НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВОДНОГО ГОСПОДАРСТВА ТА ПРИРОДОКОРИСТУВАННЯ

Навчально-науковий інститут кібернетики, інформаційних технологій та інженерії

04-04-90S

СИЛАБУС *навчальної дисципліни*		**SYLLABUS**
Основи Web-безпеки		Web Security Basics
Шифр за ОП	**ВБ 1.2**	Code in Degree Programme
Освітній рівень: Бакалаврський (перший)		Level of Education: Bachelor's (first)
Галузь знань **Інформаційні технології**	**12**	Field of Knowledge **Information Technology**
Спеціальність **Комп'ютерна інженерія**	**123**	Field of Study **Computer Engineering**
Освітня програма: **Комп'ютерна інженерія**		Degree Programme: **Computer Engineering**

РІВНЕ – 2025

Силабус навчальної дисципліни *Основи Web-безпеки* для здобувачів вищої освіти ступеня «бакалавр», які навчаються за освітньо-професійною програмою *«Комп'ютерна інженерія»*, спеціальності *«Комп'ютерна інженерія», 123*. Рівне. НУВГП. 2025. 12 стор.

ОП на сайті університету: *https://ep3.nuwm.edu.ua/22990/*.

Розробник силабусу: *Бойчура Михайло Володимирович, к.т.н., доцент кафедри обчислювальної техніки*

Силабус схвалений на засіданні кафедри обчислювальної техніки
Протокол №6 від “27” грудня 2024 року

В.о. завідувача кафедри: *Сидор А.І., к.т.н.*

Керівник (гарант) ОП: *Сидор А.І., к.т.н., в.о. завідувача кафедри*

Схвалено науково-методичною радою з якості ННІ КІТІ
Протокол №3 від “06” січня 2025 року

Голова науково-методичної ради з якості ННІ: *Мартинюк П.М., д.т.н., професор.*

Попередня версія силабусу: *відсутня*.

ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ	
Основи Web-безпеки	
ЗАГАЛЬНА ІНФОРМАЦІЯ	
Ступінь вищої освіти	*Бакалавр*
Освітня програма	*Комп'ютерна інженерія*
Спеціальність	*123 Комп'ютерна інженерія*
Рік навчання, семестр	*2-й рік, 1-й семестр*
Кількість кредитів	*4*
Лекції:	*20/2 годин*
Лабораторні заняття:	*20/10 годин*
Самостійна робота:	*80/108 годин*
Курсова робота:	*ні*
Форма навчання	*денна/заочна*
Форма підсумкового контролю	*залік*
Мови викладання	*українська*
ІНФОРМАЦІЯ ПРО РОЗРОБНИКА	

Лектор 	*Бойчура Михайло Володимирович* *к.т.н., доцент кафедри обчислювальної техніки*
Вікіситет	*http://wiki.nuwm.edu.ua/index.php/Бойчура_Михайло_Володимирович*
ORCID	*https://orcid.org/0000-0002-9073-4037*
Канали комунікації	*m.v.boichura@nuwm.edu.ua*, *групи у месенджерах*

ІНФОРМАЦІЯ ПРО НАВЧАЛЬНУ ДИСЦИПЛІНУ

Мета та завдання

Сучасний світ неможливий без веб-додатків, які стали невід'ємною частиною нашого життя. Проте водночас з розвитком веб-технологій зростають і загрози, пов'язані з безпекою даних. Кіберзлочинці постійно вдосконалюють свої методи атак, що вимагає від розробників та адміністраторів глибоких знань про потенційні вразливості та способи їх запобігання.

Курс «Основи Web-безпеки» спрямований на формування розуміння ключових аспектів безпеки веб-додатків. Студенти дізнаються про поширені типи атак, такі як XSS, SQL-ін'єкції, атаки на HTTP-заголовки, а також ознайомляться з методами їхнього виявлення та захисту. Окрім цього, дисципліна охоплює питання автентифікації, шифрування та безпечного зберігання паролів. Лабораторні заняття передбачають практичну роботу з тестування вразливостей та впровадження захисних механізмів.

***Метою** дисципліни «Основи Web-безпеки» є ознайомлення студентів із фундаментальними принципами безпеки веб-ресурсів, вивчення методів атак та способів їхнього запобігання.*

***Завдання** дисципліни:*

- *формування розуміння ключових аспектів безпеки веб-додатків;*
- *вивчення поширених атак (XSS, SQL-ін'єкції, атаки на HTTP-заголовки);*
- *ознайомлення з методами виявлення та захисту від атак;*
- *розгляд питань автентифікації, шифрування та безпечного зберігання паролів;*
- *практичне тестування вразливостей та впровадження захисних механізмів.*

Посилання на розміщення освітнього компонента на навчальній платформі Moodle, на платформі освітніх програм та їхніх освітніх компонентів
https://exam.nuwm.edu.ua/course/view.php?id=7324
Передумови вивчення (місце освітнього компоненту в структурно-логічній схемі)
Для засвоєння даної дисципліни у повній мірі необхідно засвоїти ОК 3 «Іноземна мова». *Отримані навички будуть корисними при вивченні ВБ 6.2 «Безпека банківських систем».*
Компетентності
Р1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі комп'ютерної інженерії. *Р3. Здатність створювати системне та прикладне програмне забезпечення комп'ютерних систем та мереж.* *Р6. Здатність проектувати, впроваджувати та обслуговувати комп'ютерні системи та мережі різного виду та призначення.* *Р7. Здатність використовувати та впроваджувати нові технології, включаючи технології розумних, мобільних, зелених і безпечних обчислень, брати участь в модернізації та реконструкції комп'ютерних систем та мереж, різноманітних вбудованих і розподілених додатків, зокрема з метою підвищення їх ефективності.*
Програмні результати навчання (ПРН). Результати навчання (РН)*
N9. Вміти застосовувати знання технічних характеристик, конструктивних особливостей, призначення і правил експлуатації програмно-технічних засобів комп'ютерних систем та мереж для вирішення технічних задач спеціальності. *N11. Вміти здійснювати пошук інформації в різних джерелах для розв'язання задач комп'ютерної інженерії.*

СТРУКТУРА ТА ЗМІСТ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

№	Тема	Опис лекції	Опис лабораторного заняття
МОДУЛЬ 1. Змістовий модуль 1. Вступ до безпеки веб-додатків			
1	Вступ до безпеки веб-ресурсів. 2 год. лекцій 2 год. лабораторних N9, N11	Основні поняття веб-безпеки. Сучасні загрози та тенденції у сфері захисту веб-додатків. Огляд стандартів та найкращих практик безпеки.	Ознайомлення з базовими інструментами для аналізу безпеки веб-ресурсів (Burp Suite, OWASP ZAP). Виконання тестового аналізу простого веб-сайту.
2	Міжсайтові сценарії (XSS). 2 год. лекцій 2 год. лабораторних N9, N11	Види XSS-атак (відбиті, збережені, DOM). Наслідки атак на веб-додатки та методи їх запобігання.	Виявлення вразливостей XSS у спеціально підготовленому веб-додатку. Реалізація та тестування контрзаходів.
3	Атаки на рівні DOM (DOM XSS). 2 год. лекцій 2 год. лабораторних N9, N11	Взаємодія JavaScript із DOM. Способи виконання DOM XSS атак та методи захисту.	Аналіз коду веб-додатку на предмет DOM XSS. Практичне виправлення вразливостей.
4	SQL-ін'єкції. 2 год. лекцій 2 год. лабораторних N9, N11	Основи SQL-ін'єкцій. Способи виконання атак. Методи захисту (підготовлені запити, валідація введених даних).	Використання SQLMap для виявлення SQL-ін'єкцій. Захист бази даних від атак.
5	Використання SQL-ін'єкцій UNION. 2 год. лекцій 2 год. лабораторних N9, N11	Як працює UNION SQL-ін'єкція. Способи вилучення даних із бази через UNION-запити.	Проведення атаки за допомогою UNION SELECT. Впровадження засобів захисту.
МОДУЛЬ 2. Змістовий модуль 2. Захист веб-додатків від атак			
6	XML-ін'єкції (XXE). 2 год. лекцій 2 год. лабораторних N9, N11	Використання XML у веб-додатках. XXE-атаки та їхні наслідки.	Атакування XML-процесора за допомогою XXE. Практична реалізація засобів захисту.
7	Отруєння веб-кешу. 2 год. лекцій 2 год. лабораторних N9, N11	Механізми кешування у веб-додатках. Атаки на кеш. Методи запобігання отруєнню.	Проведення тестів з отруєння кешу. Впровадження заголовків захисту кешу.
8	Атаки на HTTP-заголовки. 2 год. лекцій 2 год. лабораторних N9, N11	Вразливості, пов’язані з HTTP-заголовками (Host Header Attack, CORS, Clickjacking).	Атака на заголовки HTTP. Налаштування серверної конфігурації для їхнього захисту.
9	Вразливості розкриття інформації. 2 год. лекцій 2 год. лабораторних N9, N11	Розкритя даних через невірні налаштування. Слабкі місця коду.	Аналіз логів та публічно доступних даних для виявлення витоків інформації.
10	Практичне тестування безпеки. 2 год. лекцій 2 год. лабораторних N9, N11	Комплексний підхід до тестування безпеки веб-додатків. Автоматизовані та ручні методи тестування.	Виконання комплексного тесту безпеки веб-додатку. Підготовка звіту про знайдені вразливості та пропозиції щодо їх усунення.

Форми, методи та технології навчання

Форми навчання	• *очна (денна) з, можливо, елементами дистанційного навчання;* • *заочна.*
Форми навчального процесу	• *навчальні заняття (лекції, лабораторні заняття, консультації);* • *самостійна робота здобувачів;* • *робота в наукових бібліотеках та мережі Інтернет;* • *контрольні заходи (поточна складова оцінювання, модульні контролі, підсумковий контроль).*
Методи та технології навчання	• *індивідуальна робота;* • *контекстне навчання.*
Засоби навчання	• *відеозапис лекції;* • *презентація;* • *конспект лекцій;* • *різні туторіали.*

Інструменти, обладнання, програмне забезпечення

- *Virtual VM Box;*
- *Kali Linux;*
- *Parrot OS;*
- *Burp Suite;*
- *OWASP ZAP;*
- *SQLMap;*
- *Wireshark;*
- *Postman;*
- *веб-сайт для проведення олімпіад (API, база даних та ін.).*

Порядок оцінювання програмних результатів навчання/ результатів навчання

Студент може отримати 100 балів, враховуючи наступну розбаловку:

1) *модульні контролі: 40 балів;*
2) *поточний контроль: 50-60 балів;*
3) *додаткові бали: 0-10 балів.*

Розподіл балів:

1) *за модульні контрольні роботи:*
   - *модульний контроль №1 (20 балів):*
     Рівень 1 – 19 запитань по 0.5 балів за кожне.
     Рівень 2 – 6 запитань по 0.9 балів за кожне.
     Рівень 3 – 3 запитання по 1.7 балів за кожне.
   - *модульний контроль №2 (20 балів):*
     Рівень 1 – 19 запитань по 0.5 балів за кожне.

Рівень 2 – 6 запитань по 0.9 балів за кожне.

Рівень 3 – 3 запитання по 1.7 балів за кожне.

2) *за поточний контроль (50-60 балів):*

Передбачено по 6 балів за кожну лабораторну роботу; у випадку правильного виконання лабораторної роботи оцінка лінійно залежить від глибини аналізу вразливостей та коректності їх усунення. Як альтернатива, студенти можуть виконувати завдання з використанням інших методів тестування безпеки веб-додатків, але за умови попереднього узгодження деталей з викладачем.

3) *додаткові бали за вагому громадянську та студентську активність (0-10 балів):*

Виставляється до 10 балів за волонтерство, олімпіади, спартакіади, конкурси, конференції, написання статей, активну студентську діяльність, конкретні пропозиції з удосконалення змісту навчальної дисципліни тощо.

Основні критерії, що характеризують рівень компетентності здобувача вищої освіти при оцінюванні результатів поточного та підсумкового контролів з навчальної дисципліни:

- *виконання всіх видів навчальної роботи, що передбачені силабусом навчальної дисципліни;*
- *глибина і характер знань навчального матеріалу за змістом навчальної дисципліни, що міститься в основних та додаткових рекомендованих літературних джерелах;*
- *вміння аналізувати явища, що вивчаються, у їх взаємозв'язку і розвитку;*
- *характер відповідей на поставлені запитання (чіткість, лаконічність, логічність, послідовність тощо);*
- *вміння застосовувати теоретичні положення під час розв'язання практичних задач;*
- *вміння аналізувати достовірність одержаних результатів;*
- *дотримання вимог до оформлення (технологічної документації, ДСТУ тощо).*

Критерії оцінювання лабораторних робіт (у % від кількості балів, виділених на завдання із заокругленням до цілого числа):

- *0% – завдання не виконано;*
- *40% – завдання виконано частково та містить суттєві помилки методичного або розрахункового характеру, порушені вимоги до оформлення;*
- *60% – завдання виконано повністю, але містить суттєві помилки у розрахунках або в методиці, порушені вимоги до оформлення;*
- *80% – завдання виконано повністю, проте містить окремі несуттєві недоліки;*
- *100% – завдання виконано правильно і без зауважень.*

Рекомендована література (основна, допоміжна)

Основна література

1. *Остапов С.Е., Євсеєв С.П., Король О.Г. Кібербезпека: сучасні технології захисту: навч. посіб. Львів: «Новий Світ-2000», 2020. 678 с.*
2. *Борсуковський Ю.В., Борсуковська В.Ю., Бурячок В.Л. та ін. Прикладні аспекти інформаційної та кібернетичної безпеки держави. Аналіз мережевого трафіку: навч. посіб. Львів: Видавництво «Магнолія 2006», 2024. 222 с.*
3. *Hsu T.H.-C. Practical Security Automation and Testing. Birmingham: Packt Publishing Ltd, 2019. 245 p.*
4. *Ball C.J. Hacking APIs. Burlingame: No Starch Press, 2022. 368 p.*
5. *Wear S. Burp Suite Cookbook: Web application security made easy with Burp Suite. 2nd ed. Birmingham: Packt Publishing, 2023. 450 p.*

Допоміжна література

1. *OWASP Web Security Testing Guide | OWASP Foundation. URL: https://owasp.org/www-project-web-security-testing-guide/ (Last access: 27.11.2024).*
2. *What is ParrotOS? | ParrotOS Documentation. URL: https://parrotsec.org/docs/introduction/what-is-parrot (Last access: 27.11.2024).*
3. *Живило Є.О. Тестування на проникнення: навч. посіб. Полтава: ПНТУ "Полтавська політехніка ім. Юрія Кондратюка", 2024. 239 с.*
4. *Rakshit S.K. Ethical Hacker's Penetration Testing Guide. London: BPB Online, 2022. 509 p.*
5. *Савченко В., Мнушка О. Сучасні технології безпечного програмування: навч. посіб. Харків: НТУ «ХПІ», 2024. 180 с.*

Інформаційні ресурси в Інтернеті

1. *https://www.youtube.com/playlist?list=PLQ-w8CQDSqFBsH_fm34QmFv-iWY0e2AWQ (список відтворення Script kiddie від Lazy IT).*
2. *https://www.youtube.com/playlist?list=PLUHSo5hXwGIh0Yrr0pKCkdpImEdUd1MSP (список відтворення Kali Linux від Hacker Joe).*
3. *https://www.youtube.com/watch?v=AL5YcDTbnS0 (відео How to Use SQLmap to Test for SQL Injection Vulnerability | Full Tutorial від Motasem Hamdan).*

ПОЛІТИКИ ВИКЛАДАННЯ ТА НАВЧАННЯ

Перелік соціальних, «м'яких» навичок (soft skills)

Вміння комунікувати.	• *здатність спілкуватися державною мовою як усно, так і письмово;* • *навички усного спілкування;* • *навички письмового спілкування.*
Здатність до аналізу та синтезу.	• *вміння критично мислити;* • *здатність знаходити вихід з складних ситуацій;* • *здатність до навчання;* • *вміння комплексного рішення проблем.*
Здатність застосовувати знання у практичних ситуаціях.	

Дедлайни та перескладання

Дедлайн здачі лабораторних робіт – остання середа перед закінченням сесії. Здача лабораторних робіт відбувається на парі або під час консультації, дата та час якої гнучко узгоджується між студентом та викладачем.

На здачу кожного з модульних контролів студенту надається одна спроба. Перший модуль здається на будь-якій лекції у жовтні, а другий – на передостанній чи останній лекції. Перездача окремого модульного контролю передбачена лише за виключних обставин.

У випадку, якщо студент не набрав 60 балів або здав менше двох модулів, він має право на початку сесії звернутись до викладача з проханням організувати здачу підсумкового контролю. При цьому, набрані попередньо оцінки за модульні контролі – анулюються.

У разі, якщо по закінченню сесії здобувач не набрав 60 балів, його відправляють на комісію для розгляду результатів підсумкового контролю, яка рекомендує здобувачу із академічною заборгованістю покращити результати підсумкового контролю одним із наступних шляхів: повторного складання підсумкового контролю, повторного вивчення освітньої компоненти чи повторного курсу навчання.

Неформальна та інформальна освіта

Здобувачі мають право на часткове або повне перезарахування дисципліни за умови написання ними відповідної заяви, заповнення декларації та надання документів, які підтверджують ті результати навчання, які здобувач отримав (див. положення https://ep3.nuwm.edu.ua/28363/). Зокрема студенти можуть самостійно проходити онлайн-курси на таких навчальних платформах, як Prometheus, Coursera, edX, edEra, FutureLearn та інших, для наступного перезарахування результатів навчання. Проте доцільно попередньо узгодити з викладачем відповідність обраного онлайн-курсу суті навчальної дисципліни. Деякий перелік підходящих курсів наведено нижче:

- *Coursera – Getting Started in Port Scanning Using Nmap and Kali Linux (Початок роботи зі скануванням портів за допомогою Nmap і Kali Linux);*
- *Coursera – IBM Cybersecurity Analyst Professional Certificate (Професійний сертифікат аналітики з кібербезпеки IBM);*
- *Coursera – Advanced Network Security and Analysis (Розширена мережева безпека та аналіз).*

Зручний пошук курсів доступний тут: https://www.classcentral.com/.

Також університет має до 5000 кредитів на платформі для навчання Google Cloud Skills Boost, частину з яких студенти можуть отримати, звернувшись на корпоративну пошту адміністратора платформи m.v.boichura@nuwm.edu.ua.

Окрім того, *якщо з'являються обставини для здобуття неформальної чи інформальної освіти від викладачів-практиків, то пропонуються ці можливості для студентів; рекомендуються відео-уроки практикуючих програмістів з YouTube тощо.*

Правила академічної доброчесності

Задля запобігання академічної недоброчесності вимагається наступне:

- *кожен студент у групі виконує завдання згідно запропонованого йому варіанту або пропонує свою тему, яку обов'язково узгоджує з викладачем;*
- *студентам забороняється: плагіатити, самоплагіатити, фабрикувати, фальсифікувати, списувати, обманювати або будь-яким чином намагатись вплинути на викладача.*

Залежно від виду та ступеня порушення викладач може накладати наступні санкції:

- *усне або письмове зауваження від викладача;*
- *попередження про можливість притягнення до академічної відповідальності;*
- *зниження чи анулювання результатів оцінювання навчального завдання здобувача вищої освіти;*
- *повторне виконання навчального завдання;*
- *виконання іншого навчального завдання;*
- *призначення додаткового навчання з питань академічної доброчесності;*
- *призначення додаткових контрольних заходів (додаткові індивідуальні навчальні завдання, тести тощо);*
- *подання клопотання на ім'я ректора з метою порушення формальної процедури розгляду питання про притягнення студента до відповідальності.*

За списування під час проведення модульного контролю чи підсумкового контролю студент позбавляється подальшого права здавати матеріал і у нього виникає академічна заборгованість.

Документи стосовно академічної доброчесності (про плагіат, порядок здачі курсових робіт, кодекс честі студентів, документи Національного агентства стосовно доброчесності) наведені на сторінці «Якість освіти» сайту НУВГП – https://nuwm.edu.ua/sp/akademichna-dobrochesnistj.

Вимоги до відвідування

Санкції за пропуски пар не передбачені. Студент має право самостійно вивчити необхідний для здачі модульних контролів та лабораторних робіт матеріал, який в повному обсязі дублюється викладачем одночасно на платформі Moodle та/або у групі з даної дисципліни в певному месенджері. Також викладач розміщує відеозаписи пар на YouTube. У разі необхідності проведення консультації – викладач йде назустріч.

Відвідування пари допускається із використанням власного ноутбука. Студенти не повинні порушувати дисципліну на парі.

Для студентів, які знаходяться на індивідуальному плані навчання, надаються індивідуальні завдання.

Автор
Доцент ОТ

Михайло БОЙЧУРА

Затверджено

Проректор з науково-педагогічної та навчальної роботи

Валерій СОРОКА

документ підписаний КЕП
Номер документа СИЛ №767
Підписувач Сорока Валерій Степанович
Підписувач (дані КЕП):
Сертифікат 3FAA9288358EC003040000009B6C3700C8C2C100