**ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ**

**ЗАТВЕРДЖУЮ**

Декан факультету інформаційних технологій

_____ Тетяна ГОВОРУЩЕНКО
Підпис Ім'я, ПРІЗВИЩЕ

29 серпня 2025 р.

# РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

## ***Безпека вебресурсів***

***Галузь знань*** 12 – Інформаційні технології
***Спеціальність*** – 125 Кібербезпека
***Рівень вищої освіти*** – Перший (бакалаврський)
***Освітньо-професійна програма*** – Кібербезпека та захист інформації
***Обсяг дисципліни*** – 5 кредитів ЄКТС
***Шифр дисципліни*** – ОПП.07
***Мова навчання*** – Українська
***Статус дисципліни*** – Обов'язкова (професійної підготовки)
***Факультет*** – Інформаційних технологій
***Кафедра*** – Кібербезпеки

| Форма здобуття освіти | Курс | Семестр | Загальний обсяг | | Кількість годин | | | | | | Курсовий проєкт* | Курсова робота | Форма семестрового контролю | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Аудиторні заняття | | | | | Самостійна робота, у т.ч. ІРС | | | | |
| | | | Кредити ЄКТС | Години | Разом | Лекції | Лабораторні роботи | Практичні заняття | Семінарські заняття | | | | Залік | Іспит |
| Д | 2 | 4 | 5 | 150 | 50 | 16 | 34 | | | 100 | | | + | |
| **Разом ДФН** | | | **5** | **150** | **50** | **16** | **34** | | | **100** | | | **1** | |

Робоча програма складена на основі освітньо-професійної програми «Кібербезпека та захист інформації» за спеціальністю 125 «Кібербезпека та захист інформації»

Робоча програма складена _____ канд. техн. наук, доцент Ігор МУЛЯР
Підпис автора(ів) Науковий ступінь, вчене звання, Ім'я, ПРІЗВИЩЕ автора(ів)

Схвалена на засіданні кафедри Кібербезпеки

Протокол від 29.08.2025 № 1. Зав. кафедри _____ Юрій КЛЬОЦ
Підпис Ім'я, ПРІЗВИЩЕ

Робоча програма розглянута та схвалена вченою радою факультету інформаційних технологій

Голова вченої ради факультету _____ Тетяна ГОВОРУЩЕНКО
Підпис Ім'я, ПРІЗВИЩЕ

Хмельницький 2025

# ЛИСТ ПОГОДЖЕННЯ

| Посада | Назва кафедри | Підпис | Ініціали, прізвище |
|---|---|---|---|
| Завідувач кафедри, канд. техн. наук, доц. | Кібербезпеки | | Юрій КЛЬОЦ |
| Гарант освітньо-професійної програми, канд. техн. наук, доц. | Кібербезпеки | | Віктор ЧЕШУН |

### 3. Пояснювальна записка

Дисципліна «Безпека вебресурсів» є однією із дисциплін фахової підготовки здобувачів першого (бакалаврського) рівня вищої освіти, очної (денної) форми здобуття вищої освіти, які навчаються за освітньо-професійною програмою «Кібербезпека та захист інформації» в межах спеціальності 125 «Кібербезпека та захист інформації».

***Пререквізити*:** ОПП.01 Основи інформаційної безпеки, ОПП.02 Операційні системи та технології їх захисту

***Постреквізити*:** ОПП.15 Виробнича практика 1, ОПП.16 Виробнича практика 2.

Відповідно до освітньої програми дисципліна сприяє забезпеченню:

***компетентностей*:** ІК Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки і/або кібербезпеки, що характеризуються комплексністю та неповною визначеністю умов; ЗК 2 Знання та розуміння предметної області та розуміння професії; ЗК 4 Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням; ФК 2 Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки; ФК 5 Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.

***програмних результатів навчання*:** ПРН 4 Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення; ПРН 6 Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності; ПРН 11 Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах.

***Мета дисципліни.*** Формування у здобувачів умінь та компетенцій для оцінювання та забезпечення необхідного рівня захищеності вебресурсів; розвиток у студентів фахового стилю мислення.

***Предмет дисципліни.*** Сучасні програмні та програмно-апаратні методи та засоби оцінювання та забезпечення необхідного рівня захищеності вебресурсів

***Завдання дисципліни.*** Формування у майбутніх спеціалістів умінь, навичок та компетентностей для забезпечення безпеки вебресусів у комп'ютерних та інформаційно-комунікаційних системах та реагування на кіберінциденти.

***Результати навчання.*** Після вивчення дисципліни студент повинен: *реалізовувати* заходи з протидії отриманню несанкціонованого доступу до вебресурсів в інформаційних та інформаційно-телекомунікаційних системах; *використовувати* сучасні методи та моделі інформаційної безпеки та/або кібербезпеки, теорії та методи захисту для забезпечення безпеки вебресурсів, як елементів інформаційно-телекомунікаційних систем; *застосовувати* сучасні технології захисту інформації; *реагувати* на кіберінциденти; *аналізувати* загрози; *забезпечувати* відновлення систем.

### 4. Структура залікових кредитів дисципліни

**IV семестр**

| Назва теми | Кількість годин відведених на: | | |
|---|---|---|---|
| | **лекції** | **практичні заняття** | **СРС** |
| Тема 1. Основи безпеки вебдодатків та методології тестування на проникнення | 3 | 12 | 36 |
| Тема 2. Вебатаки та вразливості вебресурсів | 5 | 22 | 64 |
| Тема 3. Основи Безпека вебресурсів (ІБ) та системи управління ІБ (СУІБ) | 8 | 10 | 28 |
| **Разом:** | **16** | **34** | **100** |

**5. Програма навчальної дисципліни**

**5.1 Зміст лекційного курсу**

**IV семестр**

| Номер лекції | Перелік тем лекцій, їх анотація | Години |
|---|---|---|
| **Тема 1. Основи безпеки вебдодатків та методології тестування на проникнення** | | **6** |
| **1** | **Безпека вебдодатків та її значення в сучасному цифровому світі.** HTTP-запити та відповіді, методи та повідомлення. HTTPS. Cookie. Поняття тестування на проникнення: мета, завдання та етапи проведення. Методології пентестингу: модель PTES (Penetration Testing Execution Standard), OSSTMM (Open Source Security Testing Methodology Manual) та їх застосування. Етичні та правові аспекти тестування на проникнення. Типи пентестингу: white box, black box, gray box. Огляд інструментів та платформ для тестування безпеки вебдодатків. Літ.: [1] с.16-30, 89-124; [2] с.37-46; [3] с.19-45; [4] с. 8-26; [15]; [21]; [26] | 2 |
| **2** | **OWASP Top 10: критичні вразливості вебдодатків** Організація OWASP (Open Web Application Security Project) та її роль у сфері веб-безпеки. Огляд OWASP Top 10: порушення контролю доступу (Broken Access Control), криптографічні помилки (Cryptographic Failures), ін'єкції (Injection). Небезпечний дизайн (Insecure Design) та неправильні налаштування безпеки (Security Misconfiguration). Застарілі та вразливі компоненти (Vulnerable and Outdated Components). Проблеми ідентифікації та автентифікації (Identification and Authentication Failures). Помилки у перевірці цілісності програмного забезпечення та даних (Software and Data Integrity Failures). Недостатнє логування та моніторинг (Security Logging and Monitoring Failures). Підробка запитів на стороні сервера (Server-Side Request Forgery). Літ.: [1] с. 32-46; [2] с.37-46; [27] | 2 |
| **3** | **Розвідка та збір інформації (Reconnaissance & Information Gathering)** Пасивна розвідка: збір інформації без прямої взаємодії з цільовою системою. Використання пошукових систем для збору інформації (Google Dorking). WHOIS запити та аналіз DNS записів. Аналіз метаданих документів та зображень. Моніторинг соціальних мереж та витоків даних (OSINT). Активна розвідка: сканування портів та служб за допомогою Nmap. Визначення версій програмного забезпечення та операційних систем. Виявлення технологій, що використовуються вебсайтом (Wappalyzer, BuiltWith). Інструменти для збору інформації: theHarvester, Shodan, Maltego, Recon-ng. Автоматизація процесу розвідки та документування результатів за допомогою ШІ. Літ.: [1] с. 40-89, 150-156; [2] с.46-89; [3] с.53-75; [4] с. 88-118; [19-22]; [24] | 2 |
| **Тема 2. Вебатаки та вразливості вебресурсів** | | **10** |
| **4** | **Тестування автентифікації та управління сесіями** Механізми автентифікації у вебдодатках: форми входу, багатофакторна автентифікація, SSO. Атаки на механізми автентифікації: брутфорс, підбір облікових даних (credential stuffing). Тестування на слабкі паролі та політики паролів. Атаки на відновлення паролів та реєстрацію користувачів. Управління сесіями: cookies, токени (JWT), session ID. Вразливості управління сесіями: фіксація сесії (session fixation), викрадення сесії (session hijacking). Cross-Site Request Forgery (CSRF) та методи захисту. Тестування на наявність небезпечних функцій запам'ятовування користувача. Аналіз механізмів logout та таймаутів сесій. Інструменти для тестування автентифікації: Burp Suite, Hydra, John the Ripper. Літ.: [1] с. 139-169, 183-207; [2] с.139-216; [3] с.46-51; | 2 |
| **5** | **Лекція 5. SQL ін'єкції та атаки на бази даних** Основи SQL та архітектура баз даних у вебдодатках. Що таке SQL ін'єкція та чому вона виникає. Типи SQL ін'єкцій: in-band (error-based, union-based), blind (boolean-based, time-based), out-of-band. Виявлення точок ін'єкції у вебдодатках. Експлуатація SQL ін'єкцій для читання даних, модифікації та видалення записів. Обхід механізмів автентифікації через SQL ін'єкції. Отримання доступу до файлової системи та виконання команд операційної системи. Автоматизація атак за допомогою SQLMap. NoSQL ін'єкції та їх | 2 |

| | | |
|---|---|---|
| | особливості. Методи захисту: параметризовані запити, ORM, валідація вхідних даних, принцип найменших привілеїв для БД. Інструменти для виявлення та експлуатації SQL ін'єкцій.<br>Літ.: [1] с. 157-160; 256-294; [2] с.217-276; [3] с.147-158; [12] с. 223-237 | |
| **6** | **Cross-Site Scripting (XSS) та атаки на клієнтську сторону**<br>Основи JavaScript та Document Object Model (DOM). Що таке Cross-Site Scripting та механізм виникнення вразливості. Типи XSS атак: reflected XSS, stored XSS, DOM-based XSS. Виявлення точок ін'єкції JavaScript коду у вебдодатках. Експлуатація XSS для викрадення cookies та session токенів. Модифікація контенту сторінки та фішингові атаки через XSS. Обхід фільтрів та механізмів захисту від XSS. Інструменти для автоматизації виявлення XSS: XSSer, BeEF. Cross-Site Request Forgery (CSRF) та його зв'язок з XSS. Clickjacking та UI redressing атаки. Content Security Policy (CSP) як механізм захисту. HTTPOnly та Secure flags для cookies. Методи санітизації вхідних даних та виходу. Практичні сценарії експлуатації XSS вразливостей.<br>Літ.: [1] с. 71-75; [2] с.281-333; [3] с.117-146; [4] с. 61-76; | 2 |
| **7** | **Тестування API та сучасних веб-архітектур**<br>Архітектура REST API та принципи RESTful дизайну. GraphQL API: особливості та відмінності від REST. Методи HTTP та їх безпечне використання. Автентифікація та авторизація в API: OAuth 2.0, JWT, API keys. Специфічні вразливості API: Broken Object Level Authorization (BOLA), Broken Function Level Authorization. Масове призначення (Mass Assignment) та його експлуатація. Lack of Resources & Rate Limiting атаки. Injection вразливості в API endpoints. OWASP API Security Top 10 2023. Тестування мікросервісної архітектури та serverless додатків. Захист API: rate limiting, input validation, proper authentication. Інструменти для тестування API: REST Client, Insomnia.<br>Літ.: [1] с. 115-123; [2] с.353-428; [3] с.77-84; [29] | 2 |
| **8** | **Лекція 8. Звітність, документування та методології виправлення вразливостей**<br>Структура професійного звіту про тестування на проникнення. Класифікація вразливостей за рівнем критичності: CVSS (Common Vulnerability Scoring System). Рекомендації щодо усунення вразливостей та best practices. Bug bounty програми: платформи, правила участі, етика. Continuous security testing та інтеграція безпеки в CI/CD. Інструменти для автоматизації тестування безпеки: SAST, DAST, IAST. Метрики безпеки та KPI для вимірювання ефективності. Побудова кар'єри в галузі тестування на проникнення та кібербезпеки.<br>Літ.: [1] с. 226-277; [3] с.225-235; [16]; [28] | 2 |
| | **Разом за семестр:** | **16** |

**5.2 Зміст лабораторних робіт (IV семестр)**

| № п/п | Теми лабораторних робіт | Кількість годин |
|---|---|---|
| **Тема 1. Основи безпеки вебдодатків та методології тестування на проникнення** | | **12** |
| **1** | Налаштування локального віртуального мережевого середовища<br>Мережева розвідка<br>Літ.: [4] с. 8-26; [5] с. 9-18; [13]; [17] [18]; [23]; [24] | 4 |
| **2** | Використання атак грубої сили та словникових атак<br>Літ.: [5] с. 19-27; [11] с. 8-135; | 4 |
| **3** | Використання інструментів автоматизованого пошуку вразливості<br>Літ.: [5] с. 28-35; [21, 22]; [25] | 4 |
| **Тема 2. Вебатаки та вразливості вебресурсів** | | **20** |
| **4** | Клієнтські ін'єкції скриптів. Міжсайтовий скриптинг. CSRF<br>Літ[5] с. 36-41 | 4 |
| **5** | Атаки на сесії<br>Літ.: [5] с. 42-46 | 4 |
| **6** | Атаки на бази даних. SQL-ін'єкції<br>Літ[5] с. 47-52; [12] с. 223-237 | 4 |

| | | |
|---|---|---|
| **7** | Атаки на API. Атаки десеріалізації. XML атаки<br>Літ.: [5] с. 53-57 | 4 |
| **8** | Атаки на комплексну вебінфраструктуру на основі мікросервісів<br>Літ.: [5] с. 58-64; [13] | 4 |
| **Підсумкове заняття** | | **2** |
| **9** | Тестування | 2 |
| | **Разом за семестр:** | **34** |

### 5.3 Зміст самостійної (у т.ч. індивідуальної) роботи

Самостійна робота студентів полягає у систематичному опрацюванні програмного матеріалу з відповідних джерел інформації, підготовці до виконання і захисту лабораторних робіт, підготовці до практичних занять, підготовці до тестування тощо. Керівництво самостійною роботою здійснюється викладачем згідно з розкладом консультацій у позаурочний час. Крім цього, до послуг студентів сторінка навчальної дисципліни у Модульному середовищі для навчання, де розміщені Робоча програма дисципліни та необхідні документи з її навчально-методичного забезпечення.

| **№ тижня** | **Теми самостійної роботи (VII семестр)** | **Кількість годин** |
|---|---|---|
| **1** | Опрацювання конспекту лекцій та теоретичного матеріалу лекції №1. Підготовка до лабораторної роботи №1. | 6 |
| **2** | Опрацювання конспекту лекцій та теоретичного матеріалу лекції №1. Виконання лабораторної роботи №1. | 6 |
| **3** | Опрацювання конспекту лекцій та теоретичного матеріалу лекції №2. Підготовка до лабораторної роботи №2. | 6 |
| **4** | Опрацювання конспекту лекцій та теоретичного матеріалу лекції №2. Виконання лабораторної роботи №2. | 6 |
| **5** | Опрацювання конспекту лекцій та теоретичного матеріалу лекції №3. Підготовка до лабораторної роботи №3. | 6 |
| **6** | Опрацювання конспекту лекцій та теоретичного матеріалу лекції №3. Виконання лабораторної роботи №3. | 6 |
| **7** | Опрацювання конспекту лекцій та теоретичного матеріалу лекції №4. Підготовка до лабораторної роботи №4. | 6 |
| **8** | Опрацювання конспекту лекцій та теоретичного матеріалу лекції №4. Виконання лабораторної роботи №4. | 6 |
| **9** | Опрацювання конспекту лекцій та теоретичного матеріалу лекції №5. Підготовка до лабораторної роботи №5. | 6 |
| **10** | Опрацювання конспекту лекцій та теоретичного матеріалу лекції №5. Виконання лабораторної роботи №5. | 6 |
| **11** | Опрацювання конспекту лекцій та теоретичного матеріалу лекції №6. Підготовка до лабораторної роботи №6. | 6 |
| **12** | Опрацювання конспекту лекцій та теоретичного матеріалу лекції №6. Виконання лабораторної роботи №6. | 6 |
| **13** | Опрацювання конспекту лекцій та теоретичного матеріалу лекції №7. Підготовка до лабораторної роботи №7. | 6 |
| **14** | Опрацювання конспекту лекцій та теоретичного матеріалу лекції №7. Виконання лабораторної роботи №7. | 6 |
| **15** | Опрацювання конспекту лекцій та теоретичного матеріалу лекції №8. Підготовка до лабораторної роботи №8. | 6 |
| **16** | Опрацювання конспекту лекцій та теоретичного матеріалу лекції №8. Виконання лабораторної роботи №8. | 6 |
| **17** | Підготовка до тестування за пройденим матеріалом. | 4 |
| | **Разом за семестр:** | 100 |

## 6. Технології та методи навчання

Процес навчання з дисципліни ґрунтується на використанні традиційних та сучасних методів. Зокрема, лекції проводяться з використанням словесних, наочних та проблемних методів з супроводом презентаційних матеріалів; лабораторні роботи – з використанням практичних, частково-пошукових та ігрових методів, із застосуванням сучасних інформаційно-комп'ютерних технологій; практичні заняття – з використанням практичних методів; самостійна робота (опрацювання теоретичного матеріалу, підготовка до виконання та захисту лабораторних робіт, практичних занять, тестування) – з використанням пояснювально-ілюстративних та дослідницьких методів, інформаційно-комп'ютерних технологій та технологій дистанційного навчання.

## 7. Методи контролю

Поточний контроль здійснюється під час лабораторних та практичних занять. а також у дні проведення контрольних заходів, встановлених робочою програмою і графіком освітнього процесу, в т.ч. з використанням Модульного середовища для навчання. При цьому використовуються такі методи поточного контролю:

- оцінювання результатів захисту лабораторних робіт;
- тестовий контроль.

При виведенні підсумкової семестрової оцінки враховуються результати як поточного, так і підсумкового контролів, який проводиться з усього матеріалу дисципліни за білетами, попередньо розробленими і затвердженими на засіданні кафедри. Здобувач вищої освіти, який набрав з будь-якого виду навчальної роботи, суму балів нижчу за 60 відсотків від максимального балу, ***не допускається*** до семестрового контролю поки не виконає весь обсяг, передбачений Робочою програмою для цього виду роботи. Здобувач вищої освіти, який набрав позитивний середньозважений бал (60 відсотків і більше від максимального балу, встановленого для кожної структурної одиниці) з усіх видів поточного контролю і не склав іспит, вважається таким, який ***має*** академічну заборгованість. Ліквідація академічної заборгованості із семестрового контролю здійснюється у період екзаменаційної сесії або за графіком,

встановленим деканатом відповідно до «Положення про контроль і оцінювання результатів навчання здобувачів вищої освіти у ХНУ».

## 8. Політика дисципліни

Політика навчальної дисципліни загалом визначається системою вимог до здобувача вищої освіти, що передбачені чинними положеннями Університету про організацію і навчально-методичне забезпечення освітнього процесу. Зокрема, проходження інструктажу з техніки безпеки; відвідування занять з дисципліни є обов'язковим. За об'єктивних причин (підтверджених документально) теоретичне навчання за погодженням із лектором може відбуватись в он-лайн режимі. Успішне опанування дисципліни і формування фахових компетентностей і програмних результатів навчання передбачає необхідність підготовки до лабораторних (вивчення теоретичного матеріалу з теми, попередню підготовку протоколу роботи, активно працювати на занятті, якісно підготувати звіт (відповідно до теми роботи), захистити результати виконаної роботи, брати участь у дискусіях щодо прийнятих конструктивних рішень при виконанні здобувачами лабораторних робіт тощо) та практичних занять (вивчення теоретичного матеріалу з теми, активно працювати на занятті, розв'язувати задачі, брати участь у дискусіях щодо прийнятих рішень при виконанні здобувачами задач).

Здобувачі вищої освіти зобов'язані дотримуватися термінів виконання усіх видів робіт у встановлені терміни, передбачених робочою програмою навчальної дисципліни. Термін захисту лабораторної роботи вважається своєчасним, якщо здобувач захистив її на наступному після виконання роботи занятті. Пропущене лабораторне або практичне заняття здобувач зобов'язаний відпрацювати в лабораторіях кафедри у встановлений викладачем термін, але не пізніше, ніж за два тижні до кінця теоретичних занять у семестрі.

Засвоєння здобувачем теоретичного матеріалу з дисципліни оцінюється за результатами тестування.

Здобувач вищої освіти, виконуючи лабораторні роботи, практичні завдання, тестування з дисципліни з дисципліни, має дотримуватися політики доброчесності (заборонені списування, плагіат (в т.ч. із використанням мобільних девайсів)). У разі виявлення плагіату в будь-яких видах навчальної роботи здобувач вищої освіти отримує незадовільну оцінку і має повторно виконати завдання з відповідної теми (виду роботи), що передбачені робочою програмою. Будь-які форми порушення академічної доброчесності ***не допускаються.***

*У* межах вивчення навчальної дисципліни здобувачам вищої освіти передбачено визнання і зарахування результатів навчання, набутих шляхом неформальної освіти, що розміщені на доступних платформах (за наявності такого переліку, доцільно вказати рекомендовані курси), які сприяють формування компетентностей і поглибленню результатів навчання, визначених робочою програмою дисципліни, або забезпечують вивчення відповідної теми та/або виду робіт з програми навчальної дисципліни (детальніше у Положенні про порядок визнання та зарахування результатів навчання здобувачів вищої освіти у ХНУ).

## 9. Оцінювання результатів навчання здобувачів освіти

Оцінювання академічних досягнень здобувача вищої освіти здійснюється відповідно до «Положення про контроль і оцінювання результатів навчання здобувачів вищої освіти у ХНУ». Залежно від важливості окремих видів навчальної роботи, і їх ролі у формуванні компетентностей і результатів навчання, визначених освітньою програмою, розробники Робочої програми присвоюють кожному виду навчальної роботи (структурній одиниці) з дисципліни певну кількість балів. При поточному оцінюванні виконаної здобувачем роботи з кожної структурної одиниці і отриманих ним результатів викладач виставляє йому певну кількість балів із встановлених Робочою програмою для цього виду роботи. При цьому кожна структурна одиниця навчальної роботи може бути зарахована, якщо здобувач набрав не менше 60 відсотків (мінімальний рівень для позитивної оцінки) від максимально можливої суми балів, призначеної структурній одиниці.

Будь-які форми порушення академічної доброчесності ***не допускаються***.

При оцінюванні результатів навчання здобувачів вищої освіти з будь-якого виду навчальної роботи (структурної одиниці) рекомендується використовувати наведені нижче узагальнені критерії:

**Таблиця – Критерії оцінювання навчальних досягнень здобувача вищої освіти**

| **Оцінка та рівень досягнення здобувачем запланованих ПРН та сформованих компетентностей** | **Узагальнений зміст критерія оцінювання** |
|---|---|
| Відмінно (високий) | Здобувач вищої освіти глибоко і у повному обсязі опанував зміст навчального матеріалу, легко в ньому орієнтується і вміло використовує понятійний апарат; уміє пов'язувати теорію з практикою, вирішувати практичні завдання, впевнено висловлювати і обґрунтовувати свої судження. Відмінна оцінка передбачає логічний виклад відповіді мовою викладання (в усній або у письмовій формі), демонструє якісне оформлення роботи і володіння спеціальними прикладними програмами. Здобувач не вагається при видозміні запитання, вміє робити детальні та узагальнюючі висновки, демонструє практичні навички з вирішення фахових завдань. При відповіді допустив дві–три несуттєві ***похибки***. |
| Добре (середній) | Здобувач вищої освіти виявив повне засвоєння навчального матеріалу, володіє понятійним апаратом, орієнтується у вивченому матеріалі; свідомо використовує теоретичні знання для вирішення практичних задач; виклад відповіді грамотний, але у змісті і формі відповіді можуть мати місце окремі неточності, нечіткі формулювання правил, закономірностей тощо. Відповідь здобувача вищої освіти будується на основі самостійного мислення. Здобувач вищої освіти у відповіді допустив дві–три ***несуттєві помилки***. |
| Задовільно | Здобувач вищої освіти виявив знання основного програмного матеріалу в обсязі, |

| | |
|---|---|
| (достатній) | необхідному для подальшого навчання та практичної діяльності за професією, справляється з виконанням практичних завдань, передбачених програмою. Як правило, відповідь здобувача вищої освіти будується на рівні репродуктивного мислення, здобувач вищої освіти має слабкі знання структури навчальної дисципліни, допускає неточності і ***суттєві помилки*** у відповіді, вагається при відповіді на видозмінене запитання. Разом з тим, набув навичок, необхідних для виконання нескладних практичних завдань, які відповідають мінімальним критеріям оцінювання і володіє знаннями, що дозволяють йому під керівництвом викладача усунути неточності у відповіді. |
| Незадовільно (недостатній) | Здобувач вищої освіти виявив розрізнені, безсистемні знання, не вміє виділяти головне і другорядне, допускається помилок у визначенні понять, перекручує їх зміст, хаотично і невпевнено викладає матеріал, не може використовувати знання при вирішенні практичних завдань. Як правило, оцінка «незадовільно» виставляється здобувачеві вищої освіти, який не може продовжити навчання без додаткової роботи з вивчення навчальної дисципліни. |

**Структурування дисципліни за видами навчальної роботи і оцінювання результатів навчання здобувачів у VII семестрі**

| **Аудиторна робота** | | | | | | | | **Контрольні заходи** | **Семестровий контроль** |
|---|---|---|---|---|---|---|---|---|---|
| Лабораторні роботи (мінімум 8 контрольних точок) | | | | | | | | Тестовий контроль: | Залік |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | Т 1, 2 | |
| Кількість балів за вид навчальної роботи (мінімум-максимум) | | | | | | | | | |
| 6-10 | 6-10 | 6-10 | 6-10 | 6-10 | 6-10 | 6-10 | 6-10 | 12-20 | За рейтингом |
| **48-80** | | | | | | | | **12-20** | **60-100*** |

***Примітки***: Т – тема навчальної дисципліни;

*За набрану з будь-якого виду роботи (дисципліни) кількість балів нижче встановленого мінімуму здобувач отримує незадовільну оцінку і має її перездати у встановлений викладачем (деканом) термін. Інституційна оцінка встановлюється відповідно до таблиці «**Співвідношення інституційної шкали оцінювання і шкали оцінювання ЄКТС»**.

**Оцінювання результатів захисту лабораторної роботи**

Виконана й оформлена відповідно до встановлених Методичними рекомендаціями вимог лабораторна робота комплексно оцінюється викладачем при її захисті з урахуванням таких критеріїв: самостійність та правильність виконання; якість оформлення звіту; вільне володіння здобувачем спеціальною термінологією і уміння професійно обґрунтувати прийняті конструктивні рішення.

Результат виконання і захисту здобувачем вищої освіти кожної лабораторної роботи оцінюється відповідно до таблиці Критеріїв оцінювання навчальних досягнень здобувача вищої освіти та рівня досягнення здобувачем запланованих ПРН та сформованих компетентностей з присвоєнням йому відповідної суми балів.

У випадку виявлення здобувачем рівня знань, нижчого ніж 60 відсотків від максимального балу, встановленого Робочою програмою для кожної структурної одиниці, лабораторна робота йому ***не зараховується*** і для її захисту він має детальніше опрацювати матеріал з теми роботи, методику її виконання, виправити грубі помилки та повторно вийти на її захист у призначений для цього викладачем час.

## Оцінювання результатів тестового контролю

Тест, передбачений Робочою програмою, складається із 20 тестових завдань, кожне з яких є рівнозначним. Максимальна сума балів, яку може набрати здобувач, складає 20.

Відповідно до таблиці структурування видів робіт за тематичний контроль здобувач залежно від кількості правильних відповідей може отримати від 12 до 20 балів.

**Розподіл балів в залежності від наданих правильних відповідей на тестові завдання**

| Кількість правильних відповідей | 0-11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
|---|---|---|---|---|---|---|---|---|---|---|
| Відсоток правильних відповідей | 0-59 | 60 | 65 | 70 | 75 | 80 | 85 | 90 | 95 | 100 |
| Кількість отриманих балів | 0 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |

На тестування відводиться 20 хвилин. Правильні відповіді записуються у талоні відповідей. Здобувач може також пройти тестування і в он-лайн режимі у Модульному середовищі для навчання.

**Семестровий залік** виставляється на останньому занятті за умови якщо загальна сума балів, яку накопичив здобувач з дисципліни (іншого освітнього компонента) за результатами ***поточного*** контролю, знаходиться у межах від 60 до 100 балів. При цьому за інституційною шкалою ставиться оцінка «***зараховано***», а за шкалою ЄКТС – буквене позначення оцінки, що відповідає набраній студентом сумі балів відповідно до таблиці Співвідношення. Присутність здобувача у цьому випадку не є обов'язковою.

**Таблиця – Співвідношення інституційної шкали оцінювання і шкали оцінювання ЄКТС**

| **Оцінка ЄКТС** | **Рейтингова шкала балів** | **Інституційна оцінка** (рівень досягнення здобувачем вищої освіти запланованих результатів навчання з навчальної дисципліни) | |
|---|---|---|---|
| | | **Залік** | **Іспит/диференційований залік** |
| A | 90-100 | Зараховано | ***Відмінно*/*Excellent*** – високий рівень досягнення запланованих результатів навчання з навчальної дисципліни, що свідчить про безумовну готовність здобувача до подальшого навчання та/або професійної діяльності за фахом |
| B | 83-89 | | ***Добре*/*Good*** – середній (максимально достатній) рівень досягнення запланованих результатів навчання з навчальної дисципліни та готовності до подальшого навчання та/або професійної діяльності за фахом<br><br>***Задовільно*/*Satisfactory*** – Наявні мінімально достатні для подальшого навчання та/або професійної діяльності за фахом результати навчання з навчальної дисципліни |
| C | 73-82 | | |
| D | 66-72 | | |
| E | 60-65 | | |
| FX | 40-59 | Незараховано | ***Незадовільно*/*Fail*** – Низка запланованих результатів навчання з навчальної дисципліни відсутня. Рівень набутих результатів навчання є недостатнім для подальшого навчання та/або професійної діяльності за фахом |
| F | 0-39 | | ***Незадовільно*/*Fail*** – Результати навчання відсутні |

**10. Питання для самоконтролю результатів навчання**

1. Протокол передачі гіпертексту.
2. HTTP-запити та відповіді, методи та повідомлення.
3. Кукі.
4. HTTPS (протокол передачі гіпертексту через захищені сокети).
5. Протокол SSL (Secure Sockets Layer).
6. Симетричне та асиметричне шифрування.
7. Перехоплення проксі та HTTPS.
8. Використання протоколу простого доступу до об’єктів (SOAP).
9. Протокол SMTP (Simple Mail Transfer Protocol).
10. Протокол поштового відділення (POP3).
11. Протокол доступу до Інтернету (IMAP).
12. Архітектура вебсистем і вебдодатків.
13. Об’єкти захисту/атаки.
14. Класифікація веб-атак (уразливості).
15. Груба сила (Brute Force).
16. Недостатня аутентифікація.
17. Недостатнє відновлення пароля (перевірка слабкого відновлення пароля).
18. Прогнозування вхідних даних/сеансів.
19. Недостатня авторизація.
20. Недостатнє закінчення сеансу.
21. Фіксація сеансу.
22. Викрадення сеансу.
23. Перехресні сценарії (XSS).
24. Сценарії крос-кадрів (XFS) або iframe-ін’єкція.
25. Підробка запитів на місцях CSRF.
26. Зловживання JSON.
27. Переповнення буфера.
28. LDAP-ін’єкція.
29. SQL-ін’єкція.
30. SSI-ін’єкція.
31. XPath-ін’єкція.
32. Індексування каталогів.
33. Витоки інформації.
34. Пошук шляху (трасування).
35. Передбачуване розташування ресурсів.
36. Забезпечення технологій вебдодатків (SWAT).
37. Обробка помилок та ведення журналу.
38. Аутентифікація.
39. Обробка вхідних і вихідних даних.
40. Конфігурація та операції.
41. Управління сеансами.
42. Контроль доступу.
43. Проект тестування OWASP.
44. Принципи тестування.
45. Пояснення техніки тестування.
46. Виведення вимог до тестування безпеки.
47. Тести безпеки, інтегровані в робочі процеси розробки та тестування.
48. Аналіз і звітність тестових даних безпеки.
49. Інструменти тестування.
50. Основні поняття аудиту вебдодатків.
51. Методика організації та проведення аудиту вебдодатків.
52. Призначення проксі-серверів.

53.Типи проксі-серверів.
54. Реалізації проксі серверів та їх характеристики

## 11. Методичне забезпечення

Освітній процес з дисципліни «Безпека вебресурсів» забезпечений необхідними навчально-методичними матеріалами, що розміщені в Модульному середовищі для навчання MOODLE:

1. Курс «Безпека вебресурсів»: https://msn.khmnu.edu.ua/course/view.php?id=6795.

## 12. Матеріально-технічне та програмне забезпечення

Інформаційна та комп'ютерна підтримка: ПК, ноутбук, планшет, смартфон або інший мобільний пристрій, проєктор, доступ до мережі Інтернет, робота з презентаціями.

Спеціальне та прикладне програмне забезпечення: OS Kali Linux, OS Ubuntu, OS MS Windows 10 або вище, Oracle Virtual Box, Nmap (Zenmap), MS Visual Studio 22 або вище, theHarvester, Shodan, Maltego, Burp Suite, Hydra, John the Ripper, REST Client тощо.

## 13. Рекомендована література

### Основна


1. Пірог О. В. Безпека вебдодатків : навчальний посібник. Житомир : Житомирська політехніка, 2025. 290 с.
2. Open Web Application Security Project. Web security testing guide. Version 4.2 [Електронний ресурс]. 2024. URL: https://owasp.org/www-project-web-security-testing-guide/ (дата звернення: 19.08.2025).
3. Hoffman A. Web application security: exploitation and countermeasures for modern web applications. 2nd ed. Beijing : O'Reilly Media, 2020. 331 p.
4. Живило Є. О. Тестування на проникнення : навчальний посібник. Ч. 1. Полтава : ПНТУ, 2024. 134 с.
5. Безпека вебресурсів : лабораторний практикум з дисципліни для здобувачів першого (бакалаврського) рівня вищої освіти спеціальності «Кібербезпека та захист інформації» / І. В. Муляр, В. М. Джулій, В. А. Анікін, О. А. Зарицька. Хмельницький : ХНУ, 2025. 67 с.


### Додаткова


6. Інформаційні мережі: навчальний посібник / Ю. В. Коваль, А. Б. Ставровський. Київ, 2021. 84 с.
7. Комплексна безпека інформаційних мережевих систем: навчальний посібник/ Укладачі: А.Г. Микитишин, М.М. Митник, О.С. Голотенко, В.В. Карташов. Тернопіль: ФОП Паляниця В.А., 2023. 324 с.
8. Опановуємо Burp Suite, незамінний інструмент для пентестерів [Електронний ресурс]. URL: https://hackyourmom.com/osvita/opanovuyemo-burp-suite-nezaminnyj-instrument-dlya-pentesteriv/ (дата звернення: 19.07.2025).
9. Основи безпеки веб-сайтів [Електронний ресурс]. URL: https://www.godaddy.com/uk-ua/how-to/osnovi-bezpeki-veb-sajtiv/ (дата звернення: 16.08.2025).
10. Довбиш А. С., Ободяк В. К., Шелехов І. В. Сучасні інформаційні технології в кібербезпеці. Суми : СДУ, 2021. С. 317–329.
11. Живило Є. О. Тестування на проникнення : навчальний посібник. Ч. 2. Полтава : ПНТУ, 2024. 239 с.
12. Євсеєв С. П., Ткачов А. М., Алексієв В. О., Рябуха Ю. М. Кібербезпека: WEB-технології [Електронний ресурс] : навчально-довідковий посібник. Харків : ХНЕУ ім. С. Кузнеця ; Львів : Новий Світ – 2000, 2021. 390 с.
13. WEB-технології [Електронний ресурс] : лабораторний практикум : навчальний посібник для здобувачів ступеня бакалавра за освітньою програмою «Автоматизація та комп'ютерно-інтегровані технології кіберенергетичних систем» спеціальності 151 «Автоматизація та комп'ютерно-інтегровані технології» / КПІ ім. Ігоря Сікорського ; уклад. О. С. Бунке. 2-ге вид. Київ : КПІ ім. Ігоря Сікорського, 2022. 60 с. 1 електрон. опт. диск (CD-ROM) ; 12 см. Назва з титул. екрана.
14. Information Security Handbook/ Noor Zaman Jhanjhi, Khalid Hussain, Mamoona Humayun, Azween Bin Abdullah, João Manuel R.S. Tavares. CRC Press, 2022. 250 p.
15. Seitz J., Arnold T. Black Hat Python. 2nd ed. San Francisco : No Starch Press, 2021. 188 p.
16. Khamis A. Optimization algorithms: AI techniques for design, planning, and control problems. Shelter Island : Manning Publications, 2024. 669 p.
17. Лєнков С., Джулій В., Муляр І., Димбовський М. Модель визначення актуальних загроз безпеки конфіденційних даних в розподіленій інформаційній системі. Underwater Technologies: Industrial and Civil Engineering. 2023. Issue 13. С. 45–59.
18. Джулій В., Муляр І., Зацепіна О., Пічура В. Інформаційно-ознакова модель джерела шкідливої інформації в соціальних мережах. Вимірювальна та обчислювальна техніка в технологічних процесах. 2022. № 3. С. 73–78. URL: https://vottp.khmnu.edu.ua/index.php/vottp/article/view/62/62 (дата звернення: 19.10.2025).

19. Джулій В. М., Кльоц Ю. П., Муляр І. В., Жилевич М. Л., Джулій А. В. Контроль додатків інтернет-трафіка комп'ютерних мереж методами машинного навчання. Вісник Хмельницького національного університету. Серія: Технічні науки. 2021. № 5. С. 22–36. DOI: 10.31891/2307-5732-2021-301-5-22-26

20. Лєнков С. В., Джулій В. М., Берназ А. М., Муляр І. В., Пампуха І. В. Метод прогнозування вразливостей інформаційної безпеки на основі аналізу даних тематичних інтернет-ресурсів. Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. Київ : ВІКНУ, 2023. Вип. 78. С. 123–133.

21. Муляр І. В., Зейлик Р. Ю., Житнік Р. Л., Футорний Р. В. Аналіз підходів до побудови системи сканування хостів і портів для аналізу вразливостей мережі з веб-інтерфейсом, збереження та обробкою даних. Військова освіта і наука: сьогодення та майбутнє : зб. тез доп. XX Міжнар. наук.-практ. конф., Київ, 29 листоп. 2024 р. Київ : ВІКНУ, 2024. Т. 1. С. 50–51.

22. Муляр І. В., Лєнков С. В., Гловюк В. С., Анікін В. А., Сотніков Є. О. Метод пошуку вразливостей вебзастосунків з використанням API ChatGPT. Smart Technologies: Industrial and Civil Engineering. 2024. Issue 1 (14). С. 46–55

23. Kali documentation. [Електронний ресурс]. URL: https://www.kali.org/docs/ (дата звернення: 19.08.2025).

24. Kali tools. [Електронний ресурс]. URL: https://www.kali.org/tools/ (дата звернення: 19.08.2025).

25. Shodan. [Електронний ресурс]. URL: https://www.shodan.io/ (дата звернення: 19.08.2025).

26. PTES. [Електронний ресурс]. URL: http://www.pentest-standard.org/index.php/Main_Page (дата звернення: 20.08.2025).

27. OWASP Top Ten. [Електронний ресурс]. URL: https://owasp.org/www-project-top-ten/ (дата звернення: 18.08.2025).

28. Common Vulnerability Scoring System Calculator. [Електронний ресурс]. URL: https://nvd.nist.gov/vuln-metrics/cvss/v4-calculator/ (дата звернення: 18.08.2025).

29. OWASP API Security Top 10 2023. [Електронний ресурс]. URL: https://owasp.org/API-Security/editions/2023/en/0x11-t10/ (дата звернення: 21.08.2025).

**14. Інформаційні ресурси**

1. Модульне середовище для навчання. URL : https://msn.khmnu.edu.ua/course/view.php?id=6795
2. Електронна бібліотека ХНУ. URL: http://lib.khmnu.edu.ua/
3. Інституційний репозитарій ХНУ. URL : https://library.khmnu.edu.ua/

# БЕЗПЕКА ВЕБРЕСУРСІВ

| | |
|---|---|
| **Тип дисципліни** | Обов'язкова |
| **Рівень вищої освіти** | Перший (бакалаврський) |
| **Мова викладання** | Українська |
| **Семестр** | четвертий |
| **Кількість встановлених кредитів ЄКТС** | 5 |
| **Форми здобуття освіти, для яких викладається дисципліна** | Очна (денна) |

**Результати навчання.** Після вивчення дисципліни студент повинен: *реалізовувати* заходи з протидії отриманню несанкціонованого доступу до вебресурсів в інформаційних та інформаційно-телекомунікаційних системах; *використовувати* сучасні методи та моделі інформаційної безпеки та/або кібербезпеки, теорії та методи захисту для забезпечення безпеки вебресурсів, як елементів інформаційно-телекомунікаційних систем; *застосовувати* сучасні технології захисту інформаціїм *реагувати* на кіберінциденти; *аналізувати* загрози; *забезпечувати* відновлення систем.

**Зміст навчальної дисципліни.** Основи управління ІБ. Правила управління ІБ. Політики інформаційної безпеки. Системи Безпека вебресурсів (СУІБ). Основи та поняття СУІБ. Вимоги до СУІБ. Розробка СУІБ. Моніторинг ІБ та SIEM. Розуміння інцидентів кібербезпеки. Організація реагування та розслідування кіберінцидентів. Структура групи реагування на інциденти. Життєвий цикл атаки (Kill Chain). Опрацьовування інциденту. Координація та обмін інформацією. Відновлення функціонування ІКС. Організаційно-технічні заходи відновлення функціонування ІКС. Резервування ресурсів ІКС та резервне зберігання даних.

**Пререквізити**: ОПП.01 Основи інформаційної безпеки, ОПП.02 Операційні системи та технології їх захисту

**Постреквізити:** ОПП.15 Виробнича практика 1, ОПП.16 Виробнича практика 2.

**Запланована навчальна діяльність**: Мінімальний обсяг навчальних занять в одному кредиті ЄКТС навчальної дисципліни для першого (бакалаврського) рівня вищої освіти за денною формою здобуття освіти становить 10 годин на 1 кредит ЄКТС.

**Форми (методи) навчання:** лекції (з використанням словесних, наочних та проблемних методів з супроводом презентаційних матеріалів);; самостійна робота (з використанням пояснювально-ілюстративних та дослідницьких методів).

**Форми оцінювання результатів навчання**: оцінювання результатів захисту лабораторних робіт; тестовий контроль.

**Вид семестрового контролю:** залік**.**

**Навчальні ресурси:**


1. Пірог О. В. Безпека вебдодатків : навчальний посібник. Житомир : Житомирська політехніка, 2025. 290 с.
2. Open Web Application Security Project. Web security testing guide. Version 4.2 [Електронний ресурс]. 2024. URL: https://owasp.org/www-project-web-security-testing-guide/ (дата звернення: 19.08.2025).
3. Hoffman A. Web application security: exploitation and countermeasures for modern web applications. 2nd ed. Beijing : O'Reilly Media, 2020. 331 p.
4. Живило Є. О. Тестування на проникнення : навчальний посібник. Ч. 1. Полтава : ПНТУ, 2024. 134 с.
5. Безпека вебресурсів : лабораторний практикум з дисципліни для здобувачів першого (бакалаврського) рівня вищої освіти спеціальності «Кібербезпека та захист інформації» / І. В. Муляр, В. М. Джулій, В. А. Анікін, О. А. Зарицька. Хмельницький : ХНУ, 2025. 67 с.
6. Модульне середовище для навчання. Доступ до ресурсу: https://msn.khmnu.edu.ua/course/view.php?id=6795
7. Електронна бібліотека ХНУ. Доступ до ресурсу: http://lib.khmnu.edu.ua


**Викладач**: канд. техн. наук, доцент Ігор Муляр.