone, Nmap, FFuF, Wfuzz, Burp Suite, OWASP ZAP, Hydra, WPScan, Sqlmap, Online Hash Crack, Responder, John the Ripper, Wireshark. Приманка (Honeypot). Metasploit: інтерфейси, модулі, Meterpreter. Зворотна оболонка (reverse shell). Netcat. Прибирання. Докази. Видалення. Звіт про тестування.

Тема 7. Безпечне програмування.

Безпека протягом усього процесу розробки. Вимоги. Фази, шаблони атак. Проблеми якості ПЗ. Превентивний захист. Вразливості конфігурації, інфраструктури, людський фактор. Атаки соціальної інженерії. Інтерфейс користувача. Сприяння безпечній поведінці. Обмеження користувацького вводу. Політика аутентифікації. Життєвий цикл розробки ПЗ (SDLC). Вбудована система безпеки на всіх етапах. Стандарти та моделі безпечного SDLC. Безпека процесу розробки. Принципи проектування безпеки. Захист середовища розробки. Безпека через невідомість (Security by Obscurity). Підхід Security by Design. Принципи проектування безпеки OWASP. Шаблони безпеки. Модульний дизайн. Рекомендації щодо уникнення поширених помилок при проектуванні. Визначення ризику. Моделювання загроз. Інструменти та методики моделювання: PASTA, DREAD. Стратегії реагування. Контрзаходи STRIDE. Поширені помилки програмування. Переповнення буфера. Умови перегонів. Рекомендації щодо запобігання вразливостям (Web, Mobile, IoT). Контроль сесії. Керування паролями. Відновлення пароля. Типи тестів протягом SDLC. Статичний, динамічний аналіз коду. PyLint, OWASP ZAP. Моніторинг ПЗ. Технічне обслуговування ПЗ.

Тема 8. Економіка web-безпеки.

Причини комп'ютерних злочинів. Результативність (effectiveness). Ефективність (efficiency). Збитковість економічних комп'ютерних злочинів. Собівартість комп'ютерних злочинів. Методи підвищення собівартості комп'ютерних злочинів. Спам (spam), дорвеї (doorway), ринок посилань, накруток (заходи, постінг, підписки, перегляди, лайкі), сателіти (satellite), DoS-атаки. Принципи інвестування у web-безпеку.

4. Структура (тематичний план) навчальної дисципліни

Змістові модулі і теми	Кількість годин			
	денна форма			
	усього	лекції	лабораторні	самостійна робота
Тема 1. Вступ до безпеки web-систем.	11	4		7
Тема 2. Контроль доступу.	25	4	14	7
Тема 3. Вразливості web-додатків.	25	4	14	7
Тема 4. DoS-атаки.	9	2		7
Тема 5. Розкриття інформації.	13	2	4	7
Тема 6. Тестування web-додатків.	11	4		7
Тема 7. Безпечне програмування.	15	8		7
Тема 8. Економіка web-безпеки.	11	4		7
ВСЬОГО	120	32	32	56

5. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин	
		денна форма	заочна форма
1	Вступне заняття.	4	–
2	Вразливості контролю доступу. Міжсайтові сценарії (XSS). Підробка міжсайтових запитів (CSRF)	4	–
3	Аутентифікація. Авторизація.	4	–
4	Адміністрування сервера Apache та баз даних MySQL.	4	–
5	Права доступу в web-системах.	4	–
6	SQL-ін’єкції. Введення зовнішньої сутності XML (XXE)/ Введення команд ОС.	4	–
7	Вразливості бізнес-логіки. Обхід каталогу. Розкриття інформації.	4	–
8	Підсумкове заняття.	4	–
РАЗОМ		32	–

6. Завдання для самостійної роботи

№ з/п	Назва теми	Кількість годин	
		денна форма	заочна форма
1	**Тема 1. Вступ до безпеки web-систем.** 1. Document Object Model. 2. HTML, JavaScript. 3. WebSockets. 4. SQL. 5. Методи кодування, шифрування, хешування. 6. HTTP заголовки безпеки.	7	-
2	**Тема 2. Контроль доступу.** 1. Інструменти злому паролів (John the Ripper, Hydra, Medusa). 2. JSON, JWT, JWK. 3. Адміністрування MySQL.	7	-
3	**Тема 3. Вразливості web-додатків.** 1. Вразливості бізнес-логіки. 2. Контрабанда запитів HTTP. 3. Вразливості на основі DOM. 4. Введення шаблону на стороні сервера. 5. Отруєння web-кешем.	7	-
4	**Тема 4. DoS-атаки.** 1. ReDoS та регулярні вирази. 2. Переповнення буферу.	7	-
5	**Тема 5. Розкриття інформації.** 1. Обхід шляху (Path Traversal). 2. Індексація каталогів (Directory Indexing).	7	-
6	**Тема 6. Тестування web-додатків.** 1. Whois, Shodan, TheHarvester, Google dorking. 2. Nmap, Nikto, Greenbone, FFuF, ZAP, Hydra, WPScan, Sqlmap.	7	-
7	**Тема 7. Безпечне програмування.** 1. PASTA. 2. DREAD 3. STRIDE	7	-
8	**Тема 8. Економіка web-безпеки.** 1. Спам (spam), дорвеї (doorway), сателіти (satellite).	7	-
	РАЗОМ	**56**	**-**

7. Індивідуальні самостійні завдання

(не передбачені навчальним планом)

8. Методи навчання

Під час викладання навчальної дисципліни використовуються наступні методи навчання:
– Вербальні методи (лекція, пояснення);
– Наочні методи (спостереження, демонстрація, ілюстрація);
– Практичні методи (проведення дослідів, експериментів);
– Дискусійний метод;
– Методи самостійної роботи (опрацьованого матеріалу, підготовка звітів).

9. Методи контролю

Перевірка досягнення результатів навчання здійснюється з використанням наступних методів:

- Перевірка виконання та захист лабораторних робіт;
- Тестування;
- Залік.

10. Оцінювання результатів навчання здобувачів вищої освіти

Оцінювання результатів навчання здобувачів вищої освіти з навчальної дисципліни здійснюється відповідно до Положення про оцінювання результатів навчання здобувачів вищої освіти у Державному університеті «Житомирська політехніка» та розподілу балів, що наведений нижче.
Система оцінювання результатів навчання здобувачів вищої освіти з навчальної дисципліни включає поточний та підсумковий контроль.
Поточний контроль проводиться для оцінювання рівня засвоєння знань, формування умінь і навичок здобувачів вищої освіти впродовж вивчення ними матеріалу навчальної дисципліни. Поточний контроль здійснюється під час проведення навчальних занять.
Підсумковий контроль проводиться для підсумкового оцінювання результатів навчання здобувачів вищої освіти з навчальної дисципліни. Підсумковий контроль здійснюється після завершення вивчення навчальної дисципліни. Підсумковий контроль проводиться у формі заліку. Процедура складання заліку

визначена у Положенні про організацію освітнього процесу у Державному університеті «Житомирська політехніка».

Розподіл балів з навчальної дисципліни

Види робіт здобувача вищої освіти	Кількість балів за семестр	
	денна форма	заочна форма
Виконання завдань поточного контролю	100	–
Підсумкова семестрова оцінка	**100**	**–**

Розподіл балів за виконання завдань поточного контролю

Види робіт здобувача вищої освіти	Кількість балів за семестр	
	денна форма	заочна форма
Виконання завдань під час навчальних занять	100	–
Виконання науково-дослідної роботи та інших видів робіт (**додаткові – заохочувальні бали**)[3]: 1. Виступ на засіданні гуртку «Application security» 2. Участь в CTF.	 до 10 до 10	–
Разом за виконання завдань поточного контролю	**100**	**–**

Розподіл балів за виконання завдань під час навчальних занять

Види робіт здобувача вищої освіти[1]	Кількість балів за семестр	
	денна форма	заочна форма
Виконання та захист лабораторних робіт	50	–
Виконання поточних тестових завдань	50	–
Разом за виконання завдань під час навчальних занять	**100**	**–**

З метою застосування цілих чисел для оцінювання активностей здобувачів вищої освіти під час навчальних занять протягом семестру використовується 100-бальна шкала оцінювання кожного окремо виду робіт. Розрахунок набраних здобувачем вищої освіти балів за виконання завдань під час навчальних занять за семестр проводиться за формулою:

$$Р_{НЗ} = Р_{ЛР100} \times ВК_{ЛР} + Р_{ТЗ100} \times ВК_{ТЗ}, \quad (1)$$

де $Р_{НЗ}$ – кількість набраних здобувачем вищої освіти балів за виконання завдань під час навчальних занять за семестр;

$Р_{ЛР100}$ – середнє арифметичне значення набраних здобувачем вищої освіти балів за виконання та захист лабораторних робіт (кожна окремо лабораторна робота оцінюється за 100-бальною шкалою);

$Р_{ТЗ100}$, – кількість набраних здобувачем вищої освіти балів за виконання поточних тестових завдань (оцінюється за 100-бальною шкалою);

$ВК_{ЛР}$, $ВК_{ТЗ}$ – вагові коефіцієнти відповідно за виконання та захист лабораторних робіт, за виконання поточних тестових завдань. Значення вагових коефіцієнтів становить:

$ВК_{ЛР} = 0,5$;

$ВК_{ТЗ} = 0,5$.

Якщо здобувач вищої освіти набрав за поточний контроль 60 балів або більше, він може погодити дану оцінку в електронному кабінеті і вона стане семестровою оцінкою за вивчення навчальної дисципліни.

Якщо здобувач вищої освіти під час вивчення навчальної дисципліни набрав 60 балів або більше і бажає покращити свій результат успішності, він проходить процедуру підсумкового контролю у формі заліку. За складання заліку здобувач вищої освіти може набрати 100 балів. Семестрова оцінка з навчальної дисципліни формується за результатами підсумкового контролю.

Здобувач вищої освіти допускається до процедури підсумкового контролю у формі заліку, якщо за виконання завдань поточного контролю набрав 50 балів або більше.

Якщо здобувач вищої освіти за результатами поточного контролю набрав 35□49 балів, він отримує право за власною заявою повторно опанувати окремі теми навчальної дисципліни понад обсяги, встановлені навчальним планом освітньої програми. Повторне вивчення окремих складових навчальної дисципліни понад обсяги, встановлені навчальним планом освітньої програми, здійснюється у вільний від занять здобувача вищої освіти час.

Якщо здобувач вищої освіти за результатами поточного контролю набрав від 0 до 34 балів (включно), він вважається таким, що не виконав вимоги робочої програми навчальної дисципліни та має академічну заборгованість. Здобувач вищої освіти отримує право за власною заявою повторно опанувати навчальну дисципліну у наступному семестрі понад обсяги, встановлені навчальним планом освітньої програми.

Процедура надання додаткових освітніх послуг здобувачу вищої освіти з метою повторного вивчення навчальної дисципліни чи її окремих складових частин визначена у Положенні про надання додаткових освітніх послуг здобувачам вищої освіти в Державному університеті «Житомирська політехніка».

Визнання результатів навчання, набутих у неформальній та/або інформальній освіті

Визнання результатів навчання, набутих у неформальній та/або інформальній освіті в рамках окремих тем навчальної дисципліни, здійснюється викладачем за зверненням здобувача вищої освіти та представленням документів, які підтверджують результати навчання (сертифікати, свідоцтва, скріншоти тощо). Рішення про визнання та оцінка за відповідну частину освітнього компонента приймається викладачем за результатами співбесіди зі здобувачем вищої освіти.
Рекомендованими ресурсами для неформальної освіти за даним курсом є: The Web Security Academy (https://portswigger.net/web-security), TryHackMe (https://tryhackme.com/), курс Ethical Hacker від Академії Cisco (https://www.netacad.com/courses/ethical-hacker).
Визнання результатів навчання, набутих у неформальній та/або інформальній освіті в рамках цілого освітнього компонента, здійснюється за процедурою, яка визначена у Положенні про організацію освітнього процесу у Державному університеті «Житомирська політехніка».

Шкала оцінювання

Шкала ЄКТС	Національна шкала	100-бальна шкала
A	Зараховано	90-100
B	Зараховано	82-89
C		74-81
D	Зараховано	64-73
E		60-63
FX	Не зараховано	35-59
F	Не зараховано	0-34

11. Глосарій

№ з/п	Термін державною мовою	Відповідник англійською мовою
1	Уніфікований локатор ресурсів або адреса ресурсу	Uniform Resource Locator, URL
2	Протокол передачі гіпертекстових документів	HyperText Transfer Protocol, HTTP
3	Мова розмітки гіпертексту	HyperText Markup Language, HTML
4	Безпека вебдодатків	Web application security
5	Політика однакового походження	Same-origin policy
6	Контроль доступу	Access control

№ з/п	Термін державною мовою	Відповідник англійською мовою
7	Шифрування	Encryption
8	Атака грубою силою або простого перебору	Brute-force attack
9	Атака за словником	Dictionary attack
10	Багатофакторна аутентифікація	Multi-Factor Authentication, MFA
11	Незахищені прямі посилання на об’єкти	Insecure Direct Object Reference, IDOR
12	Необмежене завантаження файлів	Unrestricted file upload
13	Міжсайтовий скріптинг	Cross-Site Scripting, XSS
14	Віртуальна приватна мережа	Virtual Private Network, VPN
15	Підробка міжсайтових запитів	Cross-Site Request Forgery, CSRF
16	Вразливості	Vulnerabilities
17	Підробка запитів на стороні сервера	Server-Side Request Forgery, SSRF
18	Відмова в обслуговуванні та Розподілена відмова в обслуговуванні	Denial of Service, DoS & Distributed Denial of Service, DDoS
19	Витік інформації	Information leakage
20	Розкриття чутливої інформації	Sensitive data exposure
21	Тестування на проникнення	Penetration testing
22	Угода про нерозголошення	Non-Disclosure Agreement, NDA
23	Підвищення привілеїв	Privilege escalation
24	Приманка	Honeypot
25	Зворотна оболонка	Reverse shell
26	Життєвий цикл розробки ПЗ	Software Development Life Cycle, SDLC
27	Безпека через невідомість	Security by Obscurity
28	Результативність	Effectiveness
29	Ефективність	Efficiency
30	Рентабельність або повернення інвестицій	Return on Investment, ROI

12. Рекомендована література

Основна література

1. The Web Security Academy. URL: https://portswigger.net/web-security
2. TryHackMe. URL: https://tryhackme.com/
3. OWASP Foundation. URL: https://owasp.org/
4. Академія Cisco, Курс Ethical Hacker. URL: https://www.netacad.com/courses/ethical-hacker

Допоміжна література

1. Aleks N., Farhi D. Black Hat Bash: Creative Scripting for Hackers and Pentesters, 2024. 344p.

2. Apache. URL: https://apache.org/
3. AttackDefense Lab. URL: https://attackdefense.com/
4. Ball C.J. Hacking APIs, 2022. 368 p.
5. Common Vulnerability Scoring System SIG. URL: https://www.first.org/cvss/
6. Content Security Policy (CSP) Quick Reference Guide. URL: https://content-security-policy.com/
7. CryptoHack. URL: https://cryptohack.org/
8. CTFlearn. URL: https://ctflearn.com/
9. CVE. URL: https://www.cve.org/
10. Death D. Information Security Handbook, 2023. 370p.
11. DREAD Threat Modeling. URL: https://threat-modeling.com/dread-threat-modeling/
12. DVWA. URL: https://github.com/digininja/DVWA
13. GDPR. URL: https://gdpr-text.com/uk/
14. Google Hacking Database. URL: https://www.exploit-db.com/google-hacking-database
15. Gray J. Practical Social Engineering. A Primer for the Ethical Hacker, 2022. – 240 p.
16. Hacker101. URL: https://www.hacker101.com/
17. HackTheBox. URL: https://www.hackthebox.com/
18. Harwood M., Price R. Internet and Web Application Security, 2022. 450p.
19. HIPAA. URL: https://www.govinfo.gov/content/pkg/CRPT-104hrpt736/pdf/CRPT-104hrpt736.pdf
20. ISO/IEC 27001. URL: https://www.iso.org/standard/27001
21. Meel U. Advanced Penetration Testing with Kali Linux, 2023. 384p.
22. Metasploit Documentation. URL: https://docs.metasploit.com/
23. MITRE CWE. URL: https://cwe.mitre.org/
24. MITRE CWSS. URL: https://cwe.mitre.org/cwss/cwss_v1.0.1.html
25. MITRE’s Adversarial Tactics, Techniques & Common Knowledge (ATT&CK). URL: https://attack.mitre.org/
26. NIST Technical Guide to Information Security Testing. URL: http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf
27. Nmap. URL: http://nmap.org/
28. Onofri S., Onofri D. Attacking and Exploiting Modern Web Applications, 2023. 338p.
29. OSINT Framework. URL: https://osintframework.com/
30. OWASP Application Security Verification Standard. URL: https://owasp.org/www-project-application-security-verification-standard/
31. OWASP Authentication Cheat Sheet. URL: https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html

32. OWASP Forgot Password Cheat Sheet. URL: https://cheatsheetseries.owasp.org/cheatsheets/Forgot_Password_Cheat_Sheet.html
33. OWASP Juice Shop. URL: https://owasp.org/www-project-juice-shop/
34. OWASP Mobile Application Security. URL: https://owasp.org/www-project-mobile-app-security/
35. OWASP SAMM. URL: https://owasp.org/www-project-samm/
36. OWASP Threat Dragon. URL: https://owasp.org/www-project-threat-dragon/
37. OWASP Top 10 Proactive Controls. URL: https://top10proactive.owasp.org/
38. OWASP Top Ten. URL: https://owasp.org/Top10/
39. OWASP Web Security Testing Guide. URL: https://owasp.org/www-project-web-security-testing-guide/
40. OWASP WebGoat Project. URL: https://owasp.org/www-project-webgoat/
41. PASTA Threat Modeling. URL: https://threat-modeling.com/pasta-threat-modeling/
42. PCI DSS. URL: https://www.pcisecuritystandards.org/standards/
43. PentesterLab. URL: https://pentesterlab.com/
44. picoCTF. URL: https://picoctf.org/
45. Prasad K. New Methods for Detection of DoS and DDoS Attacks, 2023. 366p.
46. Rakshit S.K. Ethical Hacker's Penetration Testing Guide, 2022. 472 p.
47. RedTeam-Tools. Розвідка. URL: https://hackyourmom.com/osvita/%e2%84%962-redteam-tools-rozvidka/
48. Singh G.D. Reconnaissance for Ethical Hackers, 2023. 430 p.
49. Soper R., Torres N.N., Almoailu A. Zed Attack Proxy Cookbook, 2023. 284 p.
50. STRIDE. URL: https://learn.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20)?redirectedfrom=MSDN
51. VulnHub. URL: https://www.vulnhub.com/
52. Wear S. Burp Suite Cookbook - Second Edition, 2023. 450 p.
53. WPScan User Documentation. URL: https://github.com/wpscanteam/wpscan/wiki/WPScan-User-Documentation
54. Zalewski M. Browser Security Handbook. URL: https://code.google.com/archive/p/browsersec/wikis/Main.wiki
55. Безпека by design. URL: https://hackyourmom.com/osvita/bezpeka-by-design-chastyna-1-rol-proektuvannya-u-bezpeczi/
56. Головня О. С. Основи операційних систем: Навч. посібник. Житомир: «Житомирська політехніка», 2023. 126 с.
57. Єфіменко А.А. Основи побудови локальних комп’ютерних мереж Ethernet на базі керованих комутаторів компанії Cisco: Навч. посібник. Житомир: «Житомирська політехніка», 2021. 116 с.
58. Живило Є.О. Тестування на проникнення: Навч. посібник. Ч.1. Полтава: ПНТУ, 2024. 134 с.

59. Живило Є.О. Тестування на проникнення: Навч. посібник. Ч.2. Полтава: ПНТУ, 2024. 239 с.
60. Опановуємо Burp Suite, незамінний інструмент для пентестерів. URL: https://hackyourmom.com/osvita/opanovuyemo-burp-suite-nezaminnyj-instrument-dlya-pentesteriv/
61. Основи безпеки вебсайтів. URL: https://www.godaddy.com/uk-ua/how-to/osnovi-bezpeki-veb-sajtiv/
62. Пентест від А до Я: посібник з тестування на проникнення. URL: https://kr-labs.com.ua/blog/testuvannya-na-pronyknennya-pentest-vid-a-do-ya/
63. Переповнення буфера. URL: https://cqr.company/ua/web-vulnerabilities/buffer-overflow/
64. Переповнення цілих чисел. URL: https://cqr.company/ua/web-vulnerabilities/integer-overflow/
65. Перечитування буфера. URL: https://cqr.company/ua/web-vulnerabilities/buffer-over-read/
66. Повний посібник з John the Ripper. Ч.1: знайомство та встановлення John the Ripper. URL: https://hackyourmom.com/servisy/soft/povnyj-posibnyk-z-john-the-ripper-ch-1-znajomstvo-ta-vstanovlennya-john-the-ripper/
67. Повний посібник з John the Ripper. Ч.2: утиліти для отримання хешей. URL: https://hackyourmom.com/servisy/soft/povnyj-posibnyk-z-john-the-ripper-ch-2-utylity-dlya-otrymannya-heshej/
68. Повний список інструментів для тестування і злому проникнення для хакерів і фахівців з безпеки. URL: https://hackyourmom.com/kibervijna/povnyj-spysok-instrumentiv-dlya-testuvannya-i-zlomu-pronyknennya-dlya-hakeriv-i-fahivcziv-z-bezpeky/
69. Посібник з Nmap. URL: https://hackyourmom.com/kibervijna/posibnyk-z-nmap/
70. Посібник з веббезпеки. URL: http://websecurity.com.ua/security/
71. Проценко О.Б. Інформаційна безпека вебдодатків. Сучасні інформаційні технології в кібербезпеці. Суми: СДУ, 2021. С. 317–329.
72. Терейковський І.А., Гнатюк С.О. Захист інформації в комп'ютерних системах. К.: КПІ, 2022. 135 с.
73. Умови гонки. URL: https://cqr.company/ua/web-vulnerabilities/race-conditions/
74. Щур Н.О., Покотило О.А. Основи криптології: Навч. посібник. Житомир: «Житомирська політехніка», 2021. 120 с.
75. Як провести зовнішній аудит безпеки веб-додатків? Алгоритм і методика роботи. URL: https://kr-labs.com.ua/blog/yak-provesty-audyt-bezpeky-veb-dodatkiv-metodologiya-i-algorytm/

13. Інформаційні ресурси в Інтернеті

1. The Web Security Academy. URL: https://portswigger.net/web-security
2. TryHackMe. URL: https://tryhackme.com/
3. Академія Cisco, Курс Ethical Hacker. URL: https://www.netacad.com/courses/ethical-hacker
4. OWASP Foundation. URL: https://owasp.org/