Робоча програма дисципліни «Захист інтернет ресурсів»

СПЕЦІАЛЬНІСТЬ 123 · КОМП'ЮТЕРНА ІНЖЕНЕРІЯ

БАКАЛАВР

120

Годин

Загальний обсяг дисципліни

4

Кредити ЄКТС

Відповідно до стандарту

4

Модулі

Змістовних блоки курсу

Загальна інформація про дисципліну

Ідентифікація

Назва: Захист інтернет ресурсів

Спеціальність: 123 Комп'ютерна інженерія

ОП: Організація захисту інформації в ІКС

Ступінь: Бакалавр

Обсяг: 120 годин / 4 кредити ЄКТС

Модулів: 4 змістовних блоки

Лекцій: 30 год. | **Практичних:** 15 год. | **Лабораторних:** 15 год. | **СРС:** 60 год.

Призначення дисципліни

Дисципліна «Захист інтернет ресурсів» формує у студентів системне розуміння методів та засобів забезпечення безпеки веб-додатків, інтернет-сервісів та інформаційно-комунікаційних систем у мережевому середовищі. Курс охоплює сучасні загрози інтернет-ресурсам, технології їх захисту, методи виявлення вразливостей та протидії кібератакам.

Дисципліна є обов'язковою для підготовки бакалаврів зі спеціальності «Комп'ютерна інженерія» за освітньою програмою «Організація захисту інформації в інформаційно-комунікаційних системах» та забезпечує формування фахових компетентностей у сфері захисту інтернет-ресурсів.

Загальні компетентності

Аналітичне мислення

Здатність до аналізу, синтезу та критичного оцінювання інформації про загрози безпеці інтернет-ресурсів: виявлення вразливостей, порівняння методів захисту, формування обґрунтованих висновків щодо рівня захищеності систем.

Комунікація

Здатність до усної та письмової комунікації: чітко пояснювати принципи захисту інтернет-ресурсів, аргументовано відповідати на запитання, оформлювати технічні звіти, аналітичні записки та документацію з безпеки.

Самоорганізація

Уміння самостійно навчатися, планувати роботу та організовувати виконання завдань у визначені строки, зокрема під час підготовки лабораторних робіт, звітів і дослідницьких проектів у сфері кібербезпеки.

Командна робота

Відповідальність, ініціативність та готовність працювати в команді під час групового аналізу кейсів з інцидентів безпеки, тестування захищеності систем та розробки заходів протидії кіберзагрозам.

Студент повинен вміти: аналізувати технічну та нормативну інформацію у сфері захисту інтернет-ресурсів; виявляти вразливості та планувати заходи захисту; дотримуватися дедлайнів; коректно комунікувати з викладачами та колегами; брати участь у командній роботі з аналізу безпеки систем.

Фахові компетентності

Розуміння загроз інтернет-ресурсам

Розуміння сутності та класифікації кіберзагроз інтернет-ресурсам: веб-атаки (XSS, SQL-ін'єкції, CSRF), DDoS-атаки, фішинг, шкідливе програмне забезпечення. Знання сучасного ландшафту загроз та методів їх виявлення.

Технології захисту веб-додатків

Здатність застосовувати технічні засоби захисту веб-додатків та інтернет-сервісів: налаштування міжмережевих екранів, систем виявлення вторгнень (IDS/IPS), SSL/TLS, HTTPS, WAF; проведення тестування на проникнення та аудиту безпеки.

Криптографічний захист даних

Знання методів криптографічного захисту інформації в інтернет-середовищі: симетричне та асиметричне шифрування, цифровий підпис, інфраструктура відкритих ключів (PKI), протоколи безпечної передачі даних.

Нормативно-правова база

Орієнтування в нормативно-правовій базі у сфері захисту інформації та кібербезпеки України; застосування стандартів ISO/IEC 27001, OWASP, NIST для організації захисту інтернет-ресурсів підприємства.

Результати навчання

01

Пояснення понять безпеки

Пояснювати сутність ключових понять і явищ: вразливість, загроза, атака, захист, аутентифікація, авторизація, шифрування, цілісність, конфіденційність, доступність (тріада CIA) інтернет-ресурсів.

02

Характеристика загроз та методів захисту

Характеризувати основні типи кіберзагроз інтернет-ресурсам, застосовувати методи аналізу ризиків, класифікувати засоби захисту та визначати оптимальні рішення для конкретних умов застосування.

03

Виявлення та усунення вразливостей

Аналізувати веб-додатки та інтернет-сервіси на наявність вразливостей за методологіями OWASP Top 10; використовувати інструменти тестування безпеки (Nmap, Burp Suite, OWASP ZAP) для виявлення і усунення загроз.

04

Розробка і реалізація заходів захисту

Розробляти та впроваджувати організаційно-технічні заходи захисту інтернет-ресурсів; складати технічну документацію, звіти з аудиту безпеки та рекомендації щодо підвищення рівня захищеності систем.

МОДУЛЬ 1

Основи безпеки інтернет-ресурсів та веб-технологій

1 — Тема 1.1

Вступ до захисту інтернет-ресурсів. Архітектура веб-систем. Моделі загроз та ризиків.

2 — Тема 1.2

Мережева безпека: протоколи TCP/IP, DNS, HTTP/HTTPS. Криптографічні основи захисту даних в інтернеті.

3 — Тема 1.3

Аутентифікація та авторизація в інтернет-системах. Управління ідентифікаційними даними та сесіями.

4 — Тема 1.4

Нормативно-правова база у сфері захисту інтернет-ресурсів. Міжнародні стандарти ISO/IEC 27001, OWASP, NIST.

МОДУЛЬ 1 · ТЕМА 1.1

Вступ до захисту інтернет-ресурсів. Архітектура веб-систем

Лекційний матеріал (2 год.)

Лекція 1: Поняття «інтернет-ресурс» та його складові. Архітектура клієнт-сервер. Модель OSI та рівні захисту. Тріада CIA (конфіденційність, цілісність, доступність). Класифікація загроз та атак на інтернет-ресурси. Поверхня атаки (attack surface). Основні вектори атак.

Моделі загроз: STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege). Методологія PASTA. Оцінка ризиків. Поняття вразливості (vulnerability), загрози (threat), ризику (risk). Стандарти та фреймворки: OWASP, NIST Cybersecurity Framework, ISO/IEC 27001.

Ключові питання лекції

- Архітектура сучасних веб-систем та їх компоненти
- Тріада CIA та її значення для захисту інтернет-ресурсів
- Класифікація загроз та атак на веб-додатки
- Моделі загроз STRIDE та PASTA
- Огляд стандартів і фреймворків кібербезпеки

Практичне заняття (1 год.)

Завдання 1. Складання моделі загроз для типового веб-додатку за методологією STRIDE: ідентифікація компонентів, виявлення загроз, оцінка ризиків.

Завдання 2. Кейс: аналіз реального кібер інциденту — виявлення вектора атаки, наслідків та можливих заходів захисту. Групове обговорення.

Лабораторна робота (1 год.)

Лаб. 1. Знайомство з інструментами аналізу мережевого трафіку (Wireshark): захоплення та аналіз пакетів HTTP/HTTPS, виявлення аномалій.

Самостійна робота (7 год.)

- Опрацювання: Пірог О. В. «Безпека вебдодатків» (2023) — розділ «Основи веббезпеки»
- Підготовка реферату: «OWASP Top 10: класифікація вразливостей сучасних веб-додатків»
- Складання таблиці «Порівняння стандартів кібербезпеки: ISO 27001, NIST CSF, OWASP»

Очікуваний результат: студент розуміє архітектуру веб-систем, класифікує загрози та застосовує методологію моделювання загроз.

МОДУЛЬ 1 · ТЕМА 1.2

Мережева безпека та криптографічні основи захисту

1

Мережеві протоколи

TCP/IP стек, DNS, HTTP/HTTPS. Вразливості протоколів та методи їх експлуатації.

2

Криптографія

Симетричне (AES), асиметричне (RSA) шифрування. Хеш-функції. Цифровий підпис.

3

PKI та сертифікати

Інфраструктура відкритих ключів. SSL/TLS. Сертифікати X.509. HTTPS та HTTP Strict Transport Security.

4

Захист каналу

VPN-технології. TLS 1.3. Certificate Transparency. HSTS, HPKP. Атаки на SSL/TLS та захист від них.

Лекційний матеріал (2 год.)

Огляд мережевих протоколів у контексті безпеки: TCP/IP, UDP, DNS, HTTP, HTTPS. Вразливості DNS (DNS spoofing, DNS hijacking). Симетрична та асиметрична криптографія: принципи, алгоритми AES, RSA, ECC. Хеш-функції MD5, SHA-2, SHA-3. Цифровий підпис. PKI та X.509 сертифікати. Протоколи SSL/TLS: версії, вразливості (POODLE, BEAST, Heartbleed), сучасні вимоги TLS 1.3. Технологія HTTPS, HSTS, Certificate Transparency.

Практичне заняття (1 год.) та СРС (7 год.)

Практика: Аналіз TLS-сертифікатів реальних сайтів; виявлення помилок конфігурації SSL/TLS за допомогою онлайн-інструментів (SSL Labs); обговорення кейсу «Heartbleed: вразливість, що потрясла інтернет».

Лаб. 2: Налаштування HTTPS та SSL/TLS на тестовому веб-сервері Apache/Nginx; генерація самопідписаного сертифікату та перевірка конфігурації.

СРС: Опрацювання: Маліновський В. І., Куперштейн Л. М., Каплун В. А. «Кібербезпека мобільних пристроїв та інтернету речей» (ВНТУ, 2024) — розділ «Безпека передачі даних»; підготовка аналітичної записки «TLS 1.3 vs TLS 1.2: переваги та вимоги міграції».

МОДУЛЬ 1 · ТЕМА 1.3–1.4

Аутентифікація, авторизація та нормативна база захисту

Тема 1.3 — Аутентифікація та управління доступом (Лекція 3, 2 год.)

Ідентифікація, аутентифікація, авторизація (IAA). Методи аутентифікації: парольна, багатофакторна (MFA), токени, біометрія. Управління сесіями: Session ID, Cookie, JWT-токени. Атаки на аутентифікацію: brute-force, credential stuffing, session hijacking, IDOR. Протоколи OAuth 2.0, OpenID Connect, SAML. SSO (Single Sign-On): переваги та ризики. Управління привілейованим доступом (PAM).

Практика (1 год.): Аналіз вразливостей механізмів аутентифікації на тестових стендах; моделювання атаки brute-force та налаштування захисту (rate limiting, CAPTCHA, блокування).

Лаб. 3 (1 год.): Налаштування MFA для тестового веб-додатку; аналіз JWT-токенів та виявлення помилок їх реалізації за допомогою jwt.io.

СРС (7 год.): Опрацювання: Пірог О. В. «Безпека вебдодатків» (2023) — розділи «Контроль доступу», «Управління сесіями»; підготовка звіту «OAuth 2.0 та OpenID Connect: механізм роботи та безпека».

Тема 1.4 — Нормативно-правова база захисту інтернет-ресурсів (Лекція 4, 2 год.)

Законодавство України у сфері кібербезпеки: Закон «Про основні засади забезпечення кібербезпеки України» (2017), Стратегія кібербезпеки України. Регулятори: ДССЗЗІ, CERT-UA, Національний координаційний центр кібербезпеки. Стандарти: ISO/IEC 27001:2022, OWASP ASVS, NIST SP 800-53. GDPR та захист персональних даних в інтернеті. Закон «Про захист персональних даних». Відповідальність за кіберзлочини (ст. 361–363 КК України). Поняття критичної інформаційної інфраструктури (КІІ).

Практика (1 год.): Аналіз вимог стандарту ISO/IEC 27001:2022 до захисту інтернет-сервісів; кейс «GDPR у практиці українських веб-компаній: вимоги та штрафи».

Лаб. 4 (1 год.): Аналіз публічної звітності CERT-UA про інциденти за 2023–2024 рр.; складання реєстру загроз для модельного підприємства.

СРС (7 год.): Опрацювання: Сілін Є. С., Кадубовський О. А. «Основи кібербезпеки» (Дніпро, 2023) — розділ «Нормативно-правове регулювання кібербезпеки»; підготовка аналітичної записки «Кримінальна відповідальність за кіберзлочини в Україні».

МОДУЛЬ 2

Атаки на веб-додатки та методи протидії (OWASP Top 10)

Тема 2.1

Ін'єкційні атаки: SQL-ін'єкції, XSS (Cross-Site Scripting), XXE, SSRF. Виявлення та протидія.

Тема 2.2

CSRF, Clickjacking, IDOR та порушення контролю доступу. Методи захисту бізнес-логіки.

Тема 2.3

DoS та DDoS-атаки: різновиди, інструменти, наслідки. Засоби захисту та пом'якшення атак.

Тема 2.4

Безпечне програмування та SDLC. DevSecOps. Моделювання загроз на етапі розробки.

МОДУЛЬ 2 · ТЕМА 2.1

Ін'єкційні атаки та міжсайтовий скриптинг (XSS)

Лекційний матеріал (2 год.)

SQL-ін'єкції: принцип дії, різновиди (in-band, inferential/blind, out-of-band), методи виявлення (sqlmap), превентивні заходи (параметризовані запити, ORM, prepared statements). XSS (Cross-Site Scripting): Stored, Reflected, DOM-based XSS. Методи виявлення та блокування. Content Security Policy (CSP). XXE (XML External Entity) Injection. SSRF (Server-Side Request Forgery). Вразливості десеріалізації. Огляд OWASP Top 10 (2021): A01–A10.

Ключові питання

- Механізм SQL-ін'єкції та методи її виявлення
- Різновиди XSS та техніки захисту
- Content Security Policy (CSP) як засіб захисту
- SSRF та XXE: принцип дії та протидія
- OWASP Top 10 (2021): огляд актуальних загроз

Практичне заняття (1 год.)

Завдання 1. Аналіз вразливого веб-додатку DVWA (Damn Vulnerable Web Application): демонстрація SQL-ін'єкцій різних рівнів складності, обговорення заходів захисту.

Завдання 2. Кейс: «Реальні інциденти SQL-ін'єкцій в Україні — аналіз, наслідки, уроки». Групова робота та презентація висновків.

Лабораторна робота (1 год.)

Лаб. 5. Виявлення та експлуатація SQL-ін'єкцій у навчальному середовищі DVWA (рівень low/medium); виправлення вразливості у вихідному коді; перевірка результату.

Самостійна робота (7 год.)

- Опрацювання: Пірог О. В. «Безпека вебдодатків» (2023) — розділи «SQL-ін'єкції», «XSS», «XXE»
- Підготовка реферату: «OWASP Top 10 (2021): аналіз вразливостей та методи захисту»
- Складання таблиці «Класифікація ін'єкційних атак: вид, механізм, приклад, захист»

Очікуваний результат: студент вміє ідентифікувати SQL-ін'єкції та XSS у вихідному коді, застосовувати превентивні заходи захисту.

МОДУЛЬ 2 · ТЕМА 2.2

CSRF, Clickjacking, IDOR та порушення контролю доступу

CSRF

Cross-Site Request Forgery: підроблення міжсайтових запитів. CSRF-токени, SameSite Cookie.

IDOR

Insecure Direct Object Reference: несанкціонований доступ до ресурсів через маніпуляцію ідентифікаторами.

Захист

Принцип мінімальних привілеїв. Перевірка авторизації на серверній стороні. Аудит доступу.

Clickjacking

Накладання прозорих фреймів. X-Frame-Options, CSP frame-ancestors як захист.

Broken Access Control

#1 OWASP 2021. Горизонтальне та вертикальне ескалювання привілеїв. RBAC, ABAC.

Лекційний матеріал (2 год.)

CSRF (Cross-Site Request Forgery): механізм атаки, CSRF-токени, атрибут SameSite для Cookie, подвійна перевірка Cookie. Clickjacking: iframe-атаки, X-Frame-Options, CSP frame-ancestors. IDOR та порушення контролю доступу (Broken Access Control — OWASP A01:2021): горизонтальне та вертикальне ескалювання. Моделі управління доступом: RBAC, ABAC, DAC, MAC. Принцип мінімальних привілеїв (PoLP). Виявлення вразливостей контролю доступу та методи захисту.

Практика (1 год.) та СРС (7 год.)

Практика: Демонстрація CSRF-атаки та налаштування CSRF-токенів у тестовому додатку; аналіз вразливостей IDOR в DVWA; дискусія «Broken Access Control — найнебезпечніша вразливість 2021 року: чому?».

Лаб. 6 (1 год.): Виявлення CSRF-вразливостей за допомогою Burp Suite; реалізація захисту за допомогою CSRF-токенів та SameSite Cookie; перевірка результату.

СРС: Опрацювання: Пірог О. В. «Безпека вебдодатків» (2023) — розділи «CSRF», «Контроль доступу»; підготовка аналітичної записки «IDOR у реальних системах: приклади витоків даних та методи запобігання».

МОДУЛЬ 2 · ТЕМА 2.3–2.4

DDoS-атаки, безпечне програмування та DevSecOps

Тема 2.3 — DoS та DDoS-атаки (Лекція 7, 2 год.)

DoS та DDoS: класифікація (об'ємні, протокольні, атаки на рівні додатку). Ботнети. Інструменти атак (LOIC, HOIC, hping3). Статистика DDoS-атак в Україні у 2022–2024 рр. Методи захисту: rate limiting, anycast, CDN, WAF, Anti-DDoS сервіси (Cloudflare, Akamai). Технологія BGP Blackholing. Налаштування firewall проти DDoS. SYN flood та захист від нього (SYN cookies).

Практика (1 год.): Аналіз реальних DDoS-атак на Ukrainian інтернет-ресурси; моделювання SYN flood у ізольованому середовищі та налаштування захисту; обговорення звітів CERT-UA.

Лаб. 7 (1 год.): Налаштування rate limiting та базових правил WAF на тестовому сервері nginx/Apache; тестування ефективності захисту за допомогою навантажувальних тестів.

СРС (7 год.): Опрацювання: Маліновський В. І., Куперштейн Л. М., Каплун В. А. «Кібербезпека мобільних пристроїв та інтернету речей» (ВНТУ, 2024) — розділ «Захист від DDoS-атак»; підготовка звіту «DDoS-атаки на критичну інфраструктуру України: аналіз інцидентів 2022–2024 рр.».

Тема 2.4 — Безпечне програмування та DevSecOps (Лекція 8, 2 год.)

Безпечний цикл розробки ПЗ (SDLC): фази та інтеграція безпеки. DevSecOps: зміщення безпеки «вліво» (shift-left security). Моделювання загроз на етапі проектування. SAST (Static Application Security Testing) та DAST (Dynamic AST). Інструменти: SonarQube, OWASP ZAP, Bandit. Принципи безпечного програмування: валідація вхідних даних, параметризовані запити, безпечна обробка помилок. Управління секретами (secrets management): HashiCorp Vault, AWS Secrets Manager. Security Code Review.

Практика (1 год.): Аналіз вразливого коду: виявлення дефектів безпеки (hardcoded credentials, SQL concat, XSS у шаблонах); демонстрація SAST-інструментів; кейс «DevSecOps у практиці Ukrainian IT-компаній».

Лаб. 8 (1 год.): Статичний аналіз коду тестового веб-додатку за допомогою SonarQube або Bandit; виявлення та класифікація вразливостей; підготовка звіту.

СРС (7 год.): Підготовка аналітичної записки «DevSecOps як сучасна практика інтеграції безпеки у розробку: інструменти та переваги».

МОДУЛЬ 3

Захист мережевої інфраструктури та хмарних сервісів

Тема 3.1

Міжмережеві екрани (Firewall) та системи виявлення/запобігання вторгненням (IDS/IPS). WAF.

Тема 3.2

Безпека DNS та електронної пошти. SPF, DKIM, DMARC. Захист від фішингу та спуфінгу.

Тема 3.3

Безпека хмарних сервісів (Cloud Security). AWS/Azure/GCP: моделі відповідальності, IAM, захист даних.

Тема 3.4

Соціальна інженерія та фішинг як загрози інтернет-ресурсам. Методи виявлення та протидії.

МОДУЛЬ 3 · ТЕМА 3.1

Міжмережеві екрани, IDS/IPS та WAF

Лекційний матеріал (2 год.)

Класифікація міжмережевих екранів (Firewall): пакетні фільтри, stateful inspection, proxy, NGFW (Next-Generation Firewall). Налаштування правил firewall. Системи виявлення вторгнень (IDS) та запобігання вторгненням (IPS): принципи роботи, сигнатурний та аномальний аналіз, HIDS/NIDS. Snort та Suricata. WAF (Web Application Firewall): правила ModSecurity, OWASP Core Rule Set (CRS). DMZ-архітектура. Honeypot та Honeynet. Моніторинг та журналювання подій безпеки (SIEM: Splunk, ELK Stack).

Ключові питання

- Класифікація та принципи роботи міжмережевих екранів
- IDS vs IPS: переваги та обмеження
- WAF: принцип роботи та правила OWASP CRS
- SIEM: збір та кореляція подій безпеки
- DMZ-архітектура як принцип ешелонованого захисту

Практичне заняття (1 год.)

Завдання 1. Аналіз журналів (logs) веб-сервера: виявлення ознак сканування портів, спроб підбору паролів та SQL-ін'єкцій у реальних логах.

Завдання 2. Кейс: «Архітектура захисту інтернет-ресурсів великого Ukrainian інтернет-банку». Групова розробка схеми захисту та захист рішення.

Лабораторна робота (1 год.)

Лаб. 9. Встановлення та налаштування ModSecurity WAF для Apache/Nginx; тестування правил OWASP CRS на тестових атаках; аналіз журналів WAF.

Самостійна робота (7 год.)

- Опрацювання: Сілін Є. С., Кадубовський О. А. «Основи кібербезпеки» (Дніпро, 2023) — розділ «Мережева кібербезпека»
- Підготовка реферату: «SIEM-системи: принципи роботи та застосування для моніторингу безпеки веб-ресурсів»
- Складання схеми «Ешелонований захист (Defense in Depth) для типового веб-сервісу»

Очікуваний результат: студент вміє налаштовувати базові засоби захисту мережі та аналізувати журнали подій безпеки.

МОДУЛЬ 3 · ТЕМА 3.2

Безпека DNS та електронної пошти. Протидія фішингу

Лекційний матеріал (2 год.)

Безпека DNS: атаки DNS spoofing, DNS cache poisoning, DNS hijacking, typosquatting. DNSSEC. DNS-over-HTTPS (DoH) та DNS-over-TLS (DoT). Безпека електронної пошти: протоколи SMTP, IMAP, POP3 та їх вразливості. Аутентифікація відправника: SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail), DMARC. Спуфінг email та захист від нього. Фішинг та спір-фішинг: механізм, ознаки, інструменти виявлення. Email-шлюзи та антиспам-системи. Технології email encryption: S/MIME, PGP.

Практика (1 год.) та СРС (7 год.)

Практика: Налаштування SPF, DKIM та DMARC записів для тестового домену; перевірка конфігурації через онлайн-інструменти (MXToolbox, DMARC Analyzer); розбір реального фішингового листа — ознаки та методи виявлення.

Лаб. 10 (1 год.): Аналіз заголовків підозрілого email; налаштування SPF/DKIM/DMARC у DNS-записах; перевірка ефективності захисту.

СРС: Опрацювання: Онищенко С., Глушко А. «Аналітичний вимір кібербезпеки України в умовах зростання викликів та загроз» (2022) — розділ «Фішинг та соціальна інженерія»; підготовка аналітичної записки «Фішинг проти Ukrainian організацій: тактики APT-груп та методи захисту».

Очікуваний результат: студент вміє налаштовувати захист DNS та електронної пошти, розпізнавати фішингові атаки та аналізувати їх механізм.

МОДУЛЬ 3 · ТЕМА 3.3–3.4

Безпека хмарних сервісів та соціальна інженерія

Тема 3.3 — Безпека хмарних сервісів (Лекція 11, 2 год.)

Моделі хмарних сервісів: IaaS, PaaS, SaaS — моделі спільної відповідальності за безпеку. Основні загрози хмарних середовищ: неправильна конфігурація (misconfiguration), витоки через публічні S3-бакети, небезпечні API. IAM (Identity and Access Management) у хмарі. Захист даних у хмарі: шифрування at-rest та in-transit, CASB. Container security: Docker, Kubernetes. Безпека API (REST API, GraphQL): OWASP API Security Top 10. Хмарні сервіси безпеки: AWS Shield, Azure Security Center, Cloudflare.

Практика (1 год.): Аналіз конфігурації хмарного середовища на наявність типових помилок; аудит прав доступу IAM; кейс «Витік даних через неправильно налаштований S3-бакет».

Лаб. 11 (1 год.): Налаштування базових правил безпеки в тестовому хмарному середовищі (або локальний Docker-стенд); аналіз OWASP API Security Top 10 на практичних прикладах.

СРС (7 год.): Опрацювання: Маліновський В. І., Куперштейн Л. М., Каплун В. А. «Кібербезпека мобільних пристроїв та інтернету речей» (ВНТУ, 2024) — розділ «Безпека хмарних сервісів»; підготовка звіту «OWASP API Security Top 10: аналіз вразливостей та рекомендації».

Тема 3.4 — Соціальна інженерія та психологічні атаки (Лекція 12, 2 год.)

Соціальна інженерія як нетехнічний вектор атак: класифікація (фішинг, вішинг, смішинг, претекстинг, бейтинг). Психологічні принципи маніпуляції (Чалдіні). Техніки атак: CEO fraud, BEC (Business Email Compromise). Методи виявлення та протидії: навчання персоналу, процедури верифікації, Security Awareness. Фішинг-симуляції та їх ефективність. Вплив соціальної інженерії на безпеку інтернет-ресурсів організацій.

Практика (1 год.): Аналіз реальних кейсів соціальної інженерії проти Ukrainian організацій; розробка навчальної програми Security Awareness для умовної компанії; дискусія «Людський фактор — найслабша ланка в безпеці».

Лаб. 12 (1 год.): Аналіз фішингових сайтів та email з використанням відкритих інструментів (VirusTotal, PhishTank, URLScan.io); складання звіту про ознаки фішингу.

СРС (7 год.): Підготовка аналітичної записки «BEC (Business Email Compromise) — глобальна загроза та засоби захисту організацій».

МОДУЛЬ 4

Тестування безпеки, реагування на інциденти та перспективи захисту

Тема 4.1

Тестування на проникнення (Penetration Testing): методологія, інструменти Kali Linux, Metasploit, Burp Suite.

Тема 4.2

Реагування на інциденти (Incident Response). SIEM та SOC. Криміналістичний аналіз (Digital Forensics).

Тема 4.3

Захист персональних даних та API. GDPR, Закон «Про захист персональних даних». REST API Security.

Тема 4.4

Сучасні тренди: Zero Trust, AI у кібербезпеці, кіберстійкість. Кіберзахист в умовах воєнного стану.

МОДУЛЬ 4 · ТЕМА 4.1

Тестування на проникнення (Penetration Testing)

Лекційний матеріал (2 год.)

Поняття пентесту та його відмінність від реальної атаки. Правові аспекти: Bug Bounty, відповідальне розкриття (responsible disclosure), договірна база. Методологія пентесту: PTES (Penetration Testing Execution Standard), OWASP Testing Guide. Фази: розвідка (OSINT, Shodan, Maltego), сканування (Nmap), ідентифікація вразливостей, експлуатація (Metasploit), пост-експлуатація, звітування. Інструментарій: Kali Linux, Burp Suite Pro, OWASP ZAP, Nikto, Dirb/Gobuster. Веб-пентест vs мережевий пентест. Black/White/Grey box тестування.

Ключові питання

- Методологія PTES та OWASP Testing Guide
- Фази пентесту та їх зміст
- Інструменти розвідки та сканування
- Правові аспекти пентесту в Україні
- Bug Bounty програми: переваги та практика

Практичне заняття (1 год.)

Завдання 1. Пасивна та активна розвідка тестового цільового ресурсу: збір OSINT (WHOIS, Shodan, Google dorks), сканування Nmap, аналіз результатів.

Завдання 2. Дискусія: «Етичний хакінг vs. Bug Bounty — де межа відповідальності?». Аналіз реальних Bug Bounty програм (HackerOne, Bugcrowd).

Лабораторна робота (1 год.)

Лаб. 13. Комплексний пентест тестового веб-додатку (DVWA або WebGoat) у ізольованому середовищі: сканування, виявлення вразливостей, підготовка звіту пентесту за стандартною структурою.

Самостійна робота (7 год.)

- Опрацювання: Пірог О. В. «Безпека вебдодатків» (2023) — розділи «Тестування безпеки», «Пентестинг (Nmap, Burp Suite, Metasploit)»
- Підготовка реферату «Bug Bounty програми в Україні та світі: досвід та перспективи»
- Аналіз структури звіту пентесту за методологією PTES

Очікуваний результат: студент вміє проводити базовий пентест веб-ресурсу, використовувати інструменти Kali Linux та складати технічний звіт.

МОДУЛЬ 4 · ТЕМА 4.2

Реагування на інциденти та цифрова криміналістика

Лекційний матеріал (2 год.)

Lifecycle інциденту кібербезпеки. Процес реагування на інциденти (IR): Preparation, Identification, Containment, Eradication, Recovery, Lessons Learned (PICERL / NIST SP 800-61). SOC (Security Operations Center): функції, рівні аналітиків, інструменти. SIEM (Security Information and Event Management): кореляція подій, правила виявлення, дашборди. Digital Forensics: збереження доказів, ланцюг зберігання (chain of custody), аналіз дисків та мережевого трафіку. Threat Intelligence та MITRE ATT&CK Framework. Інциденти в Україні: досвід CERT-UA.

Практика (1 год.) та СРС (7 год.)

Практика: Розбір реального інциденту кібератаки на Ukrainian організацію (за звітами CERT-UA): відновлення хронології, визначення TTP атакувальника за MITRE ATT&CK, розробка плану усунення наслідків та покращення захисту.

Лаб. 14 (1 год.): Аналіз логів та артефактів змодельованого інциденту (підготовлений набір даних): виявлення зловмисної активності, відновлення хронології атаки, складання IR-звіту.

СРС: Опрацювання: Онищенко С., Глушко А. «Аналітичний вимір кібербезпеки України» (2022) — розділ «Реагування на кіберінциденти»; підготовка аналітичної записки «CERT-UA: роль у захисті Ukrainian інтернет-ресурсів під час воєнного стану».

Очікуваний результат: студент вміє структурувати процес IR, аналізувати артефакти інцидентів, застосовувати MITRE ATT&CK для класифікації атак.

МОДУЛЬ 4 · ТЕМА 4.3–4.4

Захист персональних даних, API та сучасні тренди кібербезпеки

Тема 4.3 — Захист персональних даних та безпека API (Лекція 15, 2 год.)

Персональні дані в контексті інтернет-ресурсів: класифікація, вимоги до обробки. GDPR: принципи, права суб'єктів даних, обов'язки операторів. Закон України «Про захист персональних даних». Data Protection by Design and by Default. Безпека REST API та GraphQL: OWASP API Security Top 10. Проблеми надмірного впливу (Excessive Data Exposure), масового призначення (Mass Assignment), відсутності ліміту ресурсів. Аутентифікація та авторизація API (OAuth 2.0, API keys). API Gateway та WAF для захисту API.

Практика (1 год.): Аналіз вразливого API на основі OWASP API Security Top 10; виявлення проблем Excessive Data Exposure та Broken Object Level Authorization; розробка рекомендацій щодо усунення.

Лаб. 15 (1 год.): Тестування безпеки REST API за допомогою Postman та OWASP ZAP; виявлення вразливостей, складання звіту та рекомендацій з виправлення.

СРС (7 год.): Опрацювання нормативних документів: Закон «Про захист персональних даних», рекомендації УПОВНОВАЖЕНОГО; підготовка аналітичної записки «GDPR для Ukrainian IT-компаній: вимоги та практика виконання».

Тема 4.4 — Сучасні тренди та перспективи захисту (Лекція 16, 2 год.)

Концепція Zero Trust: «не довіряй нікому, перевіряй все». Мікросегментація мережі. Штучний інтелект та Machine Learning у кібербезпеці: виявлення аномалій, автоматизоване реагування, AI-powered атаки. Quantum Computing та постквантова криптографія. Кіберстійкість (Cyber Resilience) як стратегічна ціль. Supply chain attacks: SolarWinds, XZ Utils. Особливості кіберзахисту в умовах воєнного стану в Україні: досвід, виклики, перспективи. Кібервійна та державна кіберстратегія України.

Практика (1 год.): Дискусія «Zero Trust Architecture: від концепції до реалізації в Ukrainian організаціях»; аналіз кейсу supply chain attack та уроки для розробників; захист міні-проекту «Комплексний захист інтернет-ресурсів підприємства».

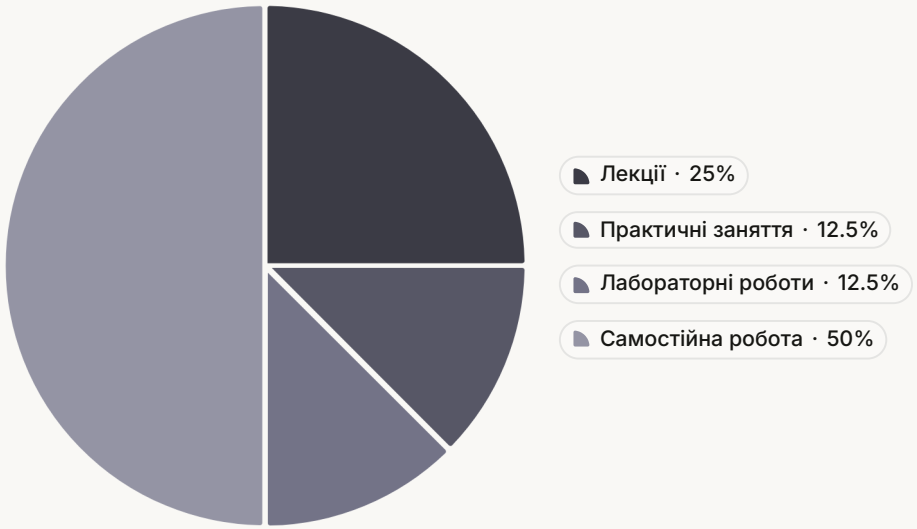
СРС (7 год.): Опрацювання: Онищенко С., Глушко А. «Аналітичний вимір кібербезпеки України» (2022) — розділ «Кіберзагрози в умовах воєнного стану»; підготовка аналітичної записки «Zero Trust як стратегія захисту інтернет-ресурсів: практика впровадження».

Розподіл навчального часу — 120 годин

Модуль	Тема	Лекції (год.)	Практ. (год.)	Лаб. (год.)	СРС (год.)
Модуль 1	Тема 1.1 — Архітектура та моделі загроз	2	1	1	7
	Тема 1.2 — Мережева безпека та криптографія	2	1	1	7
	Тема 1.3 — Аутентифікація та авторизація	2	1	1	7
	Тема 1.4 — Нормативно-правова база	2	1	1	7
Модуль 2	Тема 2.1 — SQL-ін'єкції та XSS	2	1	1	7
	Тема 2.2 — CSRF, Clickjacking, IDOR	2	1	1	7
	Тема 2.3 — DDoS-атаки та захист	2	1	1	7
	Тема 2.4 — Безпечне програмування, DevSecOps	2	1	1	7
Модуль 3	Тема 3.1 — Firewall, IDS/IPS, WAF	2	1	1	7
	Тема 3.2 — DNS, email безпека, фішинг	2	1	1	7
	Тема 3.3 — Безпека хмарних сервісів	2	1	1	7
	Тема 3.4 — Соціальна інженерія	2	1	1	7
Модуль 4	Тема 4.1 — Пентест	2	1	1	7
	Тема 4.2 — Реагування на інциденти	2	1	1	7
	Тема 4.3 — Захист ПД та API Security	2	1	1	7
	Тема 4.4 — Сучасні тренди кібербезпеки	2	1	1	7
Разом	**16 тем**	**30**	**15**	**15**	**60**

Загальний обсяг: 120 годин = 4 кредити ЄКТС. Розподіл є орієнтовним і може коригуватися відповідно до специфіки навчального процесу.

Структура навчального часу



Коментар до розподілу

Загальний обсяг — **120 годин (4 кредити ЄКТС)** — розподілено між чотирма формами роботи для забезпечення балансу між теорією, практикою та технічними навичками.

Лекції — 30 год. (25%)

Системне подання теоретичного матеріалу з безпеки інтернет-ресурсів із використанням актуальних прикладів атак, технологій захисту та стандартів галузі.

Практичні — 15 год. (12,5%)

Відпрацювання аналітичних навичок: аналіз кейсів інцидентів, розробка моделей загроз, обговорення технічних рішень та захист міні-проектів.

Лабораторні — 15 год. (12,5%)

Практичні навички роботи з інструментами кібербезпеки (Wireshark, Burp Suite, OWASP ZAP, ModSecurity, Nmap): виявлення вразливостей та налаштування захисту.

Самостійна робота — 60 год. (50%)

Поглиблене вивчення, підготовка звітів та аналітичних записок, робота з фаховою літературою. Становить **50% обсягу дисципліни**.

Самостійна робота студентів — Детальний опис

Опрацювання літератури

Поглиблене вивчення теоретичного матеріалу за навчальними посібниками з захисту інтернет-ресурсів (Пірог, Маліновський, Сілін та ін.), нормативно-правовими актами, стандартами OWASP та ISO/IEC. Студент конспектує ключові положення, виділяє головні поняття та порівнює підходи різних авторів.

Індивідуальні завдання

Виконання аналітичних завдань (аналіз кейсів інцидентів, порівняльний аналіз технологій захисту, складання моделей загроз); підготовка технічних звітів, аналітичних записок та міні-досліджень з актуальних проблем захисту інтернет-ресурсів.

Робота з інформаційними ресурсами

Опрацювання офіційних ресурсів: CERT-UA (**cert.gov.ua**), ДССЗЗІ (**cip.gov.ua**), OWASP (**owasp.org**), NIST (**csrc.nist.gov**). Аналіз наукових статей, звітів про загрози, пошук актуальної інформації для навчальних завдань.

Підготовка до занять

Підготовка до практичних та лабораторних занять (опрацювання теорії, підготовка інструментів); підготовка до тестувань (ключові терміни, класифікації загроз); підготовка до контрольних робіт за кожним модулем.

Форми контролю знань

1	2	3
Поточний контроль	Проміжний контроль	Підсумковий контроль
Завдання: тестові вправи та усне опитування за темами змістовного модуля. Оцінюються: якість виконання лабораторних робіт та практичних завдань, рівень засвоєння матеріалу, вміння застосовувати інструменти захисту. Проводиться після кожної теми у формі тестування (10–15 питань) або захисту лабораторної роботи.	Самостійна робота — комплексне ситуаційне завдання або аналітична записка, що охоплює теми змістовного модуля (теоретичні питання, аналіз загроз, розробка заходів захисту). Оцінюються повнота відповіді, технічна грамотність та обґрунтованість рекомендацій. Проводиться після кожного модуля.	Іспит відповідно до навчального плану. Форма: тестування (теоретичні питання) та практичне завдання з аналізу безпеки. Підсумкова оцінка враховує поточний, проміжний та підсумковий контроль: **100-бальна система** з переведенням у національну шкалу та ЄКТС (A, B, C, D, E, FX, F).

Методи викладання

Викладання дисципліни «Захист інтернет ресурсів» поєднує класичні академічні та інтерактивні методи, що забезпечує формування не лише міцної теоретичної бази, а й практичних навичок роботи з реальними інструментами кібербезпеки, необхідних для фахівця з комп'ютерної інженерії.

Лекції

Системне подання теоретичного матеріалу з використанням схем архітектур захисту, демонстрацій атак та прикладів реальних інцидентів; студенти ведуть конспекти та ставлять уточнювальні запитання.

Кейс–аналіз інцидентів

Розбір реальних інцидентів кібербезпеки (звіти CERT-UA, CVE, публічні post-mortems); формування навичок аналізу векторів атак та розробки захисних заходів.

Лабораторні практикуми

Робота у навчальних стендах (DVWA, WebGoat, Metasploitable) із реальними інструментами (Burp Suite, Wireshark, OWASP ZAP, Nmap, ModSecurity); формування практичних навичок захисту.

Дискусії

Обговорення дискусійних питань: Zero Trust vs. традиційна модель периметру; AI у кібербезпеці — допомога чи загроза; Bug Bounty як інструмент покращення безпеки.

Самостійне дослідження

Підготовка аналітичних записок, звітів та презентацій за обраними темами захисту інтернет-ресурсів; розвиток навичок пошуку та систематизації актуальної інформації з кібербезпеки.

Пентест–практикуми

Проведення контрольованого тестування на проникнення у ізольованих середовищах; відпрацювання повного циклу: розвідка → сканування → виявлення → звітування.

Усі методи спрямовані на формування компетентностей ОП «Організація захисту інформації в інформаційно-комунікаційних системах» спеціальності 123 «Комп'ютерна інженерія».

Рекомендована література — Підручники та посібники (2022–2024 рр.)

1. Пірог О. В.

Безпека вебдодатків : навчальний посібник. — Київ, 2023. — 215 с. *Охоплює основи веббезпеки, захист від XSS, CSRF, SQL-ін'єкцій, тестування безпеки (Nmap, Burp Suite, Metasploit), безпечне програмування.*

2. Маліновський В. І., Куперштейн Л. М., Каплун В. А.

Кібербезпека мобільних пристроїв та інтернету речей : електронний практикум. — Вінниця : ВНТУ, 2024. — 208 с. *Включає захист від DDoS, безпеку HTTP/IoT, хмарні сервіси.*

3. Сілін Є. С., Кадубовський О. А.

Основи кібербезпеки : навчальний посібник [електронний ресурс]. — Дніпро, 2023. — 200 с. *Мережева кібербезпека, управління паролями, захист браузерів, Proxy/VPN/Firewall.*

4. Онищенко С., Глушко А.

Аналітичний вимір кібербезпеки України в умовах зростання викликів та загроз. Економіка і регіон. — Нац. ун-т ім. Юрія Кондратюка. — 2022. — № 1 (84). — С. 13–20. *Аналіз загроз у воєнний час, реагування на інциденти.*

5. Жилін А. В., Шаповал О. М., Успенський О. А.

Технології захисту інформації : навчальний посібник. — Київ : КПІ ім. Ігоря Сікорського (ІС33І), 2022. — 210 с. *Технічний захист інформації в ІТС, оцінка захищеності, стандарти.*

6. Довгань О. та ін. (ред.)

Кібербезпека в інформаційному суспільстві : інформаційно-аналітичний дайджест. — Київ : Інститут інформації, безпеки і права НАПрН України; НБУВ, 2024. — № 5. — 316 с. *Актуальний огляд кіберзагроз, IoT, кіберзлочинність.*

7. Когут Ю.

Кібербезпека та ризики цифрової трансформації компаній. — Київ : Наш Формат, 2022. — 320 с. *Системний аналіз загроз у кіберпросторі, технології протидії, захист бізнесу.*

8. Остапов С. Е., Євсеєв С. П., Король О. Г.

Кібербезпека: сучасні технології захисту : навчальний посібник. — Харків : Новий світ-2000, 2022. — 380 с. *Технології захисту, криптографія, безпека мереж та систем.*

Додаткова література та наукові ресурси

9. OWASP Testing Guide v4.2

OWASP Foundation, 2022. Доступно: **owasp.org**. *Основна методологія тестування безпеки веб-додатків. Рекомендується для всіх тем модулів 2 та 4.*

10. NIST SP 800-53 Rev. 5

Security and Privacy Controls for Information Systems. NIST, 2022. Доступно: **csrc.nist.gov**. *Рекомендується для тем 1.4 та 4.3 (нормативна база, захист ПД).*

11. CERT-UA. Звіти про кіберінциденти 2022–2024 рр.

Урядова команда реагування на комп'ютерні надзвичайні події України. — Доступно: **cert.gov.ua**. *Рекомендується для тем 4.2 та 4.4 (реагування на інциденти, тренди кіберзагроз).*

12. ISO/IEC 27001:2022

Information security management systems — Requirements. International Organization for Standardization, 2022. *Міжнародний стандарт управління інформаційною безпекою. Рекомендується для тем 1.4 та 3.1.*

Нормативно-правова база

→ Закон «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII

Визначає основи державної політики у сфері кібербезпеки, повноваження суб'єктів та вимоги до захисту критичної інформаційної інфраструктури. **zakon.rada.gov.ua**

→ Закон «Про захист персональних даних» від 01.06.2010 № 2297-VI (зі змінами)

Регулює відносини, пов'язані із захистом персональних даних під час їх обробки, у т. ч. в інтернет-ресурсах. **zakon.rada.gov.ua**

→ Кримінальний кодекс України. Статті 361–363-1

Кримінальна відповідальність за несанкціоноване втручання в роботу ЕОМ, систем та комп'ютерних мереж, кіберзлочини. **zakon.rada.gov.ua**

→ Стратегія кібербезпеки України (2021–2025)

Затверджена Указом Президента від 26.08.2021 № 447. Визначає стратегічні цілі та пріоритети у сфері кібербезпеки держави. **zakon.rada.gov.ua**

→ Закон «Про електронні комунікації» від 16.12.2020 № 1089-IX

Регулює відносини у сфері електронних комунікацій, у т. ч. вимоги до безпеки мереж та послуг. **zakon.rada.gov.ua**

Офіційні ресурси та фахові видання

CERT-UA

cert.gov.ua — Урядова команда реагування на кіберінциденти. Звіти про загрози, бюлетені безпеки, рекомендації щодо захисту.

ДССЗЗІ України

cip.gov.ua — Державна служба спеціального зв'язку та захисту інформації. Нормативна база, новини кіберзахисту, реєстр атак на Україну.

OWASP Foundation

owasp.org — Некомерційна організація з веббезпеки: OWASP Top 10, ASVS, Testing Guide, безкоштовні інструменти (ZAP, WebGoat, DVWA).

NIST Cybersecurity

csrc.nist.gov — Національний інститут стандартів і технологій США: стандарти SP 800, NIST CSF, бібліотека вразливостей NVD.

CVE / NVD

nvd.nist.gov — Національна база вразливостей (NVD/CVE): актуальна інформація про вразливості програмного забезпечення та рейтинги CVSS.

Національна бібліотека України

nbuv.gov.ua — Електронні ресурси, наукові статті, монографії з інформаційної безпеки та кібербезпеки.

Журнал «Кібербезпека»

ippi.org.ua — Інформаційно-аналітичний дайджест НДІП НАПрН України та НБУВ. Огляди загроз, аналітика, нові публікації.

Міністерство освіти і науки України

mon.gov.ua — Освітні стандарти, навчальні програми, методичні матеріали зі спеціальності 123 «Комп'ютерна інженерія».

Зв'язок дисципліни зі спеціальністю 123 «Комп'ютерна інженерія»

Чому «Захист інтернет ресурсів» для інженерів?

Дисципліна є невід'ємною складовою ОП «Організація захисту інформації в ІКС» для бакалаврів зі спеціальності 123. Кожен сучасний інженер-програміст або системний архітектор створює, розгортає або супроводжує інтернет-ресурси, що є постійними цілями кібератак.

Сучасний IT-фахівець, який розуміє принципи атак і захисту, — це не просто технічний спеціаліст, а відповідальний інженер, здатний проектувати системи з урахуванням безпеки з першого дня (Security by Design).

Практичне значення для майбутньої кар'єри

- Розуміння вразливостей власного коду та архітектурних рішень для розробки захищених систем
- Навички роботи з інструментами кібербезпеки, затребуваними на ринку праці (Burp Suite, OWASP ZAP, Wireshark)
- Знання нормативної бази України та міжнародних стандартів для роботи у regulated industries
- DevSecOps-компетенції для інтеграції безпеки у цикл розробки ПЗ
- Розуміння принципів Zero Trust та сучасних архітектур захисту для проектування захищених систем
- Готовність до роботи в умовах активної кіберпротидії, актуальної для Ukrainian IT-сектору

Ключові компетентності курсу — Підсумок

Курс охоплює повний цикл захисту інтернет-ресурсів — від розуміння архітектури загроз до практичного тестування та реагування на інциденти — і формує у студентів компетентності, необхідні для роботи у сфері кібербезпеки та розробки захищених систем.

Бажаємо успіхів у вивченні дисципліни «Захист інтернет ресурсів»!

120

Годин

Загальний обсяг дисципліни

4

Кредити ЄКТС

Відповідно до стандарту

16

Тем

У 4 змістовних модулях

15

Лаб. робіт

Практичних годин у лабораторіях

> «Безпека — це не продукт, а процес.» — Брюс Шнайєр

Спеціальність 123 · Комп'ютерна інженерія · Бакалавр · ОП: Організація захисту інформації в ІКС · 4 кредити ЄКТС