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

# СИЛАБУС
## *Технології безпеки web-ресурсів*

**ЗАТВЕРДЖУЮ**
Завідувач кафедри
_____ __Ткач Ю.М.__
(підпис) (прізвище та ініціали)

«_26_» ___08_____ 2024 р.

Розробник (-и): Мехед Д.Б., доцент, кандидат педагогічних наук, доцент _____
(прізвище та ініціали, посада, науковий ступінь і вчене звання) (підпис)

Силабус навчальної дисципліни обговорено на засіданні кафедри кібербезпеки та математичного моделювання

Протокол від «_26____»__08_____2024р. №_7___

Узгоджено з гарантом освітньої програми: _____ _____Ю.М.Ткач_____
(підпис) (прізвище та ініціали)

---

1. Загальна інформація про дисципліну.

| | |
|---|---|
| **Тип дисципліни** | *Вибіркова* |
| **Мова викладання** | українська |
| **Рік навчання та семестр** | 2024-2025 навчальний рік, І семестр, ОП Кібербезпека за спеціальністю 125 Кібербезпека та захист інформації галузь знань 12 Інформаційні технології |
| **Викладач (-і)** | Мехед Д.Б., доцент кафедри кібербезпеки та математичного моделювання, кандидат педагогічних наук. |
| **Профайл викладача (-ів)** | https://mmi.stu.cn.ua/personal-kafedry/ |
| **Контакти викладача** | Т.м. +38(063) 690-80-00, E-mail: d.mekhed@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.**

Метою дисципліни є надання студентам знань і практичних навичок для забезпечення безпеки web-ресурсів. Вони мають навчитися виявляти та усувати вразливості, впроваджувати ефективні механізми захисту даних і користувачів, а також захищати web-додатки від потенційних атак з використанням сучасних технологій і методів кібербезпеки.

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:**

Після завершення курсу студенти повинні:

- **Знати**:
  - Основні принципи безпеки web-ресурсів та веб-додатків.
  - Типові загрози та вразливості web-ресурсів, зокрема SQL-ін'єкції, XSS, CSRF, атаки на аутентифікацію та інші.
  - Методи захисту даних, механізми аутентифікації та авторизації в web-додатках.
  - Техніки шифрування та захисту конфіденційності даних користувачів в web-додатках.
  - Основи правових аспектів безпеки web-ресурсів, зокрема міжнародні стандарти та вимоги щодо захисту персональних даних.
- **Вміти**:
  - Ідентифікувати та аналізувати вразливості в web-ресурсах за допомогою інструментів для тестування безпеки (наприклад, Burp Suite, OWASP ZAP).
  - Виконувати атаки типу SQL-ін'єкцій, XSS та CSRF в контрольованому середовищі для тестування вразливостей.
  - Впроваджувати механізми захисту від атак, зокрема засоби захисту від SQL-ін'єкцій, захист від кроссайтного скриптингу та використання належної аутентифікації та авторизації.
  - Використовувати сучасні методи шифрування та захисту переданої через мережу інформації.

- Оцінювати безпеку web-ресурсів за допомогою методів регулярного сканування та моніторингу вразливостей.
- Застосовувати правові норми і стандарти безпеки в процесі розробки та підтримки web-ресурсів.
- Підготовлювати звіти та рекомендації для покращення безпеки web-ресурсів та веб-додатків.

КЗ 1. Здатність застосовувати знання у практичних ситуаціях.

КЗ 2. Здатність проводити дослідження на відповідному рівні.

КЗ 4. Здатність оцінювати та забезпечувати якість виконуваних робіт.

КФ 6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

КФ 9. Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому

ПРН 6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.

ПРН 11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

**5. Пререквізити.** Відсутні.

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

**7. Тематика курсу.**

**Змістовий модуль 1. Основи безпеки web-ресурсів**

Тема 1. **Вступ до безпеки web-ресурсів**.

Поняття та основи безпеки web-ресурсів та веб-додатків. Основні принципи безпеки в веб-розробці: конфіденційність, цілісність, доступність. Роль безпеки web-ресурсів в контексті кібербезпеки.

Тема 2. **Типові загрози та вразливості web-ресурсів.**

SQL-ін'єкція: механізм атаки, приклади, захист від SQL-ін'єкцій. Кроссайтний скриптинг (XSS): типи (Stored, Reflected, DOM-based), методи захисту. CSRF (Cross-Site Request Forgery): принцип атаки, запобігання та захист.

Тема 3. **Механізми аутентифікації та авторизації в web-додатках.**

Основи аутентифікації та авторизації в веб-додатках. Порівняння різних методів аутентифікації (Basic, Digest, OAuth, SSO). Механізми захисту паролів (хешування, соління).

**Змістовий модуль 2. Інструменти, правові аспекти та управління безпекою web-ресурсів**

Тема 4. **Захист конфіденційності даних та шифрування в web-додатках**

Принципи захисту даних: шифрування даних на сервері та в процесі передавання. HTTPS та SSL/TLS протоколи: їх роль у захисті даних на web-ресурсах. Асиметричне та симетричне шифрування. Алгоритми та їх застосування.

Тема 5. **Інструменти для тестування безпеки web-ресурсів**

Огляд популярних інструментів для тестування безпеки web-додатків: Burp Suite, OWASP ZAP, Nikto. Використання інструментів для виявлення вразливостей та їх усунення.

Тема 6. **Захист від атак на web-ресурси**

Захист від SQL-ін'єкцій, XSS, CSRF, атаки на сесії. Механізми фільтрації вхідних даних. Практичні методи захисту web-додатків від атак: використання Content Security Policy (CSP), введення правил безпеки для форм.

Тема 7. **Правові аспекти безпеки web-ресурсів** .

Міжнародні стандарти та нормативні акти щодо безпеки web-ресурсів (GDPR, PCI DSS). Захист персональних даних: вимоги до безпеки web-ресурсів в контексті законодавства.

Тема 8. **Моніторинг та управління безпекою web-ресурсів** (2 години)

Регулярне тестування на вразливості та моніторинг безпеки web-ресурсів. Використання логів та систем моніторингу для виявлення атак. Кращі практики та рекомендації для підтримки високого рівня безпеки web-ресурсів.

**8. Система оцінювання та вимоги**

| | |
|---|---|
| **Загальна система оцінювання курсу** | Оцінювання курсу базується на **накопичувальній системі** та включає: **поточний контроль** (оцінювання лабораторних занять) – 40 балів, **проміжний модульний контроль** – 10 балів, **виконання індивідуального завдання (РГР)** – 10 балів **та підсумковий контроль** – 40 балів. Оцінювання кожного виду діяльності здійснюється окремо відповідно до **досягнення навчальних цілей**. |
| **Вимоги до РГР, КР, КП тощо** | **Критерії оцінювання РГР:**<br>1) відповідність завдання вимогам курсу – **2 балів;**<br>2) обґрунтування вибору стандартів та методів захисту – **2 балів;**<br>3) якість аналізу ризиків та оцінка відповідності – **2 балів;**<br>4) оформлення роботи, відповідність методичним рекомендаціям – **2 балів;**<br>5) своєчасність здачі роботи – **2 бали.** |
| **Практичні заняття** | Оцінка кожного практичного заняття здійснюється за наступними критеріями: |

| | |
|---|---|
| | 1) виконання практичного завдання – **3 бали;**<br>2) аналіз отриманих результатів – **1 бал**;<br>3) належне оформлення звіту – **1 бал.** |
| **Умови допуску до підсумкового контролю** | 1. Виконання та захист **не менше 50% практичних робіт** (щонайменше 4 із 8).<br>2. Проходження проміжного модульного контролю.<br>3. Виконання **розрахунково-графічної роботи** (РГР). |

**Розподіл балів, які отримують здобувачі вищої освіти**

| **Модуль за тематичним планом дисципліни та форма контролю** | | **Кількість балів** |
|---|---|---|
| ***Змістовий модуль 1. Основи безпеки web-ресурсів*** | | **30** |
| **1** | Вступ до безпеки web-ресурсів | **5** |
| **2** | Типові загрози та вразливості web-ресурсів | **10** |
| **3** | Механізми аутентифікації та авторизації в web-додатках. | **15** |
| ***Змістовий модуль 2.* Інструменти, правові аспекти та управління безпекою web-ресурсів** | | **30** |
| **1** | Захист конфіденційності даних та шифрування в web-додатках | **5** |
| **2** | Інструменти для тестування безпеки web-ресурсів. Захист від атак на web-ресурси | **15** |
| **3** | Правові аспекти безпеки web-ресурсів | **5** |
| **4** | Моніторинг та управління безпекою web-ресурсів | **5** |
| **Усього поточний і проміжний модульний контроль** | | **60** |
| **Семестровий контроль (Диференційований залік)** | | **40** |
| **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 (за необхідності).**

При вивченні цього курсу для дистанційного навчання, тестування та обговорення питань курсу використовуються платформи *Moodle* та *Microsoft Teams*, для виконання лабораторних робіт застосовується комутаційне й серверне обладнання, а також ПК та програмне забезпечення навчальних аудиторій 105, 106, 110, 111 кафедри кібербезпеки та математичного моделювання.

**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 (25), 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*

Своєчасність здачі лабораторної роботи оцінюється в 0,5 балу за кожну лабораторну роботу. Своєчасність здачі РГР оцінюється в 1 бал. Відповідно, 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. Babak Akhgar, Andrew Staniforth, Francesca Bosco. Cyber Crime and Cyber Terrorism Investigator's Handbook. Syngress is an Imprint of Elsevier. USA, 2014. 435 p.

7. 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