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

ЗАТВЕРДЖУЮ

Декан ФКІТ
Ігор ЯКИМЕНКО

«__29__» __08_____ 2025 р.

ЗАТВЕРДЖУЮ

Проректор з науково-
педагогічної роботи
Віктор ОСТРОВЕРХОВ

«__29__» __08_____ 2025 р.

РОБОЧА ПРОГРАМА

з дисципліни «Безпека WEB ресурсів»
ступінь вищої освіти - бакалавр
галузь знань - 12 Інформаційні технології
спеціальність - 125 Кібербезпека та захист інформації
освітньо-професійна програма – Кібербезпека

Кафедра кібербезпеки

Форма навчання	Курс	Семестр	Лекції (год.)	Лаб. (год.)	ІРС (год.)	Тренінг (год.)	СРС (год.)	Разом (год.)	іспит (сем.)
денна	3	6	30	30	4	8	78	150	6

29.08.2025 р.

Тернопіль –2025

Робоча програма розроблена на основі освітньо-професійної програми підготовки бакалавра галузі знань 12 «Інформаційні технології» спеціальності 125 «Кібербезпека та захист інформації», затвердженої Вченою радою ЗУНУ (протокол № 10 від 23.06.2023 р.).

Робочу програму склали доцент кафедри кібербезпеки, к.т.н., доцент Цаволик Тарас Григорович, викладач кафедри кібербезпеки Бараннік Богдан Олександрович

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

Завідувач кафедри кібербезпеки _____ Василь ЯЦКІВ

Гарант освітньо-професійної програми _____ Михайло КАСЯНЧУК

СТРУКТУРА РОБОЧОЇ ПРОГРАМИ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

1. Опис дисципліни «Безпека WEB ресурсів»

Дисципліна - «Безпека WEB ресурсів»	**Галузь знань, спеціальність, СВО**	**Характеристика навчальної дисципліни**
Кількість кредитів – 5	Галузь знань – 12 Інформаційні технології	Статус дисципліни – обов'язкова Мова навчання - українська
Кількість залікових модулів - 5	Спеціальність - 125 Кібербезпека та захист інформації	Рік підготовки: *Денна - 3* Семестр: *Денна - 6*
Кількість змістових модулів – 3	Ступінь вищої освіти – бакалавр	Лекції (год): *Денна - 30* Лабораторні заняття (год): *Денна - 30*
Загальна кількість годин – 150 год.		Самостійна робота (год): *Денна* – 78 Тренінг (год): *Денна* – 8 Індивідуальна робота (год): *Денна – 4*
Тижневих годин: 10 год., з них аудиторних – 4 год.		Вид підсумкового контролю – іспит

2. Мета й завдання вивчення дисципліни «Безпека WEB ресурсів»

2.1. Мета вивчення дисципліни

Програма та тематичний план дисципліни орієнтовані на глибоке та ґрунтовне засвоєння здобувачами ОПП основних понять щодо особливостей безпеки WEB ресурсів.

Ця дисципліна відноситься до дисциплін циклу професійної та практичної підготовки. Метою викладання курсу є надання здобувачам ОПП знань про захист Web–технологій, засвоєння можливостей використання різноманітних атак та протидія їм на WEB ресурси.

Вивчення курсу "Безпека WEB ресурсів" вимагає цілеспрямованої роботи над вивченням спеціальної літератури, активної роботи на лекціях та практичних заняттях, самостійної роботи та виконання індивідуальних завдань.

2.2. Завдання вивчення дисципліни

У результаті вивчення курсу "Безпека WEB ресурсів" здобувачі ОПП повинні засвоїти:

- основи WEB атак та захисту від них;
- особливості використання SQL injection;
- особливості використання різних XSS атак;
- особливості атаки на заголовки хостів HTTP(HTTP Host Header attacks);
- отруєння веб-кешом.

Завдання лекційних занять.

Мета проведення лекцій полягає у тому, щоб ознайомити здобувачів ОПП із основними відомостями щодо атак та захисту WEB ресурсів.

Мета проведення лекцій полягає у:

- викладенні здобувачам ОПП у відповідності з програмою та робочим планом основних понять безпеки WEB ресурсів;
- сформувати цілісну систему теоретичних знань з курсу "Безпека WEB ресурсів".

Завдання лабораторних занять.

Мета проведення лабораторних занять полягає у тому, щоб виробити у здобувачів ОПП практичні навички атакуючої безпеки WEB ресурсів.

Завдання проведення лабораторних занять:

- ознайомити з особливостями ураження WEB ресурсів;
- ознайомитись з сучасними засобами для виявлення вразливостей WEB ресурсів;
- отримання навиків з захисту WEB ресурсів;
- глибше засвоїти та закріпити теоретичні знання, які були одержані на лекціях.

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

КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.

КФ 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.

КФ 14. Здатність здійснювати пошук, оцінювання вразливостей та захист WEB-додатків.

2.4. Передумови для вивчення дисципліни

Вивчення курсу «Безпека WEB ресурсів» передбачає наявність систематичних та ґрунтовних знань із суміжних курсів, таких як «Основи програмування», «Кібернетична безпека», «Комп'ютерні мережі»

2.5. Результати навчання

ПРН12. Розробляти моделі загроз та порушника.

ПРН20. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно телекомунікаційних системах.

ПРН23. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно телекомунікаційних (автоматизованих) системах.

ПРН56. Здійснювати пошук, оцінювання вразливостей та захист WEB-додатків.

3. Програма навчальної дисципліни «Безпека WEB ресурсів»

Змістовий *модуль 1.* Виявлення атак на веб ресурси.

Тема 1. Введення в безпеку WEB ресурсів.

Вивчення основ WEB безпеки.

Тема 2. Міжсайтові сценарії XSS атаки.

Як працює XSS. Типи XSS атак. Відбиті XSS сценарії. Збережені XSS сценарії. Тестування виявлених вразливостей.

Тема 3. Міжсайтові сценарії XSS на основі DOM атаки.

Тестування на виконання JavaScript. DOM XSS у поєднанні з відображеними та збереженими даними.

Тема 4. SQL ін'єкції.

Вплив успішних SQL атак. Отримання прихованих даних. Підміна логіки програми. Вивчення баз даних. Запобігання SQL ін'єкцій.

Тема 5. SQL-ін'єкційні UNION атаки.

Вплив UNION атак. Пошук кількості стовпців під час атаки. Використання SQL – ін'єкцій UNION для отримання даних з таблиць баз даних. Сліпі SQL ін'єкції.

Змістовий модуль 2. **Атаки та ін'єкції веб ресурсів.**

Тема 6. XML (XXE) ін'єкція.

Що таке XML (XXE) ін'єкція? Вразливості XML (XXE). Типи атак XXE. Використання XXE для отримання файлів з веб ресурсів. Сліпі вразливості XXE. XXE атаки через завантаження файлів. Запобігання вразливостей XXE.

Тема 7. Отруєння веб - кешем.

Основні поняття отруєння веб – кешем. Вплив атак на отруєння веб - кешем. Запобігання отруєнню веб – кешем.

Змістовий модуль 3. Атаки на заголовки HTTP та викриття вразливостей.

Тема 8. Атаки заголовку хоста HTTP.

Протокол HTTP. Маршрутизація трафіку через посередника. Вразливості заголовка хоста HTTP. Запобігання атак заголовків хоста.

Тема 9. Вразливості розкриття інформації.

Пошук та використання вразливостей розкриття інформації. Оцінка вразливостей при розкритті інформації. Запобігання вразливостей при розкритті інформації.

4. Структура залікового кредиту з дисципліни «Безпека WEB ресурсів»

	Кількість годин					
	Лек-ції	Лаб. роботи	СРС	ІРС	Тренінг	Контрольні заходи
Змістовий модуль 1. Виявлення атак на веб ресурси						
Тема 1. Введення в безпеку WEB ресурсів	2	2	4	2	4	Поточне опитування
Тема 2. Міжсайтові сценарії XSS атаки	2	2	4			
Тема 3. Міжсайтові сценарії XSS на основі DOM атаки	2	2	10			
Тема 4. SQL ін'єкції	2	2	10			
Тема 5. SQL-ін'єкційні UNION атаки	2	2	10			
Змістовий модуль 2. Атаки та ін'єкції веб ресурсів						
Тема 6. XML (XXE) ін'єкція	5	5	10	1	2	Поточне опитування
Тема 7. Отруєння веб - кешем	5	5	10			
Змістовий модуль 3. Атаки на заголовки HTTP та викриття вразливостей						
Тема 8. Атаки заголовку хоста HTTP.	5	5	10	1	2	Поточне опитування
Тема 9. Вразливості розкриття інформації	5	5	10			
Разом	30	30	78	4	8	

5. Тематика лабораторних робіт

Лабораторна робота №1

Тема: XSS атака у контексті HTML.

Мета: Освоїти основи XSS атаки.

Лабораторна робота №2

Тема: XSS атака на основі DOM.

Мета: Навчитись виявляти атаки на основі DOM.

Лабораторна робота №3

Тема: SQL – ін’єкція.
Мета: Навчитись виконувати SQL – ін’єкції.
Лабораторна робота №4
Тема: Union SQL – ін’єкція.
Мета: Навчитись виконувати Union SQL – ін’єкції.
Лабораторна робота №5
Тема: XML (XXE) ін’єкції.
Мета: Навчитись проводити XXE атаки.
Лабораторна робота №6
Тема: Отруєння веб - кешем.
Мета: Навчитись працювати та виявляти ін’єкції веб - кешем.
Лабораторна робота №7
Тема: HTTP атаки.
Мета: Навчитись проводити HTTP атаки.

6. Самостійна робота

Самостійна робота з курсу «Безпека WEB ресурсів» включає вивчення наведених тем та оцінюється у вигляді тесту:

1. Cross-Site Scripting (XSS) атаки та методи захисту
2. Cross-Site Request Forgery (CSRF) вразливості
3. SQL-ін'єкції та параметризовані запити
4. Content Security Policy (CSP) implementation
5. Same-Origin Policy та CORS налаштування
6. Authentication bypass та session hijacking
7. Authorization flaws та privilege escalation
8. Server-Side Request Forgery (SSRF) атаки
9. File upload vulnerabilities та bypass techniques
10. NoSQL injection attacks
11. JWT security та token-based authentication
12. Directory traversal та path manipulation
13. XML External Entity (XXE) attacks
14. CORS misconfigurations та exploitation
15. Content-Type sniffing attacks

7. Організація та проведення тренінгу з дисципліни WEB технології

Порядок проведення тренінгу:

1. Вступна частина проводиться з метою ознайомлення здобувачів ОПП з темою тренінгу.

2. Організаційна частина полягає у створенні робочого настрою у колективі.

3. Практична частина реалізується шляхом виконання завдань з певних проблемних питань теми тренінгу, які здобувач вибирає або самостійно, або з запропонованого переліку.

4. Підведення підсумків. Обговорення результатів виконаних завдань. Обмін думками з питань, що виносились на тренінг.

Тематика тренінгу: Проектування предметної області та написання WEB програми для її реалізації.

Мета тренінгу: забезпечення здобувачів ОПП комплексними теоретичними знаннями та практичними навичками.

Завдання тренінгу: презентація результатів, за орієнтовною тематикою:

1. XSS Attack Vectors
2. Content Security Policy Implementation
3. CSRF Protection Mechanisms
4. Client-Side Storage Security

5. Browser Security Features
6. Third-Party Script Security
7. Web Crypto API для шифрування в браузері
8. SQL Injection Advanced Techniques
9. NoSQL Injection Attacks
10. Server-Side Request Forgery (SSRF)
11. Authentication Bypass Techniques
12. Authorization Flaws Deep Dive
13. File Upload Vulnerabilities
14. Command Injection Exploitation
15. XML External Entity (XXE) Attacks

8. Методи навчання.

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

9. Засоби оцінювання та методи демонстрування результатів навчання

У процесі вивчення дисципліни «Безпека WEB ресурсів» використовуються наступні методи оцінювання навчальної роботи здобувача ОПП:

– підсумкове тестування за кожним змістовним модулем;
– оцінювання виконання лабораторних робіт;
– оцінювання тренінгів;
– самостійна робота;
– підсумковий екзамен.

10. Політика оцінювання

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

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

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

11. Критерії, форми поточного та підсумкового контролю

Підсумковий бал (за 100 – бальною шкалою) з дисципліни «Безпека WEB ресурсів» визначається як середньозважена величина, в залежності від питомої ваги кожної складової залікового кредиту %:

Модуль 1		Модуль 2		Модуль 3	Модуль 4	Модуль 5
10%	10%	10%	10%	5%	15%	40%
Поточне оцінювання	Модульний контроль 1	Поточне оцінювання	Модульний контроль 2	Тренінги	Самостійна робота	Екзамен
Оцінка за даний модуль визначається як середнє арифметичне за захист лабораторних робіт №1-5.	Підсумкове модульне тестування за темами № 1-5.	Оцінка за даний модуль визначається як середнє арифметичне за захист лабораторних робіт №6-7.	Підсумкове модульне тестування за темами № 6-9.	Визначається як середнє арифметичне з оцінок за виконання та презентацію одного завдання тренінгу.	Підсумкове тестування за результатами опрацювання теоретичного матеріалу. Теоретичні питання: 25 питань по 4 бали - max 100 балів	Теоретичні питання: 2 питання по 30 балів - max 60 балів. Практичне завдання - max 40 балів

Виконання лабораторних робіт:

90–100 балів – робота виконана самостійно, без помилок, усі етапи задокументовано, правильне використання інструментів.

75–89 балів – виконання із незначними помилками, що не вплинули на результат; часткова потреба в підказках.

60–74 бали – виконання із суттєвими помилками; поверхневе розуміння завдань.

1–59 балів – робота не виконана або результат неправильний; відсутність навичок.

Тренінг:

90–100 балів – повне володіння матеріалом, аргументоване застосування знань, правильне виконання завдань, наявність елементів власного дослідження, творчий підхід.

75–89 балів – здебільшого правильне виконання, незначні помилки, достатньо аргументоване використання матеріалу, частково присутні елементи власного дослідження.

65–74 бали – розв’язання завдань з помилками, недостатня аргументація, поверхневе опрацювання теми, обмежена самостійність.

60–64 бали – часткове або фрагментарне виконання завдань, відсутність повного обґрунтування, мінімальний авторський внесок.

1–59 балів – завдання практично не виконано, повністю неправильне розв’язання, відсутність дослідницького або творчого підходу.

Самостійна робота: оцінюється у вигляді тестування за результатами опрацювання теоретичного матеріалу. Теоретичні питання: 25 питань по 4 бали, Максимальна оцінка 100 балів.

Підсумкове модульне тестування:

90–100 балів – правильно виконано 90–100% завдань тесту.

75–89 балів – правильно виконано 75–89% завдань тесту.

60–74 бали – правильно виконано 60–74% завдань тесту.

1–59 балів – правильно виконано менше 60% завдань тесту.

Екзамен – підсумковий контроль, який проводиться з метою оцінювання засвоєння здобувачем вищої освіти теоретичного та практичного матеріалу. Екзаменаційне завдання складається з двох блоків:

Відповіді на теоретичні питання (максимум 60 балів):

45-60 балів – повне володіння матеріалом, аргументована та всебічна відповідь, демонстрація глибокого розуміння;

30-44 бали – достатнє володіння матеріалом, відповідь здебільшого правильна, допускаються незначні неточності;

11–29 балів – відповідь охоплює лише основні аспекти теми, бути пропущені важливі деталі. Здобувач не завжди впевнено відповідає на запитання.

0-10 балів – фрагментарне або неправильне викладення матеріалу, суттєві недоліки в аргументації.

Практичне завдання (тестове, максимум 40 балів):

20–40 балів – всі завдання виконані правильно, повне розуміння практичного матеріалу;

10–19 балів – завдання виконані частково правильно, допускаються незначні або суттєві помилки;

0–9 балів – завдання виконано неправильно або не виконано взагалі.

Шкала оцінювання:

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

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

№	Найменування	Номер теми
1	Мультимедійний проектор та проєкційний екран	1 -9
2	Персональні комп'ютери	1 -9
3	Комунікаційне програмне забезпечення (Zoom) для проведення занять у режимі он-лайн (за необхідності)	1 -9
4	Комунікаційна навчальна платформа (Moodle) для організації дистанційного навчання (за необхідності)	1 -9
5	Наявність доступу до мережі Інтернет	1 -9

РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

1. Безпека вебдодатків : навч. посібн. / О.В. Пірог. – Електронні дані. – Житомир : Житомирська політехніка, 2025. – 290 с.
2. Основи web-програмування: навч. посіб. / С. В. Баран. - Кривий Ріг, 2023. –316 с.
3. Kimminich B. Pwining OWASP Juice Shop. 2020. – 301 p.
4. Andrew Hoffman. Web Application Security. Published by O'Reilly Media, Inc. 2020. – 331 p.
5. Joseph Menn. Cult of the Dead Cow: How the Original Hacking Supergroup Might Just Save the World, June 4, 2021. – 272 p.

6. Christopher Hadnagy. Social Engineering: The Science of Human Hacking, July 31, 2022 – 320p.
7. Kevin Mitnick. The Art of Invisibility: The World's Most Famous Hacker Teaches You How to Be Safe in the Age of Big Brother and Big Data, September 10, 2022 - 320 pages.
8. Charles Arthur. Cyber Wars: Hacks that Shocked the Business World 1st Edition, May 29, 2021 - 248 pages
9. Bruce Schneier. Click Here to Kill Everybody: Security and Survival in a Hyper-connected World, October 8, 2022 - 336 pages