ЗАТВЕРДЖЕНО

Вченою радою факультету
факультету інформаційно-
комп'ютерних технологій
31 серпня 2023 р., протокол № 5

Голова Вченої ради
_____ Тетяна НІКІТЧУК

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ ВК «БЕЗПЕКА WEB-ДОДАТКІВ»

для здобувачів вищої освіти освітнього ступеня «магістр»
спеціальності 125 «Кібербезпека та захист інформації»
освітньо-професійна програма «Кібербезпека»
факультет інформаційно-комп'ютерних технологій
кафедра комп'ютерної інженерії та кібербезпеки

Схвалено на засіданні
кафедри комп'ютерної
інженерії та кібербезпеки
28 серпня 2023 р., протокол № 7

Завідувач кафедри
_____ Андрій ЄФІМЕНКО

Гарант освітньо-
професійної програми
_____ Володимир ВОРОТНІКОВ

Розробник: кандидат технічних наук, доцент кафедри комп'ютерної інженерії та кібербезпеки Олександр ПІРОГ

Житомир
2023 – 2024 н.р.

1. Опис навчальної дисципліни

Найменування показників	Галузь знань, напрям підготовки, освітній ступінь	Характеристика навчальної дисципліни	
		денна форма навчання	заочна форма навчання
Кількість кредитів 3	Галузь знань 12 «Інформаційні технології»	за вибором	
Модулів – 1	Спеціальність 125 «Кібербезпека та захист інформації»	Рік підготовки:	
Змістових модулів – 1		1	1
		Семестр	
Загальна кількість годин - 120		2	2
		Лекції	
Тижневих годин для денної форми навчання: аудиторних 2 самостійної роботи – 3,6	Освітній ступінь «магістр»	16 год.	4 год.
		Практичні	
		__ год.	__ год.
		Лабораторні	
		32 год.	6 год.
		Самостійна робота	
		72 год.	110
		Вид контролю: залік	

Співвідношення кількості годин аудиторних занять до самостійної та індивідуальної роботи становить:

для денної форми навчання – 40 % аудиторних занять, 60 % самостійної та індивідуальної роботи.

для заочної форми навчання – 8 % аудиторних занять, 92 % самостійної та індивідуальної роботи.

2. Мета та завдання навчальної дисципліни

Метою навчальної дисципліни є формування у студентів знань, умінь і компететностей, необхідних для вирішення задач захисту web-систем.

Завданнями вивчення навчальної дисципліни є формування теоретичних знань та практичних умінь у сфері забезпечення безпеки web-ресурсів, в тому числі:

– знати основні вразливості web-систем;

– вміти аналізувати, виявляти та оцінювати можливі загрози, вразливості web-систем;

– вміти розробляти політики безпеки web-систем;

– вміти забезпечувати захист програм, баз даних та інформації, що обробляється у web-системах;

– вміти забезпечувати безперервну працездатність web-систем;

– вміти вирішувати задачі забезпечення та супроводу, в тому числі: огляд, тестування web-систем на вразливості;

– вміти управляти процедурами ідентифікації, аутентифікації, авторизації користувачів у web-системах;

– вміти реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформації у web-системах.

Зміст навчальної дисципліни направлений на формування наступних **компетентностей**:

Здатність застосовувати знання у практичних ситуаціях;

Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням;

Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки;

Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки;

Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки;

Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

Отримані знання з навчальної дисципліни стануть складовими наступних **програмних результатів**:

Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень;

Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах;

Вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;

Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки;

Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;

Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових).

Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків;

Вирішувати задачі аналізу програмного коду на наявність можливих загроз.

3. Програма навчальної дисципліни

Тема 1. Web-системи: вразливості, моделі загроз та безпеки.

Клієнт-серверна архітектура. Вимоги до безпеки в контексті вимог до додатків. OWASP Top Ten. Схема атаки. Методи злому. Структура фішингової атаки. Ознаки фішингової атаки. Методи боротьби. Політики безпеки (Policy), модель загроз (Threat model), механізми забезпечення безпеки (Mechanism). Поняття web-додатку, web-системи. Види веб-додатків. Основні вразливості. Поняття web-безпеки. Стандартизація вхідного контенту. Модель безпеки браузерів – політика однакового походження (same-origin policy). HTTP заголовки безпеки. Що необхідно знати пентестеру, дерево скілів.

Тема 2. Аутентифікація. Управління сесіями. Контроль доступу. Адміністрування прав доступу в web-системах.

Ідентифікація, аутентифікація, контроль доступу. Паролі. Хеш-шифрування. Метод перебору (brute-force атаки). Rainbow tables. Інструменти злому паролів: John the Ripper, Hydra, Medusa. «Соління» паролів (salt). Протокол «виклик/відповідь» (challenge/response protocol). Обмеження числа спроб вгадування пароля (antihammer). Перебір за словником (dictionary attack). Методи кодування та шифрування. Оцінка ефективності схем аутентифікації. Біометрична аутентифікація. Багатофакторна аутентифікація (MFA). Управління сесіями (Sniffing, Hijack). Токени, JSON, JWT, JWK. Контроль доступу. Незахищені прямі посилання на об’єкти (IDOR). Необмежене завантаження файлів (Unrestricted File Upload). Адміністрування прав доступу в

web-системах. Відповіді сервера. Адміністрування Apache та MySQL. Права програм на сервері та їх обмеження. Права доступу. Розмежування прав, ролі користувачів.

Тема 3. Вразливості web-додатків.

Нульовий байт, символи рівня директорій. Web-форми. Методи GET/POST. Обробка вхідних даних. Міжсайтовий скріптинг (XSS). Контексти XSS атак. Запобігання XSS. Підробка міжсайтових запитів (CSRF). Класифікація CSRF. Захист від CSRF. SQL ін'єкції (SQL injection). Паттерни SQL ін'єкцій. UNION SQL ін'єкції. Сліпі SQL ін'єкції. Інформаційна схема БД. Ін'єкції NoSQL. Запобігання атакам SQL. Введення зовнішньої сутності XML (XXE). Запобігання атакам XXE. Введення команд ОС (OS command injection). Сліпе введення команди ОС. Запобігання атакам введення команд ОС. Небезпечна десеріалізація (Insecure Deserialization). Запобігання атакам небезпечної десеріалізації. Підробка запитів на стороні сервера (SSRF). Запобігання атакам SSRF.

Тема 4. DoS-атаки.

DoS/DDoS атаки. Ботнет. ICMP-флуд прямий (Ping) і обернений (Smurf). Переповнення буферу. Teardrop. UDP-флуд. HTTP-флуд. Атака посилення (Amplification Attack). DNS-флуд. SYN-флуд. Атака додатку. Slowloris. ReDoS. Посилення NTP. Атаки нульового дня. Серверні та клієнтські вразливості. Захист від DoS вразливостей.

Тема 5. Розкриття інформації.

Класифікація даних. Витоки даних. Класи вразливостей web-сервера. Розкриття інформації в web-системах. Відбитки пальців web-сервера / програми (Web Server/Application Fingerprinting). Індексація каталогів (Directory Indexing). Витік інформації (Information Leakage). Розкриття чутливої інформації (Sensitive Data Exposure). Обхід шляху (Path Traversal). Витік повного шляху (Full path disclosure). Розкриття структури БД (SQL DB Structure Extraction). Передбачуване місцезнаходження ресурсу (Predictable Resource Location). Захист від Full path disclosure вразливостей. Методологія хакінгу. Розвідка інфраструктури web-вузлу, web-додатку, ПЕОМ адміністраторів та користувачів. Тестування компонентів системи. Методи протидії розкриттю інформації.

Тема 6. Тестування web-додатків.

Принципи, склад та види тестування безпеки ПЗ. Вимоги до безпеки. Тестова документація. Тестування на проникнення (Pentesting). Види тестів на проникнення. Фази тестування. Визначення області тестування (Scope). Технічне завдання. Угода про нерозголошення (NDA). Збір інформації: пасивний/активний. Whois, Shodan, TheHarvester, Google dorking, Gophish. Типи сканування. Типи, причини, тактики підвищення привілеїв (Privilege Escalation). Nikto, Greenbone, Nmap, FFuF, Wfuzz, Burp Suite, OWASP ZAP, Hydra, WPScan, Sqlmap, Online Hash Crack, Responder, John the Ripper, Wireshark. Приманка

(Honeypot). Metasploit: інтерфейси, модулі, Meterpreter. Зворотна оболонка (reverse shell). Netcat. Прибирання. Докази. Видалення. Звіт про тестування.

Тема 7. Безпечне програмування.

Безпека протягом усього процесу розробки. Вимоги. Фази, шаблони атак. Проблеми якості ПЗ. Превентивний захист. Вразливості конфігурації, інфраструктури, людський фактор. Атаки соціальної інженерії. Інтерфейс користувача. Сприяння безпечній поведінці. Обмеження користувацького вводу. Політика аутентифікації. Життєвий цикл розробки ПЗ (SDLC). Вбудована система безпеки на всіх етапах. Стандарти та моделі безпечного SDLC. Безпека процесу розробки. Принципи проектування безпеки. Захист середовища розробки. Безпека через невідомість (Security by Obscurity). Підхід Security by Design. Принципи проектування безпеки OWASP. Шаблони безпеки. Модульний дизайн. Рекомендації щодо уникнення поширених помилок при проектуванні. Визначення ризику. Моделювання загроз. Інструменти та методики моделювання: PASTA, DREAD. Стратегії реагування. Контрзаходи STRIDE. Поширені помилки програмування. Переповнення буфера. Умови перегонів. Рекомендації щодо запобігання вразливостям (Web, Mobile, IoT). Контроль сесії. Керування паролями. Відновлення пароля. Типи тестів протягом SDLC. Статичний, динамічний аналіз коду. PyLint, OWASP ZAP. Моніторинг ПЗ. Технічне обслуговування ПЗ.

Тема 8. Економіка web-безпеки.

Причини комп'ютерних злочинів. Результативність (effectiveness). Ефективність (efficiency). Збитковість економічних комп'ютерних злочинів. Собівартість комп'ютерних злочинів. Методи підвищення собівартості комп'ютерних злочинів. Спам (spam), дорвеї (doorway), ринок посилань, накруток (заходи, постінг, підписки, перегляди, лайкі), сателіти (satellite), DoS-атаки. Принципи інвестування у web-безпеку.

4. Структура (тематичний план) навчальної дисципліни

Змістові модулі і теми	Кількість годин							
	денна форма				заочна форма			
	усього	лекції	практичні	самостійна робота	усього	лекції	практичні	самостійна робота
Тема 1. Web-системи: вразливості, моделі загроз та безпеки.	12	2		10	15,5	0,5		15
Тема 2. Аутентифікація. Управління сесіями. Контроль доступу. Адміністрування прав доступу в web-системах.	22	2	12	10	19,5	0,5	4	15
Тема 3. Вразливості web-додатків.	20	2	8	10	17,5	0,5	2	15
Тема 4. DoS-атаки.	11	1		10	15,5	0,5		15
Тема 5. Розкриття інформації.	15	1	4	10	17,5	0,5	2	15
Тема 6. Тестування web-додатків.	16	2	4	10	15,5	0,5		15
Тема 7. Безпечне програмування.	18	4	4	10	16,5	1		15
Тема 8. Економіка web-безпеки.	4	2		2	5			5
ВСЬОГО	120	16	32	72	120	4	6	110

5. Теми практичних (лабораторних) занять

№ з/п	Назва теми	Кількість годин	
		денна форма	заочна форма
1	Вступне заняття.	2	
2	Вразливості контролю доступу. Міжсайтові сценарії (XSS). Підробка міжсайтових запитів (CSRF)	4	1
3	Аутентифікація. Авторизація.	8	1
4	Адміністрування сервера Apache та баз даних MySQL.	4	1
5	Права доступу в web-системах.	4	1
6	SQL-ін’єкції. Введення зовнішньої сутності XML (XXE)/ Введення команд ОС.	4	1
7	Вразливості бізнес-логіки. Обхід каталогу. Розкриття інформації.	4	1
8	Підсумкове заняття: захист лабораторних робіт.	2	
РАЗОМ		32	6

6. Завдання для самостійної роботи

Тема 1. Вразливості бізнес-логіки.
Тема 2. Контрабанда запитів HTTP.
Тема 3. Атаки заголовка хосту HTTP.
Тема 4. Вразливості на основі DOM.
Тема 5. Введення шаблону на стороні сервера.
Тема 6. Спільне використання ресурсів (CORS).
Тема 7. WebSockets.
Тема 8. Отруєння web-кешем.

7. Індивідуальні завдання

(не передбачені навчальним планом)

8. Методи навчання

Навчання в аудиторіях відбувається в формі лекційних та лабораторних занять. Для полегшення засвоєння матеріалу використовуються технічні засоби.

9. Методи контролю

Навчальні досягнення студентів з дисципліни оцінюються за рейтинговою системою, в основу якої покладено принцип пооопераційної звітності, накопичувальної системи оцінювання рівня знань, умінь та навичок.

Контроль складається з поточного контролю виконання студентами самостійної роботи, контролю виконання лабораторних робіт та підсумкового контролю, в тому числі у вигляді комп'ютерних тестів, захисту лабораторних робіт у формі співбесіди. Поточний контроль здійснюється під час проведення лабораторних робіт для перевірки рівня підготовки студента до виконання конкретної роботи. Форма проведення поточного контролю: усне індивідуальне опитування, вирішення ситуаційних задач, виконання практичної роботи. Підсумковий контроль знань студентів здійснюється після завершення вивчення навчального матеріалу у вигляді комп'ютерних тестів. Методи самоконтролю: уміння самостійно оцінювати свої знання, самоаналіз.

Кількість балів за лабораторну роботу залежить від дотримання таких вимог:

- своєчасності виконання завдань;
- повноти обсягу їх виконання;
- якості виконання завдань;
- самостійності виконання;
- творчого підходу у виконанні завдань;
- ініціативності у навчальній діяльності;
- глибини розуміння теми роботи;
- якості відповідей на поставлені питання підчас захисту роботи.

Контроль успішності студентів з урахуванням поточного і підсумкового оцінювання здійснюється відповідно до таблиці розподілу балів дисципліни, де зазначено види контролю і кількість балів за видами. Систему рейтингових балів для різних видів контролю та порядок їх переведення у національну (4-бальну) та європейську (ECTS) шкалу подано нижче у таблиці шкала оцінювання.

10. Розподіл балів

Поточне тестування та самостійна робота							Сума
Л1	Л2	Л3	Л4	Л5	Л6	Тест	100
9	9	9	9	9	9	46	

Шкала оцінювання

За шкалою	Екзамен	Залік	Бали
A	Відмінно	Зараховано	90-100
B	Добре	Зараховано	82-89
C			74-81
D	Задовільно	Зараховано	64-73
E			60-63
FX	Незадовільно	Не зараховано	35-59
F		Не зараховано	0-34

11. Рекомендована література

Основна література

1. The Web Security Academy. – URL: https://portswigger.net/web-security
2. OWASP Foundation. – URL: https://owasp.org/
3. Hoffman A. Web Application Security Exploitation and Countermeasures for Modern Web Application 2021, 328 p.
4. Sinha S. Bug Bounty Hunting for Web Security, 2019, 228 p.
5. Blokdyk G. OWASP: Third Edition, Brendale: The Art of Service, 2018, 124 p.

Допоміжна література

1. Посібник з web-безпеки. – URL: http://websecurity.com.ua/security
2. Zeldovich N. Computer Systems Security. – URL: https://css.csail.mit.edu/6.858/2020/
3. Bell L. Agile Application Security, 2018, 448 p.
4. Andre A. Professional Pen Testing for Web Applications, Indianapolis: Wiley Publishing Inc., 2006, 502 p.

12. Інформаційні ресурси в Інтернеті

1. Zeldovich N. Computer Systems Security. – URL: https://css.csail.mit.edu/6.858/2020/
2. The Web Security Academy. – URL: https://portswigger.net/web-security
3. Посібник з web-безпеки. – URL: http://websecurity.com.ua/security/
4. OWASP Foundation. – URL: https://owasp.org/

*Індекс структурного підрозділу відповідно до наказу ректора «Про затвердження організаційної структури Державного університету «Житомирська політехніка» (наприклад, 22.06).
** Індекс освітньої програми відповідно до наказу ректора «Про індексацію освітніх програм Державного університету «Житомирська політехніка» (наприклад, 122.00.1/Б).
*** Шифр освітньої компоненти в освітній програмі (наприклад, ОК1).