МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ
ВІДОКРЕМЛЕНИЙ СТРУКТУРНИЙ ПІДРОЗДІЛ «РІВНЕНСЬКИЙ ФАХОВИЙ КОЛЕДЖ НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ»

Відділення інформаційних технологій
Циклова комісія *програмування та інформаційних дисциплін*

ЗАТВЕРДЖУЮ
Заступник директора
з навчальної роботи
09 грудня 2025 р.
Людмила БАЛДИЧ

ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

БЕЗПЕКА ВЕБЗСТОСУНКІВ	
галузь знань	*12 Інформаційні технології*
спеціальність	*125 Кібербезпека та захист інформації*
освітня програма	*Кібербезпека та захист інформації*

Рівне – 2025 рік

Програма навчальної дисципліни з *БЕЗПЕКА ВЕБЗАСТОСУНКІВ* розроблено на основі освітньо-професійної програми *Кібербезпека та захист інформації* для здобувачів освіти освітньо-професійного ступеня "Фаховий молодший бакалавр" галузі знань 12 Інформаційні технології, спеціальності *125 Кібербезпека та захист інформації, затвердженої Вченою радою НУБіП України протокол від 26.04.2023 №10*

Розробники: *Янок Назар Сергійович, викладач програмування та інформаційних дисциплін;*

Програму навчальної дисципліни розглянуто і схвалено на засіданні циклової комісії *програмування та інформаційних дисциплін*

Протокол від «29» серпня 2025 року № 1

Голова циклової комісії *програмування та інформаційних дисциплін*

«29» серпня 2025 року _____ *Павло СТРИК*

Погоджено методичною радою ВСП «РФК НУБіП України»

Протокол від «29» *серпня* 2025 року № 1

29 серпня 2025 року Голова _____ *Людмила БАЛДИЧ*

Ó Янок Н.С., 2025

ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Галузь знань, напрям підготовки, спеціальність, освітньо-кваліфікаційний рівень	
Освітньо-професійний ступінь	*фаховий молодший бакалавр*
Галузь знань	*12 Інформаційні технології*
Спеціальність	*125 Кібербезпека та захист інформації*
Характеристика навчальної дисципліни	
Вид	обов'язкова
Загальна кількість годин	90
Кількість кредитів ECTS	3
Кількість змістових модулів	3
Мова викладання, навчання та оцінювання	українська
Форма контролю	залік
Показники навчальної дисципліни для денної та заочної форм навчання	
Форма навчання	денна
Рік підготовки	2025-2026
Семестр	6
Аудиторні години:	64
Лекційні	30
Практичні	30
Самостійна робота	30
Кількість тижневих годин для денної форми навчання	4

МЕТА ТА ЗАВДАННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Мета навчальної дисципліни полягає в поглибленні теоретичної і практичної підготовки фахівця, спрямованої на вирішення типових та складних завдань цифрової криміналістики, що полягають у зборі цифрової криміналістичної інформації, збереженні, дослідженні і використанні цифрових доказів.

Ось завдання та очікувані результати для дисципліни "Безпека веб-застосунків":

Завдання навчальної дисципліни:

- ознайомлення з основними принципами безпеки веб-застосунків та архітектурою клієнт-серверної взаємодії;
- вивчення найпоширеніших вразливостей веб-застосунків згідно з OWASP Top 10;
- розгляд механізмів експлуатації injection атак: SQL, Command, LDAP, XXE, SSTI;
- освоєння методів виявлення та захисту від Cross-Site Scripting (XSS) атак;
- вивчення принципів роботи Cross-Site Request Forgery (CSRF) та методів протидії;
- навчання безпечній реалізації механізмів автентифікації та управління сесіями;
- дослідження вразливостей контролю доступу та методів їх експлуатації;
- аналіз специфічних вразливостей REST API та GraphQL;
- ознайомлення з основами криптографії у веб-застосунках та протоколом HTTPS/TLS;
- опрацювання методів захисту від вразливостей завантаження файлів та десеріалізації;
- вивчення Server-Side Request Forgery (SSRF) та інших критичних вразливостей;
- засвоєння принципів безпечної розробки та інтеграції безпеки в SDLC;
- розгляд методів тестування безпеки веб-застосунків та використання захисних механізмів.

Вміти:

- ідентифікувати основні типи вразливостей веб-застосунків та оцінювати їхній вплив;
- застосовувати методи виявлення та експлуатації SQL Injection атак різних типів;
- проводити аналіз веб-застосунків на наявність XSS вразливостей;
- тестувати механізми автентифікації та авторизації на стійкість до атак;
- використовувати інструменти для пентестингу веб-застосунків;
- налаштовувати Content Security Policy (CSP) та інші security headers;
- реалізовувати безпечні механізми обробки вхідних даних та валідації;

- захищати веб-застосунки від CSRF атак за допомогою токенів та SameSite cookies;
- аналізувати безпеку REST API та GraphQL endpoints;
- виявляти вразливості контролю доступу: IDOR, Path Traversal, Privilege Escalation;
- застосовувати криптографічні методи для захисту даних у веб-застосунках;
- проводити аналіз та усунення вразливостей завантаження файлів;
- використовувати Web Application Firewall (WAF) для захисту веб-застосунків;
- виявляти та протидіяти SSRF атакам;
- імплементувати безпечне зберігання паролів з використанням сучасних алгоритмів хешування;
- налаштовувати CORS політики для безпечної міждоменної взаємодії;
- складати звіти про виявлені вразливості та рекомендації щодо їх усунення;
- інтегрувати практики безпечної розробки в процес створення веб-застосунків.

Очікувані результати навчання.

Після вивчення дисципліни «Безпека вебзастосунків» у здобувачів освіти формуються такі **компетентності:**

Загальні (ЗК):

ЗК01. Здатність застосовувати знання у практичних ситуаціях.

ЗК02. Знання та розуміння предметної області та професії.

ЗК04. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.

ЗК05. Здатність здійснювати пошук, оброблення та аналіз інформації.

Спеціальні (ФК):

ФК02. Здатність використовувати інформаційно-комунікаційні технології, сучасні методи і моделі інформаційної безпеки та/або кібербезпеки.

ФК03. Здатність використовувати програмні та програмно-апаратні засоби захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.

Програмні результати навчання (ПР):

ПР06. Вміти використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності

ПР10. Знати теорію та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.

ПР11. Вміти впроваджувати заходи щодо попередження отримання несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем згідно зі встановленою політикою інформаційної безпеки та\або кібербезпеки.

ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Змістовий модуль 1: Основи безпеки веб-застосунків та injection атаки

Тема 1. Вступ до безпеки веб-застосунків та архітектура

Визначення та основи безпеки веб-застосунків. Історія розвитку веб-технологій та еволюція загроз. Ландшафт сучасних загроз веб-безпеки. OWASP Top 10: огляд найпоширеніших вразливостей. Роль безпеки в життєвому циклі розробки (SDLC). Принципи безпечної розробки. Архітектура веб-застосунків: клієнт-серверна модель. HTTP/HTTPS протокол: методи запитів, коди відповідей, заголовки. Сесії та cookies: механізми роботи. Same-Origin Policy (SOP): принципи та обмеження. Моделювання загроз: STRIDE, DREAD. Вектори атак на веб-застосунки.

Тема 2. SQL Injection атаки

Принципи роботи баз даних та SQL. SQL Injection: механізм експлуатації. Типи SQL Injection: in-band, blind, out-of-band. Error-based, Union-based, Boolean-based, Time-based SQLi. Вплив SQL Injection: витік даних, обхід автентифікації, RCE. Реальні кейси SQL Injection атак. Методи захисту від SQL Injection. Prepared Statements та Parameterized Queries. ORM (Object-Relational Mapping): переваги та обмеження. Stored Procedures: безпечне використання. Валідація та санітизація вхідних даних. Принцип найменших привілеїв для БД. WAF (Web Application Firewall) та їх роль. Моніторинг та виявлення SQL Injection атак.

Тема 3. Інші типи Injection атак

Command Injection (OS Command Injection). LDAP Injection. XPath Injection. XML Injection та XXE (XML External Entity). Template Injection (SSTI). NoSQL Injection. Mechanisms експлуатації та захист від кожного типу. Порівняння різних типів injection атак.

Змістовий модуль 2: Cross-site атаки та автентифікація

Тема 4. Cross-Site Scripting (XSS)

XSS: визначення та принцип роботи. Типи XSS: Reflected, Stored, DOM-based. Вектори атак XSS: JavaScript, HTML, CSS. Наслідки XSS: викрадення cookies, phishing, дефейс. Мутації XSS та обхід фільтрів. Browser XSS фільтри та їх обмеження. Content Security Policy (CSP): принципи роботи. Конфігурація CSP: директиви, nonce, hash. Input validation та output encoding. Санітизація HTML: DOMPurify, Bleach. HTTPOnly та Secure flags для cookies. X-XSS-Protection заголовок. Контекстуальне екранування.

Тема 5. Cross-Site Request Forgery (CSRF) та автентифікація

CSRF: механізм атаки. Різниця між XSS та CSRF. Сценарії експлуатації CSRF. GET vs POST CSRF. Login CSRF. Impact CSRF атак: зміна даних, фінансові транзакції. Real-world кейси CSRF. Методи захисту: CSRF токени, SameSite cookies, Double Submit Cookie. Механізми автентифікації: паролі, MFA, біометрія. Broken Authentication: слабкі паролі, brute force, credential stuffing. Session Management: session fixation, session hijacking. Безпечне зберігання паролів: hashing, salting, bcrypt, Argon2. Password reset механізми та їх вразливості. OAuth 2.0 та OpenID Connect: основи та вразливості.

Тема 6. Вразливості авторизації та контролю доступу

Broken Access Control: IDOR, Path Traversal, Privilege Escalation. RBAC (Role-Based Access Control). ABAC (Attribute-Based Access Control). Horizontal vs Vertical Privilege Escalation. Insecure Direct Object References (IDOR). Missing Function Level Access Control. Forced browsing. Методи тестування та захисту від порушень контролю доступу.

Змістовий модуль 3: Безпека API, криптографія та додаткові вразливості

Тема 7. Безпека REST API та GraphQL

OWASP API Security Top 10. REST API: аутентифікація (JWT, API Keys, OAuth). Rate limiting та throttling. GraphQL: основи та специфічні вразливості. GraphQL: Introspection, Batching attacks, DoS. API versioning та backward compatibility. CORS (Cross-Origin Resource Sharing): принципи та налаштування.

Тема 8. Криптографія у веб-застосунках

Основи криптографії: симетричне та асиметричне шифрування. HTTPS/TLS: handshake, сертифікати, cipher suites. SSL/TLS вразливості: POODLE, BEAST, Heartbleed. Certificate Pinning. Криптографічні помилки: слабкі алгоритми, hardcoded keys. Шифрування даних: at rest, in transit. Цифрові підписи та MAC.

Тема 9. File Upload, XXE та Десеріалізація

Unrestricted File Upload: механізм атаки. Типи файлів та MIME types. Обхід фільтрів: extension bypass, magic bytes. Веб-шелли: PHP, ASP, JSP. Path Traversal (Directory Traversal). Local File Inclusion (LFI) та Remote File Inclusion (RFI). XXE через file upload. Методи захисту від file upload вразливостей. XML: структура та парсинг. XXE (XML External Entity): механізм атаки. Типи XXE: in-band, out-of-band, blind. Impact: file disclosure, SSRF, DoS. Insecure Deserialization. Serialization в різних мовах: Java, Python, PHP. Remote Code Execution через десеріалізацію. Методи захисту від XXE та небезпечної десеріалізації.

Тема 10. SSRF та інші вразливості веб-застосунків

SSRF: механізм та вектори атаки. Blind SSRF. SSRF для доступу до внутрішніх ресурсів. SSRF та cloud metadata endpoints (AWS, Azure, GCP). Clickjacking (UI Redressing). Open Redirect. Security Misconfiguration. Using Components with Known Vulnerabilities. Security headers: HSTS, X-Frame-Options, X-Content-Type-Options.

СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

№	Назви змістових модулів і тем	Кількість годин			
		денна форма			
		всього	лекційні	практичні	самостійне вивчення
1	*2*	*3*	*4*	*5*	*6*
Змістовий модуль 1. Основи безпеки веб-застосунків та injection атаки					
Тема 1	Вступ до безпеки веб-застосунків та архітектура	12	4	4	4
Тема 2	SQL Injection атаки	12	4	4	4
Тема 3	Інші типи Injection атак	6	2	2	2
Разом за змістовим модулем 1		**30**	**10**	**10**	**10**
Змістовий модуль 2. Cross-site атаки та автентифікація					
Тема 4	Cross-Site Scripting (XSS)	12	4	4	4
Тема 5	Cross-Site Request Forgery (CSRF) та автентифікація	12	4	4	4
Тема 6	Вразливості авторизації та контролю доступу	6	2	2	2
Разом за змістовим модулем 2		**30**	**10**	**10**	**10**
Змістовий модуль 3. Безпека API, криптографія та додаткові вразливості					
Тема 7	Безпека REST API та GraphQL	6	2	2	2
Тема 8	Криптографія у веб-застосунках	6	2	2	2
Тема 9	File Upload, XXE та Десеріалізація	12	4	4	4
Тема 10	SSRF та інші вразливості веб-застосунків	6	2	2	2
Разом за змістовим модулем 3		**30**	**10**	**10**	**10**
Всього годин		**90**	**30**	**30**	**30**

5. ТЕМИ ЛЕКЦІЙНИХ, ЛАБОРАТОРНИХ ЗАНЯТЬ ТА ЗМІСТ САМОСТІЙНОГО ВИВЧЕННЯ

№ теми	№ заняття	Вид навчальної діяльності	Назва теми	Кількість годин
Змістовий модуль 1. Основи безпеки веб-застосунків та injection атаки				**22**
1	**Вступ до безпеки веб-застосунків та архітектура**			**12**
	1	лекція 1	Визначення та основи безпеки веб-застосунків. Історія розвитку веб-технологій та еволюція загроз. Ландшафт сучасних загроз веб-безпеки. OWASP Top 10: огляд найпоширеніших вразливостей. Роль безпеки в життєвому циклі розробки (SDLC). Принципи безпечної розробки.	2
		самостійне вивчення	Детальне вивчення документації OWASP Top 10 (2021/2023). Аналіз статистики вразливостей веб-застосунків. Ознайомлення з ресурсами OWASP (Web Security Testing Guide).	2
	2	практична робота 1	Налаштування лабораторного середовища Kali Linux. Встановлення та базова конфігурація Burp Suite Community Edition.	2
	3	лекція 2	Архітектура веб-застосунків: клієнт-серверна модель. HTTP/HTTPS протокол: методи запитів, коди відповідей, заголовки. Сесії та cookies: механізми роботи. Same-Origin Policy (SOP): принципи та обмеження. Моделювання загроз: STRIDE, DREAD. Вектори атак на веб-застосунки.	2
		самостійна робота	Вивчення специфікації HTTP/1.1, HTTP/2, HTTP/3. Аналіз різних методів моделювання загроз. Дослідження архітектурних патернів веб-застосунків (MVC, REST, микросервіси).	2
	4	практична робота 2	Аналіз HTTP-трафіку за допомогою Burp Suite. Перехоплення та модифікація HTTP запитів. Дослідження cookies та session tokens.	2
2	SQL Injection атаки			12
	5	лекція 3	Принципи роботи баз даних та SQL. SQL Injection: механізм експлуатації. Типи SQL Injection: in-band, blind, out-of-band. Error-based, Union-based, Boolean-based, Time-based SQLi. Вплив SQL Injection: витік даних, обхід автентифікації, RCE. Реальні кейси SQL Injection атак.	2
		самостійне вивчення	Вивчення синтаксису SQL для різних СУБД (MySQL, PostgreSQL, MSSQL, Oracle). Аналіз CVE пов'язаних з SQL Injection. Дослідження автоматизованих інструментів (sqlmap).	2

	6	практична робота 3	Ручна експлуатація SQL Injection в DVWA (error-based та union-based). Використання sqlmap для автоматизації атаки та витягу даних.	2
	7	лекція 4	Методи захисту від SQL Injection. Prepared Statements та Parameterized Queries. ORM (Object-Relational Mapping): переваги та обмеження. Stored Procedures: безпечне використання. Валідація та санітизація вхідних даних. Принцип найменших привілеїв для БД. WAF (Web Application Firewall) та їх роль. Моніторинг та виявлення SQL Injection атак.	2
		самостійне вивчення	Вивчення документації Prepared Statements для різних мов програмування. Аналіз популярних ORM фреймворків (Hibernate, Entity Framework, SQLAlchemy). Дослідження правил WAF для захисту від SQLi.	2
	8	практична робота 4	Написання вразливого та захищеного коду з використанням Prepared Statements. Налаштування та тестування ModSecurity WAF.	2
3	Інші типи Injection атак			**6**
	9	лекція 5	Command Injection (OS Command Injection). LDAP Injection. XPath Injection. XML Injection та XXE (XML External Entity). Template Injection (SSTI). NoSQL Injection. Mechanisms експлуатації та захист від кожного типу. Порівняння різних типів injection атак.	2
		самостійне вивчення	Вивчення специфіки кожного типу Injection. Аналіз реальних вразливостей в CVE база. Дослідження payload'ів для різних типів injection.	2
	10	практична робота 5	Експлуатація Command Injection та отримання shell. Тестування SSTI вразливості в одному з template engines. Розробка захищеної версії коду.	2
Змістовий модуль 2: Cross-site атаки та автентифікація				**24**
4	**Cross-Site Scripting (XSS)**			**12**
	11	лекція 6	XSS: визначення та принцип роботи. Типи XSS: Reflected, Stored, DOM-based. Вектори атак XSS: JavaScript, HTML, CSS. Наслідки XSS: викрадення cookies, phishing, дефейс. Мутації XSS та обхід фільтрів. Browser XSS фільтри та їх обмеження.	2
		самостійне вивчення	Вивчення JavaScript для розуміння XSS payload'ів. Аналіз колекцій XSS payload'ів (XSS Cheat Sheet). Дослідження browser-based XSS фільтрів.	2
	12	практична робота 6	Експлуатація Reflected та Stored XSS в лабораторному середовищі. Викрадення cookies через XSS та демонстрація session hijacking.	2

	13	лекція 7	Content Security Policy (CSP): принципи роботи. Конфігурація CSP: директиви, nonce, hash. Input validation та output encoding. Санітизація HTML: DOMPurify, Bleach. HTTPOnly та Secure flags для cookies. X-XSS-Protection заголовок. Контекстуальне екранування.	2
		самостійне вивчення	Вивчення специфікації CSP. Аналіз різних рівнів CSP (Level 1, 2, 3). Дослідження бібліотек для санітизації по мовам програмування.	2
	14	практична робота 7	Імплементація Content Security Policy та налаштування CSP заголовків. Реалізація input validation та output encoding з використанням DOMPurify.	2
5	**Cross-Site Request Forgery (CSRF) та автентифікація**			**12**
	15	лекція 8	CSRF: механізм атаки. Різниця між XSS та CSRF. Сценарії експлуатації CSRF. GET vs POST CSRF. Login CSRF. Impact CSRF атак: зміна даних, фінансові транзакції. Real-world кейси CSRF. Методи захисту: CSRF токени, SameSite cookies, Double Submit Cookie.	2
		самостійне вивчення	Аналіз CVE пов'язаних з CSRF. Вивчення різних реалізацій CSRF токенів. Дослідження CSRF в RESTful API.	2
	16	практична робота 8	Створення та експлуатація CSRF proof-of-concept. Імплементація CSRF токенів (Synchronizer Token Pattern) та налаштування SameSite cookie attribute.	2
	17	лекція 9	Механізми автентифікації: паролі, MFA, біометрія. Broken Authentication: слабкі паролі, brute force, credential stuffing. Session Management: session fixation, session hijacking. Безпечне зберігання паролів: hashing, salting, bcrypt, Argon2. Password reset механізми та їх вразливості. OAuth 2.0 та OpenID Connect: основи та вразливості.	2
		самостійне вивчення	Вивчення алгоритмів хешування паролів. Аналіз OAuth 2.0 flow'ів. Дослідження атак на механізми автентифікації.	2
	18	практична робота 9	Brute force атака на форму логіну з використанням Burp Intruder. Імплементація безпечного зберігання паролів з bcrypt та налаштування rate limiting.	2
6	**Цифрові докази: типи, збір та аналіз**			**6**
	19	лекція 10	Broken Access Control: IDOR, Path Traversal, Privilege Escalation. RBAC (Role-Based Access Control). ABAC (Attribute-Based Access Control). Horizontal vs Vertical Privilege Escalation. Insecure Direct Object References (IDOR). Missing Function	2

			Level Access Control. Forced browsing. Методи тестування та захисту від порушень контролю доступу.	
		самостійне вивчення	Вивчення моделей контролю доступу. Аналіз фреймворків авторизації (Spring Security, Django Permissions). Дослідження IDOR вразливостей у популярних додатках.	2
	20	практична робота 10	Експлуатація IDOR вразливостей для доступу до чужих даних. Демонстрація Privilege Escalation (horizontal та vertical) та імплементація правильної авторизації.	2
Змістовий модуль 3: Безпека API, криптографія та додаткові вразливості				**24**
7	**Безпека REST API та GraphQL**			**6**
	21	лекція 11	OWASP API Security Top 10. REST API: аутентифікація (JWT, API Keys, OAuth). Rate limiting та throttling. GraphQL: основи та специфічні вразливості. GraphQL: Introspection, Batching attacks, DoS. API versioning та backward compatibility. CORS (Cross-Origin Resource Sharing): принципи та налаштування.	2
		самостійне вивчення	Вивчення OWASP API Security Top 10. Аналіз структури JWT токенів. Дослідження GraphQL специфікацій та вразливостей.	2
	22	практична робота 11	Тестування REST API з слабкою аутентифікацією за допомогою Postman. Експлуатація GraphQL вразливостей (excessive data exposure) та налаштування CORS політик.	2
8	**Криптографія у веб-застосунках**			**6**
	23	лекція 12	Основи криптографії: симетричне та асиметричне шифрування. HTTPS/TLS: handshake, сертифікати, cipher suites. SSL/TLS вразливості: POODLE, BEAST, Heartbleed. Certificate Pinning. Криптографічні помилки: слабкі алгоритми, hardcoded keys. Шифрування даних: at rest, in transit. Цифрові підписи та MAC.	2
		самостійне вивчення	Вивчення принципів роботи TLS 1.2 та TLS 1.3. Аналіз історичних криптографічних вразливостей. Дослідження Let's Encrypt та процесу отримання сертифікатів.	2
	24	практична робота 12	Аналіз SSL/TLS конфігурації веб-сайту за допомогою SSLLabs. Налаштування HTTPS на веб-сервері з Let's Encrypt сертифікатом.	2
9	**File Upload, XXE та Десеріалізація**			**6**
	25	лекція 13	Unrestricted File Upload: механізм атаки. Типи файлів та MIME types. Обхід фільтрів: extension bypass, magic bytes. Веб-шелли: PHP, ASP, JSP. Path Traversal (Directory Traversal). Local File Inclusion (LFI) та Remote File Inclusion (RFI). XXE	2

			через file upload. Методи захисту від file upload вразливостей.	
		самостійне вивчення	Вивчення структури різних файлових форматів. Аналіз методів валідації файлів. Дослідження веб-шеллів та backdoors.	2
	26	практична робота 13	Експлуатація unrestricted file upload та завантаження веб-шеллу. Імплементація безпечного file upload з валідацією magic bytes.	2
	27	лекція 14	XML: структура та парсинг. XXE (XML External Entity): механізм атаки. Типи XXE: in-band, out-of-band, blind. Impact: file disclosure, SSRF, DoS. Insecure Deserialization. Serialization в різних мовах: Java, Python, PHP. Remote Code Execution через десеріалізацію. Методи захисту від XXE та небезпечної десеріалізації.	2
		самостійна робота	Вивчення XML та DTD. Аналіз серіалізації в різних мовах програмування. Дослідження CVE пов'язаних з десеріалізацією.	2
	28	практична робота 14	Експлуатація XXE для читання системних файлів. Атака на десеріалізацію в Java з використанням ysoserial.	2
10	**SSRF та інші вразливості веб-застосунків**			**6**
	29	лекція 15	SSRF: механізм та вектори атаки. Blind SSRF. SSRF для доступу до внутрішніх ресурсів. SSRF та cloud metadata endpoints (AWS, Azure, GCP). Clickjacking (UI Redressing). Open Redirect. Security Misconfiguration. Using Components with Known Vulnerabilities. Security headers: HSTS, X-Frame-Options, X-Content-Type-Options.	2
		самостійне вивчення	Вивчення cloud metadata API. Аналіз реальних кейсів SSRF. Дослідження security headers та їх налаштування.	2
	30	практична робота 15	Експлуатація SSRF для доступу до внутрішніх ресурсів та cloud metadata. Налаштування security headers (X-Frame-Options, HSTS, CSP).	2
			Всього	90

6. ІНДИВІДУАЛЬНІ ЗАВДАННЯ

№	*Тема дисципліни*	*Вид завдання (реферати, дослідницькі, розрахункові роботи тощо)*	*Календарні строки і форма контролю*
1	SQL Injection атаки: від витоку даних до Remote Code Execution	реферат	квітень
2	Blind SQL Injection: техніки експлуатації та виявлення	реферат	квітень
3	NoSQL Injection: особливості атак на MongoDB та інші NoSQL бази	реферат	квітень
4	Command Injection: експлуатація вразливостей операційної системи через веб	реферат	квітень
5	LDAP Injection та методи захисту корпоративних каталогів	реферат	квітень
6	XML External Entity (XXE): від витоку файлів до SSRF	реферат	квітень
7	Server-Side Template Injection (SSTI): атаки на шаблонізатори	реферат	квітень
8	Prepared Statements vs ORM: ефективність захисту від SQL Injection	реферат	квітень
9	DOM-based XSS: особливості клієнтських вразливостей	реферат	квітень
10	Content Security Policy (CSP): налаштування та bypass техніки	реферат	квітень
11	Stored XSS атаки: реальні кейси та наслідки для бізнесу	реферат	квітень
12	CSRF токени: механізми генерації та валідації	реферат	квітень
13	SameSite cookies: новий стандарт захисту від CSRF	реферат	квітень
14	Mutation XSS: обхід фільтрів та санітизації	реферат	квітень
15	Insecure Direct Object References (IDOR): виявлення та експлуатація	реферат	квітень
16	Privilege Escalation: горизонтальне та вертикальне підвищення привілеїв	реферат	квітень
17	Session Hijacking та Session Fixation: атаки на механізми сесій	реферат	квітень
18	Bcrypt vs Argon2: сучасні алгоритми хешування паролів	реферат	квітень
19	OAuth 2.0 вразливості: реальні атаки на систему авторизації	реферат	квітень
20	Multi-Factor Authentication (MFA): bypass техніки та захист	реферат	квітень
21	OWASP API Security Top 10: огляд критичних вразливостей API	реферат	квітень
22	JWT (JSON Web Tokens): атаки та безпечна імплементація	реферат	квітень
23	GraphQL Introspection та DoS атаки	реферат	квітень

24	Rate Limiting: методи захисту API від зловживань	реферат	квітень
25	CORS misconfiguration: вразливості Cross-Origin Resource Sharing	реферат	квітень
26	SSL/TLS атаки: POODLE, BEAST, Heartbleed	реферат	квітень
27	Unrestricted File Upload: від веб-шеллів до RCE	реферат	квітень
28	Server-Side Request Forgery (SSRF): експлуатація внутрішніх ресурсів	реферат	квітень
29	Insecure Deserialization: Remote Code Execution через серіалізацію	реферат	квітень
30	Security Headers: HSTS, X-Frame-Options, CSP та їх роль у захисті	реферат	квітень

7. ПЕРЕЛІК ПИТАНЬ НА ЗАЛІК

1. Що таке безпека веб-застосунків та чому вона є критично важливою
2. Опишіть еволюцію загроз веб-безпеки від початку інтернету до сьогодні
3. Що таке OWASP Top 10 та яка його роль у безпеці веб-застосунків
4. Поясніть принципи безпечної розробки програмного забезпечення
5. Що таке життєвий цикл розробки (SDLC) та як інтегрувати безпеку в нього
6. Опишіть архітектуру клієнт-серверної моделі веб-застосунків
7. Поясніть різницю між HTTP та HTTPS протоколами
8. Що таке методи HTTP запитів та які з них є найбільш вразливими
9. Опишіть механізм роботи cookies та сесій у веб-застосунках
10. Що таке Same-Origin Policy (SOP) та навіщо вона потрібна
11. Поясніть модель моделювання загроз STRIDE
12. Що таке модель оцінки ризиків DREAD
13. Опишіть основні вектори атак на веб-застосунки
14. Що таке коди відповідей HTTP та які з них вказують на помилки безпеки
15. Поясніть роль заголовків HTTP у безпеці веб-застосунків
16. Що таке SQL Injection та як працює ця атака
17. Опишіть різницю між in-band, blind та out-of-band SQL Injection
18. Що таке Error-based SQL Injection
19. Поясніть механізм Union-based SQL Injection атаки
20. Що таке Boolean-based blind SQL Injection
21. Опишіть принцип роботи Time-based SQL Injection
22. Які наслідки може мати успішна SQL Injection атака
23. Що таке Prepared Statements та як вони захищають від SQL Injection
24. Поясніть роль Parameterized Queries у захисті від SQL Injection
25. Що таке ORM та які його переваги з точки зору безпеки
26. Опишіть безпечне використання Stored Procedures
27. Що таке принцип найменших привілеїв для баз даних
28. Поясніть роль валідації та санітизації вхідних даних
29. Що таке Web Application Firewall (WAF) та як він захищає від SQL Injection
30. Як виявити SQL Injection атаку через моніторинг

31. Що таке Command Injection та як вона експлуатується
32. Опишіть механізм LDAP Injection атаки
33. Що таке XPath Injection
34. Поясніть різницю між XML Injection та XXE
35. Що таке Server-Side Template Injection (SSTI)
36. Опишіть особливості NoSQL Injection атак
37. Які методи захисту є спільними для всіх типів injection атак
38. Поясніть, чому валідація на клієнті недостатня для захисту від injection
39. Що таке контекстуальне екранування даних
40. Опишіть принцип white-list валідації вхідних даних
41. Що таке Cross-Site Scripting (XSS) та як працює ця атака
42. Опишіть різницю між Reflected, Stored та DOM-based XSS
43. Що таке вектори атак XSS
44. Які наслідки може мати успішна XSS атака
45. Поясніть механізм викрадення cookies через XSS
46. Що таке мутації XSS
47. Опишіть роль браузерних XSS фільтрів та їх обмеження
48. Що таке Content Security Policy (CSP)
49. Поясніть директиви CSP та їх призначення
50. Що таке nonce та hash у контексті CSP
51. Опишіть різницю між input validation та output encoding
52. Що таке санітизація HTML
53. Поясніть роль DOMPurify у захисті від XSS
54. Що таке HTTPOnly та Secure flags для cookies
55. Що таке X-XSS-Protection заголовок та чи актуальний він сьогодні
56. Що таке Cross-Site Request Forgery (CSRF)
57. Опишіть різницю між XSS та CSRF атаками
58. Які сценарії експлуатації CSRF найбільш небезпечні
59. Поясніть різницю між GET та POST CSRF
60. Що таке Login CSRF
61. Які наслідки може мати успішна CSRF атака
62. Що таке CSRF токени та як вони працюють
63. Опишіть механізм SameSite cookies
64. Що таке Double Submit Cookie патерн
65. Поясніть основні механізми автентифікації у веб-застосунках
66. Що таке Multi-Factor Authentication (MFA)
67. Опишіть поняття Broken Authentication
68. Що таке brute force та credential stuffing атаки
69. Поясніть різницю між session fixation та session hijacking
70. Що таке безпечне хешування паролів
71. Опишіть алгоритм bcrypt та його переваги
72. Що таке Argon2 та чому він рекомендований для хешування паролів
73. Поясніть роль salt у хешуванні паролів

74. Які вразливості можуть бути в механізмах password reset
75. Що таке OAuth 2.0 та OpenID Connect
76. Що таке Broken Access Control
77. Опишіть поняття IDOR (Insecure Direct Object References)
78. Що таке Path Traversal атака
79. Поясніть різницю між горизонтальним та вертикальним Privilege Escalation
80. Що таке RBAC (Role-Based Access Control)
81. Опишіть принципи ABAC (Attribute-Based Access Control)
82. Що таке Missing Function Level Access Control
83. Поясніть поняття forced browsing
84. Які методи тестування контролю доступу ви знаєте
85. Як захиститися від IDOR вразливостей
86. Що таке OWASP API Security Top 10
87. Опишіть методи аутентифікації REST API
88. Що таке JWT (JSON Web Tokens) та як він працює
89. Поясніть структуру JWT токена
90. Які вразливості можуть бути в JWT
91. Що таке API Keys та їх обмеження
92. Опишіть роль rate limiting у безпеці API
93. Що таке GraphQL та його особливості
94. Поясніть GraphQL Introspection та чому це може бути небезпечно
95. Що таке batching attacks у GraphQL
96. Опишіть різницю між симетричним та асиметричним шифруванням
97. Що таке HTTPS/TLS та як працює handshake
98. Поясніть роль сертифікатів у TLS
99. Що таке cipher suites
100. Опишіть вразливість POODLE
101. Що таке Heartbleed вразливість
102. Поясніть поняття Certificate Pinning
103. Які криптографічні помилки найчастіше зустрічаються у веб-застосунках
104. Що таке шифрування at rest та in transit
105. Опишіть різницю між цифровим підписом та MAC
106. Що таке Unrestricted File Upload вразливість
107. Опишіть типи файлів та MIME types
108. Які методи обходу фільтрів file upload ви знаєте
109. Що таке веб-шелли
110. Поясніть різницю між Path Traversal, LFI та RFI
111. Які методи захисту від file upload вразливостей
112. Що таке XML та його структура
113. Опишіть механізм XXE (XML External Entity) атаки
114. Що таке in-band XXE
115. Поясніть різницю між out-of-band та blind XXE

116. Які наслідки може мати XXE атака
117. Як XXE пов'язане з SSRF
118. Які методи захисту від XXE
119. Що таке Insecure Deserialization
120. Опишіть серіалізацію в різних мовах програмування
121. Що таке Server-Side Request Forgery (SSRF)
122. Опишіть вектори SSRF атак
123. Що таке Blind SSRF
124. Поясніть використання SSRF для доступу до внутрішніх ресурсів
125. Що таке cloud metadata endpoints та як SSRF може їх експлуатувати
126. Які методи захисту від SSRF
127. Що таке Clickjacking (UI Redressing)
128. Опишіть механізм Open Redirect вразливості
129. Що таке Security Misconfiguration
130. Поясніть ризики використання компонентів з відомими вразливостями
131. Що таке HSTS заголовок
132. Опишіть роль X-Frame-Options
133. Що таке X-Content-Type-Options заголовок
134. Поясніть роль Referrer-Policy
135. Що таке Feature-Policy/Permissions-Policy
136. Опишіть поняття defense in depth
137. Що таке принцип fail securely
138. Поясніть важливість логування та моніторингу
139. Що таке incident response plan
140. Опишіть роль security testing у SDLC
141. Що таке CORS (Cross-Origin Resource Sharing)
142. Опишіть preflight request у CORS
143. Які ризики неправильної конфігурації CORS
144. Що таке API versioning
145. Поясніть поняття backward compatibility в API
146. Що таке throttling у контексті API
147. Опишіть різницю між authentication та authorization
148. Що таке zero trust security model
149. Поясніть принцип least privilege
150. Що таке security by design
151. Опишіть роль threat modeling у розробці
152. Що таке penetration testing
153. Поясніть різницю між vulnerability assessment та penetration testing
154. Що таке bug bounty програми
155. Опишіть процес responsible disclosure вразливостей
156. Продемонструйте базову SQL Injection атаку для обходу автентифікації

157. Напишіть SQL запит для Union-based SQL Injection з 3 колонками
158. Створіть приклад Prepared Statement на PHP для захисту від SQL Injection
159. Покажіть приклад Boolean-based blind SQL Injection payload
160. Продемонструйте Time-based SQL Injection payload для MySQL
161. Напишіть простий приклад Reflected XSS payload
162. Створіть приклад Stored XSS атаки через коментар
163. Покажіть DOM-based XSS payload
164. Напишіть базову CSP політику для захисту від XSS
165. Продемонструйте обхід простого XSS фільтра
166. Створіть HTML форму з CSRF токеном
167. Покажіть приклад CSRF атаки через GET запит
168. Напишіть код для генерації та валідації CSRF токена
169. Продемонструйте налаштування SameSite cookie
170. Створіть приклад bcrypt хешування пароля на Python
171. Покажіть Command Injection payload через параметр ping
172. Напишіть безпечний код для виконання системних команд
173. Продемонструйте простий XXE payload
174. Створіть приклад безпечного XML парсингу
175. Покажіть IDOR вразливість в URL параметрі
176. Напишіть код для перевірки прав доступу до об'єкта
177. Продемонструйте Path Traversal payload
178. Створіть приклад безпечної обробки шляхів до файлів
179. Покажіть базовий JWT токен та його структуру
180. Напишіть код для валідації JWT підпису
181. Продемонструйте GraphQL Introspection запит
182. Створіть приклад rate limiting middleware
183. Покажіть SSRF payload для доступу до localhost
184. Напишіть код для валідації URL в SSRF контексті
185. Продемонструйте налаштування CORS headers
186. Створіть приклад безпечного file upload обробника
187. Покажіть payload для обходу extension фільтра при file upload
188. Напишіть код для перевірки MIME type файлу
189. Продемонструйте базовий веб-шелл на PHP
190. Створіть приклад input validation функції
191. Покажіть output encoding для HTML контексту
192. Напишіть конфігурацію всіх основних security headers
193. Продемонструйте NoSQL Injection payload для MongoDB
194. Створіть приклад безпечного NoSQL запиту
195. Покажіть SSTI payload для Jinja2 шаблонізатора

8. Методи навчання

Під час вивчення дисципліни «Безпека вебзастосунків» у навчальному процесі застосовуються такі методи навчання: розповідь, бесіда, лекція, пояснення, демонстрація, ілюстрація, навчальна дискусія, диспут, самостійне виконання завдань лабораторної роботи, виконання вправ.

9. Контроль результатів навчання

9.1. Форми та засоби поточного і підсумкового контролю

Контроль знань здобувачів освіти здійснюється за модульно-рейтинговою системою.

Засобами діагностики та методами демонстрування результатів навчання здобувачів освіти з дисципліни є:

- індивідуальне опитування, фронтальне опитування;
- поточне тестування;
- підсумкове тестування з кожного змістовного модуля;
- директорська контрольна робота;
- залік.

Зміст курсу дисципліни «Безпека вебзастосунків» поділений на два змістових модулі. Кожний модуль включає в себе лекції, практичні заняття та самостійну роботу студентів і завершуються рейтинговим контролем рівня засвоєння знань програмного матеріалу відповідної частини курсу. У змістовий модуль 1 (ЗМ1) входять теми 1-3, у змістовий модуль 2 (ЗМ2) – теми 4-6, у змістовий модуль 2 (ЗМ2) – теми 7-10. Після завершення відповідно змістового модуля проводяться модульні контрольні роботи (МК). До модульної контрольної роботи допускаються студенти, які опрацювали весь обсяг теоретичного матеріалу в т. ч і матеріал самостійно, виконали практичні роботи. Рейтингову кількість балів студента формують бали, отримані за модульні контрольні роботи, які проводяться у формі тестування, та середній рейтинг виконання практичних робіт і відпрацювання семінарських занять. Участь студентів в контрольних заходах обов'язкова. МК проводиться у письмовій тестовій формі, тестові завдання обов’язково включають матеріал, який передбачено до самостійного опрацювання студентами. Студент, який не виконав вимоги щодо самостійної роботи чи будь якого іншого виду навчальної діяльності, не допускається до складання МК і даний модуль йому не зараховується. Семестрові бали (семестровий рейтинг) студент отримує як середнє арифметичне балів змістових модулів з усіх тем трьох змістових модулів. Оцінка навчальної успішності студентів здійснюється під час семестрового оцінювання у формі заліку, який передбачає виконання тестових завдань та вирішення практичного завдання.

9.2 Критерії оцінювання результатів начиння

Оцінка «відмінно» виставляється студенту, який має стійкі системні, глибокі і різнобічні знання, відмінно володіє матеріалом, знає нормативну і законодавчу базу та її застосування за певних умов, дає обґрунтовані, правильні відповіді на питання, доцільно використовує термінологію дисципліни (предмета), усвідомлює взаємозв'язок окремих розділів дисципліни, їхнє значення для майбутньої професії, виявляє творчі здібності у розумінні та використанні навчально-програмного матеріалу, проявляє здатність до самостійного оновлення і поповнення знань. Практичні завдання і задачі вирішує правильно, розрахунки проводить без помилок, отримує достовірні результати, правильно заповнює і складає документи, робить відповідні узагальнення і висновки та охайно оформляє виконані завдання та звіти.

- глибоке, теоретично обґрунтоване розкриття питання; розрахунки, зроблені без помилок, проведено повний аналіз, відображена власна позиція – оцінюються в **48-50 балів;**

- обґрунтоване розкриття питання чи/та розрахунки, зроблені з незначними неточностями, які істотно не впливають на правильність відповіді – **45-47 балів;**

Оцінка «добре» виставляється студенту, який знає викладений матеріал і добре ним володіє але допускає незначні помилки у формулюванні термінів, категорій, понять, використанні нормативно-правової бази, показує стійкий рівень знань з дисципліни і та професійної діяльності. Під час виконання практичних завдань, вирішення задач, проведення розрахунків допускає незначні помилки, але за допомогою викладача швидко орієнтується і знаходить правильні відповіді, правильно або з незначними помилками заповнює і складає документи, робить відповідні узагальнення і висновки та охайно оформляє виконані завдання та звіти.

- відповідь не дає повного розкриття питання, не проведено повний аналіз результатів розрахунків, немає власної позиції – **42-44 балів;**

- неповне розкриття питання, доведені до завершення розрахунки але не зроблено їх аналіз; загалом наявні достатні знання – **38-41 балів;**

Оцінка «задовільно» виставляється студенту, який посередньо володіє матеріалом, виявив знання основного навчально-програмного матеріалу в обсязі, необхідному для подальшого навчання та наступної роботи за професією, справляється з виконанням завдань, передбачених програмою, дає неправильну відповідь на окремі питання або на всі питання дає малообґрунтовані, невичерпні відповіді, знання має обмежені, несистемні, слабо орієнтується у нормативно-правових документах. Під час виконання практичних завдань, вирішення задач, проведення розрахунків припускається грубих помилок і тільки за допомогою викладача може виправити допущені помилки, із значними помилками заповнює і складає документи, поверхово робить узагальнення і висновки та не зовсім охайно оформляє виконані завдання та звіти. - питання розкрите фрагментарно,

наявні фактологічні помилки під час викладу чи/та помилки під час проведення розрахунків – **34-37 балів;**

- відповідь неповна, наявні суттєві помилки при викладі та проведенні розрахунків – **30-33 балів;**

Оцінка «незадовільно» виставляється студенту, який не виявив достатніх знань основного навчально-програмного матеріалу, дає відповіді лише на деякі питання або дає неправильні відповіді на питання, може відтворити кілька термінів, не знає термінології дисципліни і основних нормативно-правових документів, не може без допомоги викладача використати знання у подальшому навчанні, не спромігся оволодіти навичками самостійної роботи. Допускає принципові помилки у виконанні передбачених програмою завдань, вирішенні задач, проведенні розрахунків припускається грубих помилок і не може їх виправити, не виконує практичне завдання у визначений термін, із значними помилками заповнює і складає документи, не робить узагальнення і висновки та не охайно оформляє виконані завдання та звіти.

- відповідь має значні помилки елементарного рівня – **1-30 бали;**
- відсутність відповіді на питання – **0 балів.**

9.3. Оцінювання за формами контролю

	Заліковий модуль 1	Заліковий модуль 2	Заліковий модуль 3	Заліковий модуль (залік)	Разом
%	20	20	20	40	100
Мінімум	0	0	0	0	0
Максимум	50	50	50	50	50

9.4 Шкала оцінювання

Відсоток формування компетентностей та набуття програмних результатів навчання	**Рейтинг за п'ятдесятибальною шкалою**	**Оцінка за п'ятибальною шкалою**	**Запис у заліковій книжці студента та відомості**
96-100	48, 49, 50	5	відмінно
90-95	45, 46, 47	5	відмінно
84-89	42, 43, 44	4	добре
75-83	38, 39, 40, 41	4	добре
67-74	34, 35, 36, 37	3	задовільно
60-66	30, 31, 32, 33	3	задовільно
менше 60	0-29	2	незадовільно

10. МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ

- Витяг з навчального плану
- Програма навчальної дисципліни
- Плани занять
- Конспект лекцій з дисципліни
- Завдання для обов'язкової контрольної роботи
- Інструкційно-методичні матеріали до практичних занять
- Питання до заліків з модулів
- Контрольні тестові завдання до заліків з модулів
- Питання до заліку
- Залікові білети
- Навчальний посібник
- Роздавальний матеріал
- Презентації до тем

11. РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

Основна література:

1. Hoffman A. Web Application Security: Exploitation and Countermeasures for Modern Web Applications / A. Hoffman. – Sebastopol : O'Reilly Media, 2020. – 336 p.
2. Yaworski P. Real-World Bug Hunting: A Field Guide to Web Hacking / P. Yaworski. – San Francisco : No Starch Press, 2019. – 264 p.
3. OWASP Foundation. OWASP Top Ten Project [Електронний ресурс] / OWASP Foundation. – Режим доступу: https://owasp.org/www-project-top-ten/
4. Пірог О. В. Кібербезпека: підручник / О. В. Пірог. – Київ : Кондор, 2023. – 346 с.
5. PortSwigger. Web Security Academy [Електронний ресурс] / PortSwigger. – Режим доступу: https://portswigger.net/web-security
6. Kettle J. Web Security Academy Research [Електронний ресурс] / J. Kettle. – PortSwigger, 2021. – Режим доступу: https://portswigger.net/research

7. OWASP Foundation. OWASP API Security Top 10 [Електронний ресурс] / OWASP Foundation. – Режим доступу: https://owasp.org/www-project-api-security/
8. OWASP Foundation. OWASP Web Security Testing Guide [Електронний ресурс] / OWASP Foundation. – Режим доступу: https://owasp.org/www-project-web-security-testing-guide/
9. Stuttard D. The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws / D. Stuttard, M. Pinto. – 2nd ed. – Indianapolis : Wiley, 2018. – 912 p.
10. Clarke J. SQL Injection Attacks and Defense / J. Clarke. – 3rd ed. – Burlington : Syngress, 2017. – 820 p.

Допоміжні

1. NIST. Secure Software Development Framework [Електронний ресурс] / NIST. – 2022. – Режим доступу: https://csrc.nist.gov/projects/ssdf
2. CWE. Common Weakness Enumeration [Електронний ресурс] / MITRE Corporation. – Режим доступу: https://cwe.mitre.org/
3. HackerOne. The Hacker-Powered Security Report [Електронний ресурс] / HackerOne. – 2023. – Режим доступу: https://www.hackerone.com/resources
4. Bugcrowd. State of Bug Bounty Report [Електронний ресурс] / Bugcrowd. – 2023. – Режим доступу: https://www.bugcrowd.com/resources/reports/
5. Mozilla. Web Security Guidelines [Електронний ресурс] / Mozilla Foundation. – Режим доступу: https://infosec.mozilla.org/guidelines/web_security
6. Google. Web Fundamentals Security [Електронний ресурс] / Google Developers. – Режим доступу: https://developers.google.com/web/fundamentals/security
7. SANS Institute. Web Application Security [Електронний ресурс] / SANS Institute. – Режим доступу: https://www.sans.org/cyber-security-courses/web-app-penetration-testing-ethical-hacking/
8. PCI Security Standards Council. Payment Card Industry Data Security Standard [Електронний ресурс] / PCI SSC. – 2022. – Режим доступу: https://www.pcisecuritystandards.org/
9. W3C. Web Security Context Working Group [Електронний ресурс] / W3C. – Режим доступу: https://www.w3.org/Security/
10. IETF. RFC 6749: The OAuth 2.0 Authorization Framework [Електронний ресурс] / IETF. – 2012. – Режим доступу: https://tools.ietf.org/html/rfc6749