МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

МІЖНАРОДНИЙ ГУМАНІТАРНИЙ УНІВЕРСИТЕТ

Кафедра комп'ютерної інженерії та інноваційних технологій

«ЗАТВЕРДЖУЮ»

Ректор Міжнародного гуманітарного університету д.ю.н., професор

_____ Костянтин ГРОМОВЕНКО

«29» серпня 2025 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ОСНОВИ WEB-БЕЗПЕКИ

Галузь знань	12 Інформаційні технології
Спеціальність	125 Кібербезпека та захист інформації
Назва освітньої програми	Кібербезпека
Рівень вищої освіти	перший (бакалаврський) рівень

Одеса - 2025 рік

Робоча програма затверджена на засіданні кафедри комп'ютерної інженерії та інноваційних технологій протокол № 1 від 28 серпня 2025 року.

Розробники і викладачі	Контактний тел.	E-mail
Професор кафедри комп'ютерної інженерії та інноваційних технологій **Радівілова Тамара Анатоліївна**	+380951609153	tamara.radivilova@gmail.com

Завідувач кафедри комп'ютерної інженерії
та інноваційних технологій
к.т.н., доцент _____ Лариса ЙОНА

Гарант освітньої програми
к.т.н., доцент _____ Лариса ЙОНА

Узгоджено
Начальник навчального відділу _____ Лілія САЄНКО

1. ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

<table>
<tr><th rowspan="2">Найменування показників</th><th rowspan="2">Галузь знань, напрям підготовки, освітньо-кваліфікаційний рівень</th><th colspan="2">Характеристика навчальної дисципліни</th></tr>
<tr><th>денна форма навчання</th><th>заочна форма навчання</th></tr>
<tr><td rowspan="10">Кількість кредитів – 3

Загальна кількість годин – 90</td><td rowspan="2">Галузь –
12 Інформаційні технології</td><td colspan="2">обов’язкова</td></tr>
<tr><td rowspan="9">Спеціальність –
125 Кібербезпека та захист інформації</td><td colspan="2">Рік підготовки:</td></tr>
<tr><td colspan="2">3-й</td></tr>
<tr><td colspan="2">Семестр</td></tr>
<tr><td>6-й</td><td>6-й</td></tr>
<tr><td colspan="2">Лекції</td></tr>
<tr><td rowspan="9">Мова навчання – українська</td><td rowspan="9">Рівень вищої освіти – перший (бакалаврський) рівень</td><td>14 год.</td><td>4 год.</td></tr>
<tr><td colspan="2">Практичні, семінарські</td></tr>
<tr><td>6 год.</td><td>2 год.</td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td>20 год.</td><td>2 год.</td></tr>
<tr><td colspan="2">Самостійна робота та індивідуальні завдання</td></tr>
<tr><td>50 год.</td><td>82 год.</td></tr>
<tr><td colspan="2">Вид контролю:</td></tr>
<tr><td>Залік</td><td>Залік</td></tr>
</table>

Дисципліна «Основи Web-безпеки» присвячена вивченню теоретичних основ та практичних методів забезпечення захищеності веб-додатків, мережевих сервісів та інфокомунікаційних систем від сучасних кіберзагроз. Дисципліна охоплює широкий спектр питань, пов'язаних із аналізом загроз, проєктуванням захищених веб-рішень, застосуванням криптографічних та організаційних заходів безпеки, а також методами тестування та аудиту веб-ресурсів.

Метою дисципліни «Основи Web-безпеки» є формування у здобувачів вищої освіти цілісного уявлення про природу веб-вразливостей, розвиток практичних навичок проєктування безпечних веб-додатків, застосування превентивних заходів захисту на етапах розробки та експлуатації, а також проведення базового аудиту безпеки. Дисципліна спрямована на набуття компетентностей з аналізу загроз, нейтралізації векторів атак, налаштування механізмів авторизації, використання засобів криптографічного захисту у веб-середовищі та впровадження практик безпечної розробки (Secure SDLC).

Курс передбачає поєднання теоретичних лекцій, практичних занять у віртуалізованому лабораторному середовищі, самостійне опрацювання навчальних матеріалів та виконання індивідуальних завдань, спрямованих на закріплення навичок виявлення та усунення вразливостей у навчальних веб-додатках.

ПРЕРЕКВІЗИТИ. Передумовами є знання з Web-технологій («Web-технології», ОК 14), комп'ютерних мереж («Комп'ютерні мережі», ОК 13), захисту інформації в мережах («Захист інформації в інфокомунікаційних системах та мережах», ОК 12) та операційних систем («Операційні системи», ОК 20).

ПОСТРЕКВІЗИТИ. Знання та навички з Web-безпеки є важливими при вивченні «Безпеки програм та даних» (ОК 16), «Комплексних систем захисту інформації» (ОК 24), «Управління інформаційною та кібербезпекою» (ОК 30), «Основ цифрової криміналістики» (ОК 26) та «Етичного хакінгу та тестування на проникнення» (ОК 18), а також при виробничій практиці (ОК 34) і захисті кваліфікаційної роботи (ОК 36).

2. ОЧІКУВАНІ КОМПЕТЕНТНОСТІ, ЯКІ ПЛАНУЄТЬСЯ СФОРМУВАТИ ТА ДОСЯГНЕННЯ ПРОГРАМНИХ РЕЗУЛЬТАТІВ

У процесі реалізації програми дисципліни «Основи Web-безпеки» формуються наступні компетентності із передбачених освітньою програмою:

Інтегральна компетентність

ІК. Здатність розв’язувати складні спеціалізовані задачі та практичні проблеми у галузі кібербезпеки та захисту інформації.

Загальні компетентності (ЗК)

ЗК1. Здатність застосовувати знання у практичних ситуаціях.

ЗК 2. Знання та розуміння предметної області та розуміння професійної діяльності

Спеціальні (фахові, предметні) компетентності

СК 4. Здатність забезпечувати захист інформації в інформаційних та інформаційно-комунікаційних системах згідно встановленої політики кібербезпеки й захисту інформації.

СК 10. Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.

Навчальна дисципліна «Основи Web-безпеки» забезпечує досягнення програмних результатів навчання (РН), передбачених освітньою програмою:

РН 6. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат.

РН 12. Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки.

РН 13. Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних і програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних й інформаційно-комунікаційних систем та/або інфраструктури організації в цілому.

РН 21. Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору й інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.

Заплановані результати навчання за навчальною дисципліною

Знання:

1 На концептуальному рівні — фундаментальні принципи безпеки веб-додатків та мережевих сервісів, архітектуру клієнт-серверної взаємодії (HTTP/HTTPS, cookies, сесії), модель загроз для веб-ресурсів, класифікацію вразливостей (OWASP Top 10, CWE) та принципи безпечного проєктування (Secure by Design).

2 Структуру та механізми ключових компонентів захисту веб-середовища: методи аутентифікації та авторизації (OAuth 2.0, OIDC, JWT, MFA), управління сесіями, захист від ін'єкційних атак (SQL, NoSQL, Command) та міжсайтового скриптингу (XSS), налаштування заголовків безпеки (CSP, HttpOnly).

3 Сучасні підходи до управління безпекою веб-ресурсів: безпеку API (REST, GraphQL), DevSecOps-підходи (інтеграція перевірок у CI/CD), методики тестування (SAST/DAST), вимоги до конфігурації серверів та хмарних сервісів, перспективи використання AI/ML для виявлення аномалій.

Уміння:

4. Аналізувати архітектуру веб-додатків та інфокомунікаційних систем з метою виявлення вразливостей, оцінювати рівень захищеності на основі аналізу коду, конфігурацій та результатів аудиту за методиками OWASP Testing Guide.

5. Обґрунтовано вибирати та інтегрувати технічні засоби захисту (WAF, механізми криптографічного захисту, системи управління доступом) залежно від специфіки веб-додатку та вимог політики інформаційної безпеки.

6. Оцінювати ефективність захисних механізмів проти типових веб-атак (ін'єкції, XSS, CSRF, IDOR), прогнозувати наслідки помилок бізнес-логіки та некоректного управління сесіями або обліковими даними.

7. Розробляти комплексні заходи з підвищення рівня захищеності, враховуючи взаємозв'язок організаційних, технічних та програмних компонентів системи захисту інформації на етапах розробки та експлуатації (Secure SDLC).

Навички:

8. Ефективно застосовувати сучасні інструменти тестування безпеки веб-додатків (Burp Suite, OWASP ZAP, Nikto) у віртуалізованому середовищі для виявлення та усунення вразливостей.

9. Виконувати моніторинг подій безпеки веб-систем, аналізувати логи для виявлення інцидентів, збирати дані для аудиту безпеки та реалізовувати заходи з нейтралізації векторів атак.

10. Працювати з автоматизованими засобами перевірки безпеки в піплайнах CI/CD, забезпечуючи постійну підтримку захищеного стану веб-додатків та API у відповідності до вимог сучасних стандартів кібербезпеки.

3. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Тема 1. Архітектура веб-безпеки та моделювання загроз.

Поняття веб-безпеки в контексті сучасних кіберзагроз. Архітектура клієнт-серверної взаємодії: HTTP/HTTPS, cookies, сесії, заголовки безпеки. Модель загроз для веб-додатків. Класифікація вразливостей (OWASP Top 10, CWE). Принципи безпечного проєктування (Secure by Design).

Тема 2. Захист від ін'єкційних атак.

Природа та механізми ін'єкцій: SQL/NoSQL-ін'єкції, Command Injection, LDAP Injection. Методи виявлення та аналізу вразливостей. Превентивні заходи: параметризовані запити, підготовлені вирази, валідація та санітизація вхідних даних, використання ORM-фреймворків. Налаштування WAF (Web Application Firewall) для захисту від ін'єкцій.

Тема 3. Захист від міжсайтового скриптингу та клієнтських атак.

Типи XSS-атак (відображуваний, збережений, DOM-based). Вектори атак через JavaScript та HTML-ін'єкції. Методи нейтралізації: екранування виводу, Content Security Policy (CSP), HttpOnly/Secure прапорці для cookies, санітизація даних на клієнті та сервері. Захист від CSRF-атак: токени, SameSite-атрибути.

Тема 4. Безпечна аутентифікація, авторизація та управління сесіями.

Механізми аутентифікації: паролі, OAuth 2.0, OpenID Connect, JWT. Вимоги до політики паролів та зберігання облікових даних (хешування, сіль). Безпечне управління сесіями: ротація ідентифікаторів, тайм-аути, захист від фіксації сесії. Багатофакторна автентифікація (MFA) у веб-додатках.

Тема 5. Безпека конфігурації та захист від логічних вразливостей.

Типові помилки конфігурації серверів, фреймворків, хмарних сервісів. Вразливості бізнес-логіки: обхід оплати, маніпуляція параметрами, IDOR (Insecure Direct Object Reference), недостатній контроль доступу. Методи запобігання: принцип найменших привілеїв, регулярний аудит конфігурацій, автоматизоване сканування налаштувань.

Тема 6. Інструменти та методики тестування безпеки веб-додатків.

Огляд інструментів: Burp Suite Community, OWASP ZAP, Nikto. Методики ручного та автоматизованого тестування. Статичний (SAST) та динамічний (DAST) аналіз коду.

Використання OWASP Testing Guide для структурованого аудиту. Побудова звітів про вразливості та пріоритезація виправлень.

Тема 7. Сучасні підходи до комплексного захисту веб-ресурсів.

Безпека API (REST, GraphQL): аутентифікація, лімітування запитів, валідація схем. Захист SPA (Single Page Applications) та PWA. DevSecOps-підходи: інтеграція перевірок безпеки в CI/CD-пайплайни. Моніторинг та логування подій безпеки. Перспективи: використання AI/ML для виявлення аномалій, підготовка до постквантової криптографії.

4. СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Назви змістових модулів і тем	Кількість годин									
	денна форма					Заочна форма				
	усього	у тому числі				усього	у тому числі			
		лекц.	лаб.	прак.	сам. роб.		лекц.	лаб.	прак.	сам роб.
Тема 1. Архітектура веб-безпеки та моделювання загроз.	12	2	2	2	6	12	2			10
Тема 2. Захист від ін'єкційних атак.	14	2	4		8	12				12
Тема 3. Захист від міжсайтового скриптингу та клієнтських атак.	14	2	4		8	14		2		12
Тема 4. Безпечна аутентифікація, авторизація та управління сесіями.	12	2	2	2	6	14	2			12
Тема 5. Безпека конфігурації та захист від логічних вразливостей.	12	2	2		8	14			2	12
Тема 6. Інструменти та методики тестування безпеки веб-додатків.	14	2	4		8	12				12
Тема 7. Сучасні підходи до комплексного захисту веб-ресурсів.	12	2	2	2	6	12				12
Усього годин	**90**	**14**	**20**	**6**	**50**	**90**	**4**	**2**	**2**	**82**
ПІДСУМКОВИЙ КОНТРОЛЬ – ЗАЛІК										

5. ПИТАННЯ ДО ПРАКТИЧНИХ ЗАНЯТЬ

№ з/п	. Назва теми	Кількість годин	
		денна форма	заочна форма
1	Тема 1. Архітектура веб-безпеки та моделювання загроз. 1. Архітектура клієнт-серверної взаємодії та особливості протоколів HTTP/HTTPS. 2. Механізми роботи cookies, сесій та налаштування заголовків безпеки. 3. Побудова моделі загроз для веб-додатків з урахуванням сучасних кіберзагроз. 4. Класифікація вразливостей за стандартами OWASP Top 10 та CWE. 5. Принципи безпечного проєктування (Secure by Design) на етапі архітектури.	2	

	6. Аналіз векторів атак на веб-архітектуру та методи їх нейтралізації.		
2	Тема 2. Захист від ін'єкційних атак. 7. Природа та механізми здійснення SQL/NoSQL-ін'єкцій та Command Injection. 8. Методи виявлення та аналізу вразливостей ін'єкційного типу у коді. 9. Превентивні заходи: використання параметризованих запитів та підготовлених виразів. 10. Валідація та санітизація вхідних даних для запобігання ін'єкціям. 11. Використання ORM-фреймворків для забезпечення безпеки даних. 12. Налаштування WAF (Web Application Firewall) для захисту від ін'єкційних атак.		
3	Тема 3. Захист від міжсайтового скриптингу та клієнтських атак. 13. Типи XSS-атак (відображуваний, збережений, DOM-based) та їх вектори реалізації. 14. Методи нейтралізації XSS через екранування виводу та санітизацію даних. 15. Налаштування Content Security Policy (CSP) для захисту клієнтської частини. 16. Використання прапорців HttpOnly/Secure для захисту cookies від перехоплення. 17. Механізми захисту від CSRF-атак (токени, SameSite-атрибути). 18. Аналіз вразливостей через JavaScript та HTML-ін'єкції у браузері.		
4	Тема 4. Безпечна аутентифікація, авторизація та управління сесіями. 19. Механізми аутенифікації: паролі, OAuth 2.0, OpenID Connect, JWT. 20. Вимоги до політики паролів та зберігання облікових даних. 21. Безпечне управління сесіями: ротація ідентифікаторів та налаштування тайм-аутів. 22. Захист від фіксації сесії та перехоплення ідентифікаторів користувачів. 23. Реалізація багатофакторної автентифікації (MFA) у веб-додатках. 24. Аналіз безпеки механізмів авторизації та контролю доступу до ресурсів.	2	
5	Тема 5. Безпека конфігурації та захист від логічних вразливостей. 25. Типові помилки конфігурації серверів, фреймворків та хмарних сервісів. 26. Вразливості бізнес-логіки: обхід оплати та маніпуляція параметрами запиту. 27. Захист від вразливості IDOR (Insecure Direct Object Reference) та недостатнього контролю доступу. 28. Застосування принципу найменших привілеїв у веб-середовищі. 29. Методики регулярного аудиту конфігурацій безпеки системи. 30. Автоматизоване сканування налаштувань для виявлення помилок конфігурації.		2
6	Тема 6. Інструменти та методики тестування безпеки веб-додатків. 31. Огляд інструментів тестування: Burp Suite Community, OWASP ZAP, Nikto. 32. Методики ручного та автоматизованого тестування безпеки веб-ресурсів. 33. Статичний (SAST) та динамічний (DAST) аналіз коду додатків. 34. Використання OWASP Testing Guide для структурованого аудиту		

	безпеки. 35. Побудова звітів про вразливості та пріоритезація виправлень. 36. Інтерпретація результатів сканування та верифікація знайдених проблем.		
7	Тема 7. Сучасні підходи до комплексного захисту веб-ресурсів. 37. Безпека API (REST, GraphQL): аутентифікація та лімітування запитів. 38. Захист SPA (Single Page Applications) та PWA від специфічних загроз. 39. DevSecOps-підходи: інтеграція перевірок безпеки в CI/CD-пайплайни. 40. Моніторинг та логування подій безпеки веб-ресурсів. 41. Використання AI/ML для виявлення аномалій у веб-трафіку. 42. Підготовка до постквантової криптографії у веб-середовищі.	2	
	Всього	**6**	**2**

6. САМОСТІЙНА РОБОТА

До самостійної роботи студентів щодо вивчення дисципліни «Основи Web-безпеки» включаються:

1. Знайомство з науковою та навчальною літературою відповідно зазначених у програмі тем.
2. Опрацювання лекційного матеріалу.
3. Підготовка до практичних занять.
4. Консультації з викладачем протягом семестру.
5. Самостійне опрацювання окремих питань навчальної дисципліни.
6. Підготовка та виконання індивідуальних завдань у вигляді есе, рефератів тощо.
7. Підготовка до підсумкового контролю.

Тематика та питання до самостійної підготовки та індивідуальних завдань

№ з/п	Назва теми	Кількість годин	
		денна форма	заочна форма
1	Тема 1. Архітектура веб-безпеки та моделювання загроз. Поняття веб-безпеки в контексті сучасних кіберзагроз. Архітектура клієнт-серверної взаємодії: HTTP/HTTPS, cookies, сесії, заголовки безпеки. Модель загроз для веб-додатків. Класифікація вразливостей (OWASP Top 10, CWE). Принципи безпечного проєктування (Secure by Design).	6	10
2	Тема 2. Захист від ін'єкційних атак. Природа та механізми ін'єкцій: SQL/NoSQL-ін'єкції, Command Injection, LDAP Injection. Методи виявлення та аналізу вразливостей. Превентивні заходи: параметризовані запити, підготовлені вирази, валідація та санітизація вхідних даних, використання ORM-фреймворків. Налаштування WAF (Web Application Firewall) для захисту від ін'єкцій.	8	12
3	Тема 3. Захист від міжсайтового скриптингу та клієнтських атак. Типи XSS-атак (відображуваний, збережений, DOM-based). Вектори атак через JavaScript та HTML-ін'єкції. Методи нейтралізації: екранування виводу, Content Security Policy (CSP), HttpOnly/Secure прапорці для cookies, санітизація даних на клієнті та сервері. Захист від CSRF-атак: токени, SameSite-атрибути.	8	12
4	Тема 4. Безпечна аутентифікація, авторизація та управління сесіями. Механізми аутентифікації: паролі, OAuth 2.0, OpenID Connect, JWT. Вимоги	6	12

	до політики паролів та зберігання облікових даних (хешування, сіль). Безпечне управління сесіями: ротація ідентифікаторів, тайм-аути, захист від фіксації сесії. Багатофакторна автентифікація (MFA) у веб-додатках.		
5	Тема 5. Безпека конфігурації та захист від логічних вразливостей. Типові помилки конфігурації серверів, фреймворків, хмарних сервісів. Вразливості бізнес-логіки: обхід оплати, маніпуляція параметрами, IDOR (Insecure Direct Object Reference), недостатній контроль доступу. Методи запобігання: принцип найменших привілеїв, регулярний аудит конфігурацій, автоматизоване сканування налаштувань.	8	12
6	Тема 6. Інструменти та методики тестування безпеки веб-додатків. Огляд інструментів: Burp Suite Community, OWASP ZAP, Nikto. Методики ручного та автоматизованого тестування. Статичний (SAST) та динамічний (DAST) аналіз коду. Використання OWASP Testing Guide для структурованого аудиту. Побудова звітів про вразливості та пріоритезація виправлень.	8	12
7	Тема 7. Сучасні підходи до комплексного захисту веб-ресурсів. Безпека API (REST, GraphQL): аутентифікація, лімітування запитів, валідація схем. Захист SPA (Single Page Applications) та PWA. DevSecOps-підходи: інтеграція перевірок безпеки в CI/CD-пайплайни. Моніторинг та логування подій безпеки. Перспективи: використання AI/ML для виявлення аномалій, підготовка до постквантової криптографії.	6	12
	Всього	**50**	**82**

7. ВИДИ ТА МЕТОДИ КОНТРОЛЮ

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

Методи діагностики знань (контролю)	**фронтальне опитування; наукова доповідь, реферати, усне повідомлення, індивідуальне опитування; робота у групах; ділова гра, розв`язання ситуаційних завдань, кейсів, практичних завдань,, залік**

Питання до заліку

1. Поняття веб-безпеки в контексті сучасних кіберзагроз: основні цілі та завдання.
2. Архітектура клієнт-серверної взаємодії: особливості протоколів HTTP/HTTPS.
3. Механізми роботи cookies, сесій та заголовків безпеки у веб-додатках.
4. Побудова моделі загроз для веб-додатків: методологія та практичне застосування.
5. Класифікація вразливостей за стандартами OWASP Top 10 та CWE: порівняльний аналіз.
6. Принципи безпечного проєктування (Secure by Design) на етапі архітектури веб-систем.
7. Аналіз векторів атак на веб-архітектуру та методи їх нейтралізації.
8. Природа та механізми здійснення SQL/NoSQL-ін'єкцій та Command Injection.
9. Методи виявлення та статичного аналізу вразливостей ін'єкційного типу у коді.

10. Превентивні заходи: використання параметризованих запитів та підготовлених виразів.
11. Валідація та санітизація вхідних даних як основа захисту від ін'єкцій.
12. Використання ORM-фреймворків для забезпечення безпеки даних.
13. Налаштування WAF (Web Application Firewall) для захисту від ін'єкційних атак.
14. Типи XSS-атак (відображуваний, збережений, DOM-based) та їх вектори реалізації.
15. Методи нейтралізації XSS через екранування виводу та санітизацію даних.
16. Налаштування Content Security Policy (CSP) для захисту клієнтської частини веб-додатків.
17. Використання прапорців HttpOnly/Secure для захисту cookies від перехоплення.
18. Механізми захисту від CSRF-атак: токени, SameSite-атрибути, перевірка Referer.
19. Аналіз вразливостей через JavaScript та HTML-ін'єкції у браузері.
20. Механізми аутентифікації: паролі, OAuth 2.0, OpenID Connect, JWT — порівняльна характеристика.
21. Вимоги до політики паролів та методи безпечного зберігання облікових даних (хешування, сіль, KDF).
22. Безпечне управління сесіями: ротація ідентифікаторів, налаштування тайм-аутів, захист від фіксації.
23. Захист від перехоплення ідентифікаторів користувачів та атак типу session hijacking.
24. Реалізація багатофакторної автентифікації (MFA) у веб-додатках: методи та інструменти.
25. Аналіз безпеки механізмів авторизації та контролю доступу до ресурсів (RBAC, ABAC).
26. Типові помилки конфігурації серверів, фреймворків та хмарних сервісів: приклади та наслідки.
27. Вразливості бізнес-логіки: обхід оплати, маніпуляція параметрами запиту, недостатній контроль доступу.
28. Захист від вразливості IDOR (Insecure Direct Object Reference): методи виявлення та усунення.
29. Застосування принципу найменших привілеїв у веб-середовищі на практиці.
30. Методики регулярного аудиту конфігурацій безпеки системи та автоматизоване сканування налаштувань.
31. Огляд інструментів тестування безпеки: Burp Suite Community, OWASP ZAP, Nikto — функціонал та сфери застосування.
32. Методики ручного та автоматизованого тестування безпеки веб-ресурсів: порівняльний аналіз.
33. Статичний (SAST) та динамічний (DAST) аналіз коду: переваги, обмеження та сфери застосування.
34. Використання OWASP Testing Guide для структурованого аудиту безпеки веб-додатків.
35. Побудова звітів про вразливості: структура, пріоритезація виправлень та комунікація з розробниками.
36. Інтерпретація результатів сканування та верифікація знайдених проблем безпеки.
37. Безпека API (REST, GraphQL): аутентифікація, лімітування запитів, валідація схем.
38. Особливості захисту SPA (Single Page Applications) та PWA від специфічних загроз.
39. DevSecOps-підходи: інтеграція перевірок безпеки в CI/CD-пайплайни.
40. Моніторинг та логування подій безпеки веб-ресурсів: інструменти та методики аналізу.
41. Використання AI/ML для виявлення аномалій у веб-трафіку: перспективи та обмеження.
42. Підготовка до постквантової криптографії у веб-середовищі: актуальність та шляхи міграції.

8. ОЦІНЮВАННЯ ЗДОБУВАЧІВ ВИЩОЇ ТА ФАХОВОЇ ПЕРДВИЩОЇ ОСВІТИ ЗА НАВЧАЛЬНУ ДИСЦИПЛІНУ У МІЖНАРОДНОМУ ГУМАНІТАРНОМУ УНІВЕРСИТЕТІ

(*поточний контроль, підсумковий контроль, загальний результат оцінювання)*

ЗАЛІК

Поточний контроль			
Види роботи	**Планові терміни виконання**	**Форми контролю та звітності**	**Максимальний відсоток оцінювання**
Систематичність і активність роботи на практичних (лабораторних) заняттях			
1.1. Підготовка до практичних (лабораторних) занять	Відповідно до робочої програми та розкладу занять	Перевірка обсягу та якості засвоєного матеріалу під час практичних (лабораторних) занять	**60**
Виконання завдань для самостійного опрацювання			
1.2. Індивідуальне тестування, завдання, підготовка реферату (есе) за заданою тематикою	Відповідно до робочої програми та розкладу занять	Розгляд відповідного матеріалу під час аудиторних занять або ІКР, перевірка конспектів навчальних текстів тощо	**20**
Виконання індивідуальних завдань, дослідна робота здобувача			
1.3. Інші види індивідуальних завдань, в т.ч.підготовка наукових публікацій, участь у роботі круглих столів, конференцій тощо.	Відповідно до робочої програми та розкладу занять	Обговорення результатів проведеної роботи під час аудиторних занять, наукових конференцій та круглих столів.	**20**
Разом балів за поточний контроль			**100**
Загальний результат оцінювання			**100**

Поточний контроль знань здобувачів освіти при формі контролю **залік** (максимум 100 балів) оцінюється за шкалою *(«2», «3», «4», «5»)*, з обов'язковим переведенням балів за кожний вид роботи таким чином:

- за підготовку до аудиторних занять (максимум 60 балів) здобувачу освіти необхідно мати не менше 1/2 оцінок від загальної кількості практичних (лабораторних) занять, для переводу балів за підготовку до аудиторних занять середньоарифметична оцінка множиться на коефіцієнт 12;
- за виконання завдань для самостійного опрацювання (тестування, завдання, підготовка реферату (есе) за заданою тематикою) (максимум 20 балів) здобувачу освіти необхідно мати не менше 1/2 оцінок від загальної кількості програмного матеріалу, що виноситься на самостійне вивчення, для переводу зазначених балів середньоарифметична оцінка множиться на коефіцієнт 4;
- за інші види індивідуальних завдань, в т.ч. підготовку наукових публікацій, участь у роботі круглих столів, конференцій тощо (максимум 20- балів) здобувачу освіти необхідно мати не менше 1/2 оцінок від загальної кількості інших видів індивідуальних завдань, для переводу балів за підготовку до аудиторних занять середньоарифметична оцінка множиться на коефіцієнт 4.

КРИТЕРІЇ ОЦІНЮВАННЯ ЗА ПОТОЧНИЙ КОНТРОЛЬ

- «2»- виставляється за неправильну відповідь (письмову роботу), яка не відповідає змісту теми та свідчить про нерозуміння її основних положень;
- «3» -виставляється за відповідь (письмову роботу), яка відповідає змісту теми, але є неповною і неточною у визначенні понять, свідчить про неповне розуміння основних положень навчального матеріалу, свідчить про те, що знання студента мають фрагментарний, поверховий характер;
- «4» - оцінюється правильна і обґрунтована відповідь (письмова робота), з якої видно, що студент знає й розуміє теоретичний матеріал в обсязі навчальної теми, володіє необхідними навичками, не допускає суттєвих помилок.
- «5» - оцінюється повна, правильна, ґрунтовна відповідь (письмова робота) на запитання теми, що передбачає логічність і послідовність викладу матеріалу, володіння термінологією, показує вміння повно й глибоко використовувати теоретичні знання в практичній площині.

9. КРИТЕРІЇ ЗАГАЛЬНИХ РЕЗУЛЬТАТІВ ОЦІНЮВАННЯ ЗНАНЬ ЗДОБУВАЧІВ (для іспиту / заліку)

Рівень знань оцінюється:

- «відмінно» / «зараховано» A - від 90 до 100 балів. Студент виявляє особливі творчі здібності, вміє самостійно знаходити та опрацьовувати необхідну інформацію, демонструє знання матеріалу, проводить узагальнення і висновки. Був присутній на лекціях та семінарських заняттях, під час яких давав вичерпні, обґрунтовані, теоретично і практично правильні відповіді, має конспект з виконаними завданнями до самостійної роботи, презентував реферат (есе) за заданою тематикою, проявляє активність і творчість у науково-дослідній роботі;
- «добре» / «зараховано» B - від 82 до 89 балів. Студент володіє знаннями матеріалу, але допускає незначні помилки у формуванні термінів, категорій, проте за допомогою викладача швидко орієнтується і знаходить правильні відповіді. Був присутній на лекціях та семінарських заняттях, має конспект з виконаними завданнями до самостійної роботи, презентував реферат (есе) за заданою тематикою, проявляє активність і творчість у науково-дослідній роботі;
- «добре» / «зараховано» C - від 74 до 81 балів. Студент відтворює значну частину теоретичного матеріалу, виявляє знання і розуміння основних положень, з допомогою викладача може аналізувати навчальний матеріал, але дає недостатньо обґрунтовані, невичерпні відповіді, допускає помилки. При цьому враховується наявність конспекту з виконаними завданнями до самостійної роботи, реферату та активність у науково-дослідній роботі;
- «задовільно» / «зараховано» D - від 64 до 73 балів. Студент був присутній не на всіх лекціях та семінарських заняттях, володіє навчальним матеріалом на середньому рівні, допускає помилки, серед яких є значна кількість суттєвих. При цьому враховується наявність конспекту з виконаними завданнями до самостійної роботи, рефератів (есе);
- «задовільно» / «зараховано» E - від 60 до 63 балів. Студент був присутній не на всіх лекціях та семінарських заняттях, володіє навчальним матеріалом на рівні, вищому за початковий, значну частину його відтворює на репродуктивному рівні, на всі запитання дає необґрунтовані, невичерпні відповіді, допускає помилки, має неповний конспект з завданнями до самостійної роботи.
- «незадовільно з можливістю повторного складання» / «не зараховано» FX – від 35 до 59 балів. Студент володіє матеріалом на рівні окремих фрагментів, що становлять незначну частину навчального матеріалу.
- «незадовільно з обов'язковим повторним вивченням дисципліни» / «не зараховано» F – від 0 до 34 балів. Студент не володіє навчальним матеріалом.

ТАБЛИЦЯ ВІДПОВІДНОСТІ ЗАГАЛЬНИХ РЕЗУЛЬТАТІВ ОЦІНЮВАННЯ ЗНАНЬ ЗА РІЗНИМИ ШКАЛАМИ

100-бальною шкалою	Шкала за ECTS	За національною шкалою	
		екзамен	залік
90-100	A	Відмінно	Зараховано
82-89	B	Добре	

10. ДОТРИМАННЯ ВИМОГ АКАДЕМІЧНОЇ ДОБРОЧЕСНОСТІ

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

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

Дотримання академічної доброчесності передбачає:

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

11. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Пірог О. В. Безпека вебдодатків : навч. посіб. Житомир : Державний університет «Житомирська політехніка», 2025. 290 с. ISBN 978-966-683-694-9.
2. Есін В. І., Кузнєцов О. О., Сорока Л. С. Основи кібербезпеки : підручник. Київ : Освіта України, 2020. 416 с.
3. Корченко О. Г. Побудова систем захисту інформації на базі міжнародних стандартів : навч. посіб. Київ : ТОВ «НВП «Інтертехнодрук», 2010. 200 с.
4. Юдін О. К., Корченко О. Г., Конахович Г. Ф. Захист інформації в мережах передачі даних : навч. посіб. Київ : ДУТ, 2009. 716 с.
5. Яремчук Ю. Є., Брежнєва К. С. Основи інформаційної безпеки : навч. посіб. Київ : КПІ ім. Ігоря Сікорського, 2017. 240 с.
6. Hoffman A. Web Application Security: Exploitation and Countermeasures for Modern Web Applications. 2nd ed. Sebastopol : O'Reilly Media, 2024. 450 p.

7. McDonald M. Web Security for Developers: Real Threats, Practical Defense. San Francisco : No Starch Press, 2020. 350 p.

8. Zalewski M. The Tangled Web: A Guide to Securing Modern Web Applications. San Francisco : No Starch Press, 2011. 368 p.

9. Yaworski P. Real-World Bug Hunting: A Field Guide to Web Hacking. San Francisco : No Starch Press, 2019. 312 p.

10. Stuttard D., Pinto M. The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws. 2nd ed. Indianapolis : Wiley, 2011. 912 p.

11. Stallings W., Brown L. Computer Security: Principles and Practice. 5th ed. Harlow : Pearson, 2023. 896 p.

12. Madden N. API Security in Action. Shelter Island : Manning Publications, 2020. 456 p.

Допоміжна

13. Anderson R. Security Engineering: A Guide to Building Dependable Distributed Systems. 3rd ed. Indianapolis : Wiley, 2020. 1232 p.

14. Bishop M. Computer Security: Art and Science. 2nd ed. Boston : Addison-Wesley, 2018. 1440 p.

15. Schneier B. Applied Cryptography: Protocols, Algorithms and Source Code in C. 20th Anniversary ed. Indianapolis : Wiley, 2015. 784 p.

16. Whitman M. E., Mattord H. J. Principles of Information Security. 7th ed. Boston : Cengage Learning, 2021. 688 p.

Інформаційні ресурси

17. Державна служба спеціального зв'язку та захисту інформації України : офіц. сайт. Київ. URL: https://cip.gov.ua/.

18. Департамент кіберполіції Національної поліції України : офіц. сайт. Київ. URL: https://cyberpolice.gov.ua/.

19. CERT-UA – Урядова команда реагування на комп'ютерні надзвичайні події України. Київ. URL: https://cert.gov.ua/.

20. OWASP Foundation. OWASP Top Ten Web Application Security Risks. 2025. URL: https://owasp.org/www-project-top-ten/.

21. OWASP Foundation. Web Security Testing Guide (WSTG). Version 4.2. URL: https://owasp.org/www-project-web-security-testing-guide/.

22. PortSwigger. Web Security Academy : онлайн-курс. URL: https://portswigger.net/web-security (дата звернення: 13.03.2026).

23. OWASP Foundation. Juice Shop : навчальний вебдодаток з вразливостями. URL: https://owasp.org/www-project-juice-shop/.

24. Snyk Ltd. Snyk Learn : інтерактивні уроки з веббезпеки. URL: https://learn.snyk.io/.

25. National Institute of Standards and Technology. Cybersecurity Framework. Gaithersburg, 2024. URL: https://www.nist.gov/cyberframework.

26. European Union Agency for Cybersecurity (ENISA). URL: https://www.enisa.europa.eu/.

27. Salt Security. API Security For Dummies. 2024. URL: https://salt.security/api-security-for-dummies.

28. Detectify. Guide To Modern Web App Security. 2024. URL: https://detectify.com/resources/guides/web-app-security.