Міністерство освіти і науки України
Національний університет «Чернігівська політехніка»
Навчально-науковий інститут електронних та інформаційних технологій
Кафедра кібербезпеки та математичного моделювання

РОБОЧА ПРОГРАМА
Технології безпеки web-ресурсів

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Ткач Ю.М.
(підпис) (прізвище та ініціали)

«26» серпня 2025 р.

Розробник (-и):
Базилевич В.М., директор ННІ ЕІТ, кандидат економічних наук наук, доцент _____
(прізвище та ініціали, посада, науковий ступінь і вчене звання) (підпис)

Робочу програму навчальної дисципліни обговорено на засіданні кафедри кібербезпеки та математичного моделювання

Протокол від «26» серпня 2025 р. №6

Узгоджено з гарантом освітньої програми: _____ Ткач Ю.М.
(підпис) (прізвище та ініціали)

---

1. Загальна інформація про дисципліну.

Тип дисципліни	*Вибіркова*
Мова викладання	Українська/англійська
Рік навчання та семестр	2025-2026 навчальний рік, І семестр, ОП Кібербезпека за спеціальністю F5 Кібербезпека та захист інформації галузь знань F Інформаційні технології
Викладач (-і)	Базилевич Володимир Маркович, директор ННІ ЕІТ, кандидат економічних наук наук, доцент
Профайл викладача (-ів)	https://cs.stu.cn.ua/bazylevych-volodymyr-markovych/
Контакти викладача	bazvlamar@stu.cn.ua

2. Анотація курсу.

Дисципліна **"Технології безпеки web-ресурсів"** є важливою складовою підготовки фахівців у галузі кібербезпеки, яка фокусується на вивченні сучасних технологій та інструментів для забезпечення безпеки веб-сайтів та веб-додатків. Курс охоплює як теоретичні, так і практичні аспекти захисту web-ресурсів від різноманітних кіберзагроз, включаючи атаки типу SQL-ін'єкції, кроссайтного скриптингу (XSS), атаки на аутентифікацію, захист конфіденційності даних користувачів та інші. Студенти будуть ознайомлені з основними принципами захисту web-додатків, інструментами для тестування безпеки, а також сучасними методами виявлення та усунення вразливостей у web-ресурсах.

3. Мета та цілі курсу.

Формування у студентів знань і практичних навичок із забезпечення безпеки веб-ресурсів, аналізу та усунення вразливостей, впровадження сучасних методів аутентифікації, шифрування та моніторингу загроз для мінімізації кіберризиків у веб-середовищі.

Цілі курсу:

1. Ознайомити студентів з основними принципами та концепціями безпеки web-ресурсів.
2. Навчити студентів ідентифікувати типові вразливості та загрози безпеці web-ресурсів, такі як SQL-ін'єкція, XSS, CSRF та інші.
3. Надати студентам практичні навички використання інструментів для тестування безпеки web-додатків (наприклад, Burp Suite, OWASP ZAP).
4. Розвинути вміння впроваджувати стратегії захисту для запобігання атакам на web-ресурси.
5. Поглибити розуміння принципів шифрування та захисту даних на веб-ресурсах.
6. Ознайомити студентів з правовими аспектами кібербезпеки в контексті web-ресурсів, зокрема, GDPR, закони про захист персональних даних.
7. Навчити методам моніторингу безпеки web-ресурсів і проведенню регулярних перевірок на вразливості.

4. Результати навчання:

ПРН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.

ПРН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.

КЗ 1. Здатність застосовувати знання у практичних ситуаціях.

КЗ 4. Здатність оцінювати та забезпечувати якість виконуваних робіт.

КФ 2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки

КФ 7. Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.

5. Пререквізити.

Базові знання за темами: Основи веб-розробки. Основи комп'ютерних мереж та їх безпеки. Основи програмування. Архітектура клієнт-сервер. Бази даних. Основи криптографії. Основи ОС і командного рядка

6. Обсяг курсу:

Вид заняття	Загальна кількість годин
Лекції	16/6
Лабораторні заняття	16/6
Самостійна робота	88/108
Індивідуальне завдання – розрахунково-графічна робота	
Всього кредитів	4

Лекційні, лабораторні заняття, розрахунково-графічна робота, самостійна робота – з використанням системи дистанційного навчання Moodle, MS Teams, рекомендованих джерел, відеоматеріалів тощо.

7. Тематика курсу.
Лекції (16/6 годин):

Тема 1. Основи безпеки web-ресурсів
Поняття та принципи безпеки web-додатків
Конфіденційність, цілісність, доступність (CIA-тріада)
Роль безпеки web-ресурсів у загальній кібербезпеці

Тема 2. Типові загрози та вразливості
Класифікація загроз web-додатків
Приклади реальних атак
Огляд OWASP Top 10

Тема 3. SQL-ін’єкції
Механізм атаки
Приклади експлуатації
Методи захисту (підготовлені запити, ORM, валідація даних)

Тема 4. XSS та CSRF
Кроссайтний скриптинг (Stored, Reflected, DOM-based)
Наслідки та методи захисту (CSP, escape-функції)
CSRF: принцип атаки, приклади, методи запобігання (токени, SameSite cookies)

Тема 5. Аутентифікація та авторизація
Основи аутентифікації та авторизації
Методи (Basic, Digest, OAuth, SSO)
Захист паролів: хешування, соління, зберігання

Тема 6. Шифрування та захист даних
Принципи захисту даних у веб-додатках
HTTPS, SSL/TLS
Симетричне й асиметричне шифрування, алгоритми та приклади застосування

Тема 7. Інструменти та практичний захист
Огляд інструментів: Burp Suite, OWASP ZAP, Nikto
Методи виявлення вразливостей
Практичний захист: фільтрація даних, CSP, правила для форм

Тема 8. Правові аспекти та моніторинг
Міжнародні стандарти та нормативи (GDPR, PCI DSS)
Вимоги до захисту персональних даних
Моніторинг безпеки: логи, системи виявлення атак
Кращі практики підтримки безпеки web-ресурсів

Лабораторні (16/6 годин):

Лабораторна робота 1 — SQL-ін'єкція, XSS, CSRF

Мета: зрозуміти механізми трьох базових веб-вразливостей, навчитися їх відтворювати в лабораторних умовах та застосовувати базові методи захисту.

Завдання:

Побудувати просту тестову веб-форму/додаток (Docker/Vagrant або готові уразливі стенди — DVWA, WebGoat).

Виконати експлуатацію: SQL-ін'єкція (витяг даних, bypass аутентифікації), Reflected/Stored XSS (вставка скрипта), CSRF (пояснення і демонстрація простого запиту).

Реалізувати захист: підготовлені запити / ORM, escape/encoding, CSP, CSRF-токени, SameSite cookies.

Очікуваний результат: робочі PoC-скрипти на локальному стенді; короткий звіт з доказами та кодом захисту.

Інструменти: sqlmap, Burp Suite/OWASP ZAP, браузерні DevTools, Postman, DVWA/WebGoat.

Етика: лише локальні стенди або письмовий дозвіл власника.

Лабораторна робота 2 — Clickjacking, DOM-based vulnerabilities, CORS

Мета: вивчити клієнтські/DOM-вразливості та проблеми, пов'язані з політикою міждержерел (CORS), і навчитися захищатися.

Завдання:

Демонстрація clickjacking — створення фрейму, який «перехоплює» кліки; захист через X-Frame-Options / CSP frame-ancestors.

Виявлення DOM-based XSS у прикладному JS (маніпуляції innerHTML, location.hash) і виправлення (безпечне маніпулювання DOM, sanitize).

Налаштування CORS на сервері (приклади дозволених/заборонених origin), демонстрація небезпек misconfigured CORS.

Очікуваний результат: PoC-демо, налаштування серверних заголовків для захисту, короткий звіт.

Інструменти: браузер, Burp, простий Node/Express або Python Flask стенд, DOM-sanitizers (DOMPurify).

Лабораторна робота 3 — XXE, SSRF, HTTP Request Smuggling

Мета: дослідити вразливості, що працюють через некоректну обробку вхідних запитів/ресурсів, і розробити запобіжні заходи.

Завдання:

XXE: створити приклад парсера XML, показати витік локальних файлів/метаданих; захист — вимкнення зовнішніх сутностей, безпечні парсери.

SSRF: створити PoC, який змушує сервер робити запит до внутрішнього хосту; захист — whitelisting, блокування небезпечних схем.

HTTP request smuggling: пояснити концепт (CL.TE/TE.CL), прості демонстрації на локальному проксі; захист — правильні проксі/серверні конфігурації, однорідність обробки заголовків.

Очікуваний результат: PoC, конфігурації/параметри захисту, коротке пояснення ризиків.

Інструменти: Burp Suite, curl, локальний XML-parser, dockerized apps, проксі для тестування.

Лабораторна робота 4 — OS command injection, Server-side template injection (SSTI), Path traversal

Мета: аналіз вразливостей, що дозволяють виконувати код або витягувати файли на сервері, та впровадження захисту.

Завдання:

OS command injection: знайти вразливість через невірну інтерполяцію параметрів у викликах shell; демонстрація, захист — валідація, використання API замість shell, екранування/whitelisting.

SSTI: пояснити шаблонні рушії (Jinja2, Twig) і виявити приклад SSTI; захист — ізоляція шаблонів, sandboxing, оновлення рушія.

Path traversal: показати доступ до файлів через ../, захист — нормалізація шляхів, перевірка дозволених директорій.

Очікуваний результат: PoC-експлойти на локальному стенді, виправлений код/конфігурації.

Інструменти: Python/Flask або Node, Burp, shell, статичний аналіз коду.

Лабораторна робота 5 — Access control, Authentication, WebSockets, Web cache poisoning

Мета: розглянути помилки контролю доступу, проблеми з автентифікацією, особливості WebSocket безпеки та загрози, пов’язані з кешуванням.

Завдання:

Access control vulnerabilities: демонстрація горизонтального/вертикального обходу прав, пошук незахищених API-ендонпойнтів; захист — правильні перевірки прав на сервері.

Authentication: атаки на слабкі механізми, brute-force, захист — rate limiting, MFA, безпечне зберігання паролів.

WebSockets: демонстрація небезпечних повідомлень/авторизації у WS; захист — авторизація при підключенні, валідація повідомлень.

Web cache poisoning: показати як маніпуляція заголовками може призвести до кеш-отруєння; захист — валідація заголовків, правильні Cache-Control/Vary.

Очікуваний результат: набір PoC і рекомендацій/виправлень, короткий звіт.

Інструменти: Burp, WebSocket клієнти, Redis/NGINX (локальні стенди), rate-limit тестери.

Розрахунково-графічна робота (РГР) — набір тем

Тематика: HTTP Host header attacks; OAuth authentication; File upload vulnerabilities; JWT; NoSQL injection.

Опис і цілі РГР: Студент(и) виконують комплексний проект, що включає аналіз однієї-двох з наведених тем, створення PoC-демонстрації в локальному стенді, розробку механізмів захисту і написання формального звіту. Мета — показати вміння застосувати знання з курсу до складнішої, інтегрованої проблеми.

Рекомендовані завдання (вибрати 2–3 з переліку):

HTTP Host header attacks: продемонструвати атаки (включно з password reset poisoning або Web cache poisoning через Host), описати вплив на додаток та запропонувати захист (strict host checking, canonicalization).

OAuth authentication: проаналізувати flow (authorization code, implicit, PKCE), знайти потенційні misconfigurations, реалізувати безпечний flow (наприклад PKCE) у простому додатку.

File upload vulnerabilities: створити PoC для небезпечного завантаження файлів (розширення, MIME/сигнатура, зберігання), запропонувати захист (сканування, зберігання поза веб-коренем, валідація MIME).

JWT: дослідити загрози (alg: none, key leakage, replay), реалізувати правильну конфігурацію, термін придатності, відмова від некоректних алгоритмів.

NoSQL injection: показати ін'єкцію в MongoDB/інші NoSQL, PoC запитів, захист — параметризовані запити, whitelisting.

Вимоги до РГР (обов'язкові):

Технічний звіт (6–10 сторінок): вступ, методи, PoC, результати тестів, рекомендації з виправлення.

Код/стенд (Git репозиторій або архів): Docker-compose або інструкція для запуску PoC локально.

Демонстрація (коротке відео 3–5 хв або live demo) + презентація 5–7 слайдів.

Оцінювання: технічна складність (35%), коректність PoC (25%), якість захисту/рекомендацій (20%), документація та демонстрація (20%).

Рекомендовані етапи/мільстоунси:

Пропозиція теми + план (тиждень 1) — 1 сторінка.

Проміжний звіт + базовий PoC (тиждень 3) — демонстрація працюючого стенду.

Фінальна здача (звіт, код, відео, презентація) — до дедлайну.

Загальні рекомендації та інструменти для всіх робіт

Стенди: Docker + готові вразливі додатки (DVWA, WebGoat, Juice Shop).

Інструменти: Burp Suite (community/Pro), OWASP ZAP, sqlmap, curl, Postman, Wireshark, Wireshark (для мережевого аналізу), Docker, scanners (Nikto).

Мова/платформа для PoC: Python/Flask, Node/Express, прості HTML/JS сторінки.

Етика/безпека: виконувати всі тести лише на власних/ліцензованих стендах, не атакувати сторонні реальні сервери без дозволу. Фіксувати і повідомляти про виявлені реальні вразливості відповідно до правила responsible disclosure, якщо такі будуть знайдені поза лабораторною інфраструктурою.

Самостійна робота (88/108 годин):

Самостійна робота студентів є важливою складовою навчального процесу і сприяє глибшому засвоєнню тем, пов'язаних з безпекою web-ресурсів. В рамках самостійної роботи студенти повинні виконати завдання, що охоплюють аналіз та реалізацію заходів безпеки для web-ресурсів, а також знайомство з сучасними техніками тестування безпеки, зокрема:

Основні завдання самостійної роботи:

Аналіз безпеки web-ресурсу:

Теоретичний аналіз:

Опис сучасних загроз для web-ресурсів (SQL-ін'єкція, XSS, CSRF, DoS/DDoS атаки, фішинг).

Огляд інструментів для тестування безпеки web-ресурсів (OWASP ZAP, Burp Suite, Nikto, Acunetix).

Дослідження існуючих стандартів і практик безпеки web-додатків, зокрема рекомендацій OWASP.

Практичне завдання:

Проведення тестування на наявність вразливостей за допомогою відкритих інструментів (наприклад, Burp Suite, OWASP ZAP).

Аналіз результатів тестування, визначення критичних вразливостей та ризиків для безпеки ресурсу.

Розробка стратегії захисту web-ресурсу:

Теоретичний аналіз:

Опис основних методів захисту від вразливостей: фільтрація вводу, контроль доступу, шифрування даних, захист сесій, двофакторна аутентифікація.

Застосування сучасних стандартів безпеки (TLS/SSL, Content Security Policy, HTTP Security Headers).

Практичне завдання:

Розробка та реалізація стратегії захисту для виявлених вразливостей (покращення захисту сесій, шифрування даних, обмеження прав доступу, захист від XSS/SQLi).

Оцінка ефективності заходів захисту на основі тестування.

Технічне налаштування серверів для захисту web-ресурсів:

Теоретичний аналіз:

Основи налаштування веб-серверів (Apache, Nginx) для забезпечення безпеки web-ресурсів.

Використання інструментів для моніторингу та аналізу трафіку (Wireshark, tcpdump).

Практичне завдання:

Налаштування конфігурацій web-сервера для забезпечення безпеки (наприклад, застосування HTTPS, налаштування правил доступу через файли .htaccess або конфігурації Nginx).

Проведення тестування на наявність вразливостей у налаштуваннях серверів.

Робота з системами контролю версій та автоматизація безпеки:

Теоретичний аналіз:

Вивчення основ роботи з системами контролю версій (Git, GitHub, GitLab).

Роль автоматизації у забезпеченні безпеки web-додатків (наприклад, CI/CD для автоматичного тестування безпеки).

Практичне завдання:

Налаштування системи CI/CD для автоматичного тестування на безпеку при кожному коміті.

Інтеграція автоматичних тестів безпеки в процеси розробки та деплойменту.

Аналіз журналів та моніторинг web-ресурсу:

Теоретичний аналіз:

Огляд основних типів журналів web-серверів: доступу, помилок, безпеки.

Методи аналізу журналів для виявлення потенційних атак або спроб вторгнення.

Практичне завдання:

Аналіз журналів web-сервера (наприклад, Apache або Nginx) для виявлення підозрілих запитів або аномалій.

Визначення патернів атак на основі аналізу журналів та розробка стратегії реагування на інциденти.

Розробка документації з безпеки для web-ресурсу:

Теоретичний аналіз:

Огляд основних типів документації з безпеки для web-ресурсів (політики безпеки, плани відновлення після інцидентів, процедури реагування на інциденти).

Практичне завдання:

Створення плану відновлення після інцидентів для web-ресурсу.

Розробка політик безпеки для web-додатків та документування процедур управління інцидентами.

8. Система оцінювання та вимоги

Загальна система оцінювання курсу	Оцінювання курсу базується на **накопичувальній системі** та включає: **поточний контроль** (оцінювання лабораторних занять) – 50 балів, **проміжний модульний**

	контроль – 40 балів, **підсумковий контроль** – 10 балів. Оцінювання кожного виду діяльності здійснюється окремо відповідно до **досягнення навчальних цілей**.
Вимоги до РГР	Відсутні
Лабораторні роботи	Оцінка кожного практичного заняття здійснюється за наступними критеріями: 1) виконання практичного завдання – **6 бали;** 2) аналіз отриманих результатів – **2 бал**; 3) належне оформлення звіту – **2 бал.**
Умови допуску до підсумкового контролю	1. Отримання не менше 50 балів протягом семестру (лабораторні + проміжний контроль + РГР). 2. Відвідування щонайменше 50% занять.

Розподіл балів, які отримують здобувачі вищої освіти

Модуль за тематичним планом дисципліни та форма контролю		**Кількість балів**
Змістовий модуль 1. Основи безпеки web-ресурсів		**50**
1	Тема 1. Основи безпеки web-ресурсів	**10**
2	Тема 2. Типові загрози та вразливості	**10**
3	Тема 3. SQL-ін’єкції	**10**
4	Тема 4. XSS та CSRF	**20**
Змістовий модуль 2. Технічне налаштування та моніторинг безпеки web-ресурсів		**40**
1	Тема 5. Аутентифікація та авторизація	**10**
2	Тема 6. Шифрування та захист даних	**10**
3	Тема 7. Інструменти та практичний захист	**10**
4	Тема 8. Правові аспекти та моніторинг	**10**
Усього поточний і проміжний модульний контроль		**90**
Семестровий контроль (Диференційований залік)		**10**
Разом		**0…100**

Шкала оцінювання результатів навчання

Оцінка в балах	**Оцінка ECTS**	**Оцінка за національною шкалою (диференційований залік)**	
		для екзамену (диференційованого заліку), курсового проєкту (роботи), практики, атестації	для заліку
90 – 100	**A** (*відмінно*)	відмінно	зараховано
82-89	**B** (*дуже добре*)	добре	
75-81	**C** (*добре*)		
66-74	**D** (*задовільно*)	задовільно	
60-65	**E** (*достатньо*)		

0-59	**FX** (*незадовільно*)	незадовільно з можливістю повторного складання	незараховано з можливістю повторного складання

9. Обладнання та програмне забезпечення.

При вивченні курсу використовується наступне **обладнання та програмне забезпечення**:

І. Апартне забезпечення:

Персональні комп'ютери або ноутбуки з підтримкою віртуалізації та можливістю роботи з образами дисків та цифровими доказами.

Операційні системи: Windows 10/11 Pro, Linux (Ubuntu, Kali Linux – для аналізу вразливостей), macOS.

Серверне обладнання для моделювання атак, аналізу мережевого трафіку та логів.

Мережеве обладнання (маршрутизатори, комутатори, мережеві екрани) для дослідження атак та аналізу цифрових слідів.

Зовнішні накопичувачі (HDD, SSD, USB-флешки) для роботи з криміналістичними копіями та створення дампів пам'яті.

Мобільні пристрої (Android, iOS) для дослідження мобільної криміналістики.

ІІ. Програмне забезпечення:

1. Для збору та збереження цифрових доказів:

FTK Imager – створення криміналістичних копій дисків.

Autopsy, Sleuth Kit – аналіз файлових систем та структури дисків.

Guymager – криміналістичне копіювання дисків у Linux.

2. Для аналізу файлових систем та метаданих:

X-Ways Forensics – глибокий аналіз файлових систем, відновлення даних.

ExifTool – витягнення метаданих із файлів (зображень, документів, відео).

Bulk Extractor – автоматичний пошук артефактів у файлах (номери кредитних карт, паролі).

3. Для дослідження операційних систем та лог-файлів:

Registry Explorer – аналіз реєстру Windows.

Event Log Explorer – дослідження журналів подій Windows.

Plaso, Timesketch – створення хронологій подій на основі логів системи.

4. Для мережевої криміналістики та аналізу трафіку:

Wireshark – аналіз мережевого трафіку.

Zeek (Bro IDS) – моніторинг і розслідування мережевих атак.

NetworkMiner – вилучення артефактів із трафіку.

5. Для криміналістики мобільних пристроїв:

MOBILedit Forensic – вилучення даних із мобільних пристроїв.

Oxygen Forensic Detective – аналіз дзвінків, повідомлень, геолокаційних даних.

Cellebrite UFED – відновлення та аналіз даних із мобільних телефонів.

6. Для аналізу шкідливого програмного забезпечення:

IDA Pro – дизасемблювання та аналіз шкідливого коду.

PE Explorer – дослідження виконуваних файлів Windows.

Cuckoo Sandbox – динамічний аналіз підозрілих файлів у віртуальному середовищі.

7. Для складання криміналістичних звітів та документування:

LaTeX, MS Word – підготовка технічної документації та звітів.

CaseNotes – ведення криміналістичних нотаток.

8. Платформи для дистанційного навчання:

Moodle, Microsoft Teams – розміщення навчальних матеріалів, тестування та проведення лекцій.

Google Drive, OneDrive – спільна робота з документами та звітами.

Використання наведеного обладнання та програмного забезпечення дозволяє студентам отримати практичний досвід у сфері цифрової криміналістики та підготуватися до роботи в реальних криміналістичних розслідуваннях.

10. Політики курсу.

У випадку, якщо здобувач протягом семестру не виконав у повному обсязі всіх видів навчальної роботи, має невідпрацьовані лабораторні роботи або не набрав мінімально необхідну кількість балів (50), він не допускається до складання диференційованого заліку під час семестрового контролю, але має право ліквідувати академічну заборгованість у порядку, передбаченому «Положенням про поточне та підсумкове оцінювання знань здобувачів НУ "Чернігівська політехніка"». Повторне складання заліку з метою підвищення позитивної оцінки не дозволяється. У випадку повторного складання заліку всі набрані протягом семестру бали анулюються, а повторний диференційований залік складається у вигляді тестування.

До загальної політики курсу відноситься дотримання принципів відвідування занять у відповідності до затвердженого розкладу, а також вільного відвідування лекційних занять для осіб, які отримали на це дозвіл відповідно до «Порядку надання дозволу на вільне відвідування занять здобувачам вищої освіти НУ «Чернігівська політехніка»». Запорукою успішного вивчення дисципліни є активність та залучення під час проведення лабораторних/практичних та лекційних занять – відповіді на запитання викладача (як один з елементів поточного контролю), задавання питань для уточнення незрозумілих моментів, вирішення практичних завдань. Консультації відбуваються в аудиторіях університету у відповідності до затвердженого розкладу або ж особистих чи групових консультацій (через вбудований форум) на сторінці курсу в системі дистанційного навчання НУ «Чернігівська політехніка».

Політика дедлайнів

Максимальна оцінка за невчасно здані роботи зменшується на зазначену кількість балів. Виключенням може бути наявність поважних причин несвоєчасної здачі зазначених робіт (хвороба, участь в зазначений час в інших видах навчальної, наукової чи організаційної роботи, офіційна робота за фахом тощо).

Політика користування ноутбуками / смартфонами

Прохання до здобувачів тримати смартфони переведеними у беззвучний режим протягом лекційних та практичних занять, так як дзвінки, переписки та спілкування у соціальних мережах відволікають від проведення занять як викладача, так й інших здобувачів. Ноутбуки, планшети та смартфони не можуть використовуватися в аудиторіях під час занять та під час проведення підсумкового контролю (за виключенням проходження тестового контролю в системі Moodle).

Політика заохочень та стягнень

За результатами навчальної, наукової або організаційної діяльності здобувачів вищої освіти за курсом їм можуть нараховуватися додаткові бали – до 10 балів, у залежності від вагомості досягнень. Види позанавчальної діяльності, за якими здобувачі вищої освіти заохочуються додатковою кількістю балів: участь у міжнародних проектах, наукові дослідження, тези, участь у науково-практичних конференціях, винаходи, патенти, авторські свідоцтва за напрямами курсу.

Політика академічної доброчесності

Академічна доброчесність повинна бути забезпечена під час проходження даного курсу, зокрема при виконанні лабораторних, контрольних та розрахунково-графічних робіт (КР/КП) (принципи описані у Кодексі академічної доброчесності НУ «Чернігівська політехніка»). Списування під час проміжного та підсумкового контролів, виконання практичних завдань на замовлення, підказки вважаються проявами академічної недоброчесності. Від усіх слухачів курсу очікується дотримання академічної доброчесності у зазначених вище моментах. До здобувачів вищої освіти, у яких було виявлено порушення академічної доброчесності, застосовуються різноманітні дисциплінарні заходи (включаючи повторне проходження певних етапів).

Правила перезарахування кредитів

Кредити, отримані в інших закладах вищої освіти, а також результати навчання у неформальній та/або інформальній освіті, можуть бути перезараховані викладачем у відповідності до положення «Порядок визначення академічної різниці та перезарахування навчальних дисциплін у НУ «Чернігівська політехніка»». Визнання результатів навчання у неформальній освіті розповсюджується на окремі змістові модулі (теми) навчальної дисципліни.

11. Рекомендована література.

Базові підручники:

1. Злочини проти інформаційної безпеки держави: поняття, виявлення, досудове розслідування: монографія / І.В. Гора, В.А. Колесник, В.В. Малюк, В.О. Ходанович, А.М. Черняк, Л.І. Щербина. Київ: 7БЦ, 2023. 512 с.

2. Research Trends, Challenges and Emerging Topics in Digital Forensics: A Review of Reviews. Received January 22, 2022, accepted February 16, 2022, date of publication February 24, 2022, date of current version March 10, 2022. URL: https://www.researchgate.net/publication/358837101_Research_Trends_Challenges_and_Emergin_Topics_in_Digital_Forensics_A_Review_of_Reviews

3. Tarun Vashishth. Cyber Forensics Up and Running. A hands-on guide to digital forensics tools and technique. Published by BPB Online WeWork, 2024. 407 p.

4. eForensics Magazine. Workshop. URL: https://eforensicsmag.com/.

5. Bruce Middleton. Cyber Crime Investigator's Field Guide. Third Edition. Chennai, India: CRC Press, 2022. 353 p.

6. Introduction to Forensic and Criminal Psychology. 7th Edition. Dennis Howitt Loughborough University. New York: Pearson Education Limited, 2022. 768 p.

Джерела:

1. ISO/IEC 27037 Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence. URL: https://www.amnafzar.net/files/1/ISO%2027000/ISO%20IEC%2027037-2012.pdf

2. Репозиторії готових дампів па'яті для аналізу на гітхаб. URL: https://github.com/SecurityNik/CTF, https://github.com/cyph3rryx/Kryptonite-RAM-Dump-Collection, https://www.baeldung.com/linux/dump-memory-image, https://github.com/504ensicsLabs/LiME

3. Образ віртуальної машини Caine, що містить необхідні інструменти в галузі Computer Forensics. URL: https://www.caine-live.net/page5/page5.html

4. Образ віртуальної машини Kali Linux. URL: https://www.kali.org/get-kali/#kali-platforms

5. Платформа для візуалізації та емуляції на MacOS. URL: https://mac.getutm.app/

6. Власний репозиторій з програмним інструментом для трансферу дампів пам'яті в ізольований контейнер Caine для аналізу. URL: https://github.com/urlinka2006/CyberInsight

7. Autopsy – платформа цифрової криміналістики та графічний інтерфейс для The Sleuth Kit та інших інструментів цифрової криміналістики. URL: https://github.com/sleuthkit/autopsy

8. WireShark – найпопулярніший у світі аналізатор мережевих протоколів. URL: https://www.wireshark.org/

9. Sleuth Kit (TSK) – бібліотека та колекція інструментів цифрової криміналістики командного рядка, які дозволяють досліджувати томи та дані файлової системи. Бібліотеку можна включити до більших інструментів цифрової криміналістики, а інструменти командного рядка можна безпосередньо використовувати для пошуку доказів. URL: https://github.com/sleuthkit/sleuthkit

10. BelkaGPT — перший автономний AI-помічник для розслідувань DFIR. URL: https://belkasoft.com/belkagpt?utm_campaign=Police%201&utm_source=Media&utm_medium=Article&utm_term=eforensicsmag&utm_content=belkagpt