МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

ЗАТВЕРДЖУЮ
В.о. декана факультету комп'ютерних інформаційних технологій
Ігор ЯКИМЕНКО
_____2023 р.

ЗАТВЕРДЖУЮ
В.о. проректора
з науково-педагогічної роботи
Віктор ОСТРОВЕРХОВ
"___" _____2023 р.

РОБОЧА ПРОГРАМА

з дисципліни «Методи та засоби захисту програмного забезпечення»

Ступінь вищої освіти: магістр

галузь знань – 12 «Інформаційні технології»

спеціальність – 121 «Інженерія програмного забезпечення»

освітньо-наукова програма – «Математичне та програмне забезпечення комп'ютерних систем»

Кафедра комп'ютерних наук

Форма навчання	Курс	Семестр	Лекції (год.)	Прак. (год.)	ІРС (год.)	Тренінг (год.)	СРС (год.)	Разом (год.)	Екзамен (сем.)
денна	І	І	30	14	4	4	98	150	1

31.08.2023р.

Тернопіль, 2023

Робоча програма складена на основі освітньо-професійної програми підготовки магістрів галузі знань 12 Інформаційні технології спеціальності 121 Інженерія програмного забезпечення, затвердженої Вченою Радою ЗУНУ (протокол № 10 від «23» 06 2023 р.).

Робочу програму склав доцент кафедри комп'ютерних наук, к.т.н. Руслан ШЕВЧУК

Робоча програма затверджена на засіданні кафедри комп'ютерних наук, протокол №1 від 28 серпня 2023р.

Завідувач кафедри д.т.н, професор _____Андрій ПУКАС

Розглянуто та схвалено групою забезпечення спеціальності 121 Інженерія програмного забезпечення, протокол №1 від 30 серпня 2023 р.

Голова групи
забезпечення спеціальності,
д.т.н., професор _____Микола ДИВАК

Гарант ОП
к.т.н., доцент _____Ірина СПІВАК

СТРУКТУРА РОБОЧОЇ ПРОГРАМИ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«Методи та засоби захисту програмного забезпечення»

1. Опис дисципліни «Методи та засоби захисту програмного забезпечення»

Дисципліна «Методи та засоби захисту програмного забезпечення»	Галузь знань, спеціальність, ступінь вищої освіти	Характеристика навчальної дисципліни
Кількість кредитів : Денна - 5	Галузь знань - 12 “Інформаційні технології”	Статус дисципліни: обов’язкова Мова навчання: українська
Кількість залікових модулів - 4	Спеціальність: 121 «Інженерія програмного забезпечення» Спеціалізація – «Математичне та програмне забезпечення комп’ютерних систем»	Рік підготовки: *Денна – 1* Семестр: *Денна – 1*
Кількість змістових модулів – 2	Ступінь вищої освіти – магістр	Лекції: *Денна* – 30 год, Практичні заняття: *Денна* – 14 год,
Загальна кількість годин: Денна – 150		Самостійна робота: *Денна* – 98 год, тренінг – 4 год., Індивідуальна робота: *Денна* – 4 год.
Тижневих годин: Денна форма навчання – 10 год., з них аудиторних 3 год. (лекційних – 2 год., практичних – 1 год.)		Вид підсумкового контролю – екзамен

2. Мета і завдання вивчення дисципліни «Методи та засоби захисту програмного забезпечення»

2.1. Мета вивчення дисципліни

Метою курсу „Методи та засоби захисту програмного забезпечення” є вивчення студентами методологічних та методичних питань щодо дослідження вразливостей та захисту програмного забезпечення, набуття спеціальних знань і практичних навиків застосування методів та засобів побудови ефективних систем захисту програмного забезпечення. Курс "Методи та засоби захисту ПЗ" охоплює теоретичні та практичні основи роботи з методами та засобами дослідження вразливостей та захисту програмного забезпечення. Названий курс

повинен сприяти формуванню висококваліфікованих фахівців в галузі знань «Інформатика та обчислювальна техніка».

Оволодіння цим курсом повинне виробити у студентів навички практичного використання сучасних методів захисту програмного забезпечення.

Вивчення курсу "Методи та засоби захисту програмного забезпечення" передбачає наявність систематичних та ґрунтовних знань із суміжних курсів (безпека програм та даних, дискретна математика, основи програмування і алгоритмічні мови, основи програмування, організація комп'ютерних мереж, програмування інтернет, операційні системи, якість програмного забезпечення та тестування, технологія NET), цілеспрямованої роботи над вивченням спеціальної літератури, активної роботи на лекціях, практичних та практичних заняттях, самостійної роботи та виконання індивідуальних завдань.

2.2. Завдання вивчення дисципліни

У результаті вивчення курсу "Методи та засоби захисту програмного забезпечення" студенти повинні знати:

- сучасні методи захисту ПЗ;
- модель SSDLC;
- вимоги безпеки для програмного забезпечення;
- методи та засоби обмеження доступу до програмного забезпечення;
- класифікацію вразливостей ПЗ;
- особливості вразливостей у ПЗ;
- особливості конфігурування систем безпеки.

Мета проведення лекцій полягає у тому, щоб ознайомити студентів із основними відомостями щодо аналізу та дослідження вразливостей програмного забезпечення та використання сучасних методів та засобів для захисту програмного забезпечення від потенційних загроз.

Мета проведення лекцій полягає у:

- викладенні студентам у відповідності з програмою та робочим планом основних понять щодо захисту програмного забезпечення;
- сформувати у студентів цілісну систему теоретичних знань з курсу "Методи та засоби захисту програмного забезпечення".

Мета проведення практичних занять полягає у тому, щоб виробити у студентів практичні навички розробки програмного забезпечення відповідно до моделі SSDLC.

Завдання проведення практичних занять:

- ознайомити з найбільш поширеними вразливостями програмного забезпечення відповідно до TOP 10 OWASP;
- отримати навики аналізу та дослідження вразливостей програмного забезпечення за допомогою сучасних програних засобів;
- отримати практичні навики розробки захищеного програмного забезпечення відповідно до моделі SSDLC.
- ознайомитись з сучасними методами та засобами захисту програм;
- глибше засвоїти та закріпити теоретичні знання, одержані на лекціях.

2.3. Найменування та опис компетентностей, формування котрих забезпечує вивчення дисципліни «Методи та засоби захисту програмного забезпечення».

- СК05. Здатність розробляти, аналізувати та застосовувати специфікації, стандарти, правила і рекомендації в сфері інженерії програмного забезпечення;
- СК08. Здатність розробляти і координувати процеси, етапи та ітерації життєвого циклу програмного забезпечення на основі застосування сучасних моделей, методів та технологій розроблення програмного забезпечення;
- СК09. Здатність забезпечувати якість програмного забезпечення;
- СК10. Здатність розробляти програмне забезпечення, використовуючи концепції інформаційної безпеки, безпеки баз даних, мережевої безпеки та криптографії.

2.4. Передумови для вивчення дисципліни базується на знанні таких дисциплін: «Безпека програм та даних», «Алгоритми та структури даних», «Аналіз вимог до програмного забезпечення», «Архітектура та проектування програмного забезпечення», «Засоби програмування баз даних», «Архітектура комп'ютера», «Основи програмної інженерії».

2.5. Результати навчання

У результаті вивчення курсу "Методи та засоби захисту програмного забезпечення" студенти повинні оцінювати і вибирати методи і моделі розробки, впровадження, експлуатації програмних засобів та управління ними на всіх етапах життєвого циклу.

Програмні результати навчання:

- РН01. Знати і застосовувати сучасні професійні стандарти і інші нормативно-правові документи з інженерії програмного забезпечення;
- РН07. Аналізувати, оцінювати і застосовувати на системному рівні сучасні програмні та апаратні платформи для розв'язання складних задач інженерії програмного забезпечення;
- РН08. Розробляти і модифікувати архітектуру програмного забезпечення для реалізації вимог замовника;
- РН13. Конфігурувати програмне забезпечення, керувати його змінами та розробленням програмної документації на всіх етапах життєвого циклу;
- РН18. Планувати, організовувати, впроваджувати та контролювати розробку програмного забезпечення систем захисту інформації, використовуючи концепції інформаційної безпеки, безпеки баз даних, мережевої безпеки та криптографії.

3. Програма навчальної дисципліни «МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ»

Змістовний модуль 1. Особливості захисту програмного забезпечення

Тема 1. ЗАГАЛЬНИЙ ОГЛЯД МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ ПЗ

Мета і доцільність використання систем захисту ПЗ. Класифікація систем захисту ПЗ. Основні методи захисту ПЗ. Критерії оцінювання та основні вимоги до розробки СЗПЗ.

Література: 9-15

ТЕМА 2. МОДЕЛЬ SSDLC.

Вимоги безпеки для розробки ПЗ. Особливості дизайну захищеного ПЗ. Реалізація захищеного ПЗ. Особливості тестування безпеки ПЗ. Експлуатація захищеного ПЗ.

Література: 1-6, 13,14

ТЕМА 3. НЕФУНКЦІОНАЛЬНІ ВИМОГИ БЕЗПЕКИ ДЛЯ РОЗРОБКИ ПЗ

Вимоги автентифікації. Вимоги до паролів. Вимоги до авторизації Вимоги до Cookies та Timeouts. Вимоги до сесій користувачів. Вимоги до введення \ виведення. Вимоги до логування

Література: 6, 9-12

Тема 4. ЗАХИСТ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ВІД НЕСАНКЦІОНОВАНОГО ДОСЛІДЖЕННЯ

Методи дослідження програмного коду. Засоби дослідження програмного коду. Принципи та підходи щодо захисту програмного коду від несанкціонованого дослідження.

Література: 13,14

Змістовний модуль 2. Особливості аналізу та дослідження вразливостей програмного забезпечення.

Тема 5. КЛАСИФІКАЦІЯ ВРАЗЛИВОСТЕЙ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

OWASP TOP 10. Web Application Security Consortium Threat Classification. OWASP Top 10 Mobile Risks. Common Vulnerabilities Scoring System.

Література: 2,3

Тема 6. ЗАСОБИ АУДИТУ БЕЗПЕКИ ТА АНАЛІЗУ ЗАХИЩЕНОСТІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Засоби аудиту безпеки web-додатків. Засоби виявлення вразливостей програмного забезпечення. Особливості конфігурування систем безпеки web-додатків.

Література: 2-7

4. Структура залікового кредиту дисципліни „Методи та засоби захисту програмного забезпечення”

денна форма навчання	Кількість годин				
	Лекції	Практичні роботи	Самостійна робота	Індивідуальна робота	Контрольні заходи
Змістовий модуль 1. Особливості захисту програмного забезпечення					
Тема 1. Загальний огляд методів та засобів захисту ПЗ	4	3	16	-	Усне опитування та тестування
Тема 2. Модель SSDLC	6	3	18	2	Усне опитування та тестування
Тема 3. Нефункціональні вимоги безпеки для розробки ПЗ	4	2	16	-	Усне опитування та тестування
Тема 4. Захист програмного забезпечення від несанкціонованого дослідження	4	2	16	-	Усне опитування та тестування
Змістовий модуль 2. Особливості аналізу та дослідження вразливостей програмного забезпечення.					
Тема 5. Класифікація вразливостей програмного забезпечення	6	2	16	-	Усне опитування та тестування
Тема 6. Засоби аудиту безпеки та аналізу захищеності програмного забезпечення	6	2	16	2	Усне опитування та тестування
Разом	30	14	98	4	

5. Тематика практичних занять

Практичне заняття № 1 (4 год.)

Тема: Вразливості та вектори атак на веб-застосунки відповідного до TOP 10 OWASP.

Мета: Отримати практичний досвід експлуатації вразливостей веб-застосунків у середовищі bWAPP.

Практичне заняття № 2 (6 год.)

Тема: Аналіз захищеності веб-базованого програмного забезпечення

Мета: Вивчення методів та засобів збору інформації про захист веб – ресурсів.
Практичне заняття №3 (4 год.)
Тема: Автоматичний аналіз вразливостей програмного забезпечення.
Мета: Формування вмінь і практичних навиків оцінки вразливостей ПЗ відповідно до CVSS з допомогою сканера OpenVAS.
Практичне заняття №4 (4 год.)
Тема: Формування вимог до захищеного програмного забезпечення відповідно до SSDLC.
Мета: Отримати практичний досвід формування нефункціональних вимог безпеки до програмного забезпечення.
Практичне заняття №5 (6 год.)
Тема: Розробка прототипу захищеного програмного забезпечення відповідно до SSDLC.
Мета: Розробити архітектуру програмне забезпечення відповідно до SSDLC.
Практичне заняття №6 (6 год.)
Тема: Реалізація захищеного програмного забезпечення відповідно до SSDLC.
Мета: Реалізувати програмне забезпечення відповідно до SSDLC.

6. Комплексне практичне індивідуальне завдання

Індивідуальні завдання з дисципліни «Методи та засоби захисту програмного забезпечення " виконується самостійно кожним студентом. КПІЗ охоплює усі основні теми дисципліни «Методи та засоби захисту програмного забезпечення». Метою виконання КПІЗ є оволодіння навичками застосування теоретичних. КПІЗ оформлюється у відповідності з встановленими вимогами. Виконання КПІЗ є одним із обов'язкових складових модулів залікового кредиту з дисципліни «Методи та засоби захисту програмного забезпечення».

Варіанти КПІЗ з дисципліни "Методи та засоби захисту програмного забезпечення":

1. Розробити інтернет ресурс для імітації фішингових атак та створити аналітичну систему для нього.
2. Розробити смарт-контракт на базі блокчейну Ethereum для продажу токенів.
3. Розробити смарт-контракт на базі блокчейну Bitcoin для продажу токенів.
4. Розробити програмний продукт для токенізації
5. Розробити стеганографічну систему для приховування інформації у bmp-файлах.
6. Розробити стеганографічну систему для приховування інформації у wav-файлах.
7. Провести реінженерію програмного продукту відповідно до вимог GDPR.
8. Оцінити рівень захищеності сайту розробленого із використанням технології ASP.NET розгорнутого на віртуальній машині, відповідно до TOP 10 OSWAP. Надати рекомендації щодо покращення захисту сайту.

9. Оцінити рівень захищеності сайту розробленого із використанням PHP розгорнутого на віртуальній машині, відповідно до TOP 10 OSWAP. Надати рекомендації щодо покращення захисту сайту.
10. Розробити програмний продукт для аналізу UDP трафіку.
11. Розробити програмний продукт для аналізу HTTP трафіку.
12. Розробити програмний продукт для аналізу TCP\IP трафіку.
13. Розробити програмний продукт для шифрування файлів симетричним алгоритмом
14. Розробити програмний продукт для шифрування файлів асиметричним алгоритмом
15. Розробити скрипт, який буде блокувати usb-порти комп'ютера. При вставленні usb-носія у usb-порт скрипт повинен формувати електронний лист із інформацією про залогіненого користувача, дату та час вставлення пристрою та відправлятись на електронну пошту.
16. Реалізувати алгоритм захисту ПЗ із прив'язкою до апаратного забезпечення (мінімум 2 пристрої ПК).
17. Реалізувати алгоритм захисту ПЗ із прив'язкою до флеш-носія.
18. Розробити веб-генератор надійних паролів
19. Розробити веб-ресурс для перевірки складності пароля
20. Реалізувати механізм CAPCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) у вигляді запиту відповіді на питання
21. Реалізувати механізм CAPCHA (Completely Automated Public Turing test to tell Computers and Humans Apart)у вигляді запиту відповіді на результат математичної дії
22. Розробити веб-ресурс для генерації простих чисел
23. Розробити веб-ресурс типу WhoiS
24. Розробити хеш-калькулятор відповідно до алгоритму SHA-1
25. Розробити хеш-калькулятор відповідно до алгоритму MD5

7. Самостійна робота

№ п/п	Тематика	К-сть годин (денна)
1	Тестування захищеності механізму управління сесіями	8
2	Тестування захищеності транспортного рівня	8
3	Аналіз протекторів	8
4	Пошук вразливостей до атак CSRF	8
5	Пошук вразливостей до атак XSS	8
6	Пошук вразливостей до атак RCE	8
7	Аналіз Metasploit Framework	8
8	Середовище тестування захищеності веб-додатків Burp Suite	8
9	Аналіз спеціалізованих сканерів вразливостей веб-застосунків	10
10	Особливості програмної реалізація криптографічних	8

	алгоритмів	
11	Методи безпечної реалізації ПЗ	8
12	Безпечна конфігурація БД	8
	Разом:	**98**

8. Тренінг з дисципліни

Тематика: Проведення CTF (Capture The Flag) на тематику захисту/атаки на програмного забезпечення.

Завдання та структура: У контексті на атаку/захист (Attack-Defence, атака-захист, напад-захист) кожна команда отримує власну мережу (або лише один хост) з vulnarable services. Зазвичай команди мають час для патчення своїх сервісів та розробки експлойтів. А тоді викладач з'єднує учасників змагань — і починається бойова гра! Необхідно захистити власні сервіси у точках захисту (пунктах оборони) та хакнути опонентів у точках атаки. Залежно від характеру конкретної гри команди можуть намагатися захопити прапор суперника або підсадити свій прапор на машину супротивника.

9. Критерії, форми поточного та підсумкового контролю

У навчальному процесі застосовуються: лекції, в тому числі з використанням мультимедіа проектора та інших ТЗН; практичні заняття, в у комп'ютерному класі; індивідуальні заняття; виконання КПІЗ, тренінг.

У процесі вивчення дисципліни «Методи та засоби захисту програмного забезпечення» використовуються наступні методи оцінювання навчальної роботи студентів:

- поточне тестування та опитування;
- залікове модульне тестування та опитування;
- оцінювання виконання КПІЗ;
- ректорська контрольна робота;
- тренінг;
- екзамен;
- інше.

10. Критерії, форми поточного та підсумкового контролю

Підсумковий бал (за 100-бальної шкалою) з дисципліни «Методи та засоби захисту програмного забезпечення» визначається як середньозважена величина, залежно від питомої ваги кожної складової залікового кредиту:

Заліковий модуль 1	Заліковий модуль 2 (ректорська контрольна робота)	Заліковий модуль 3 (підсумкова оцінка за КПІЗ, враховуючи поточне опитування)	Заліковий модуль 4 (письмовий екзамен)	Разом
20%	20 %	20 %	40%	100%

Модуль 1 (теми 1-3) 1. Усне опитування під час заняття (3 тем по 15 балів = 45 балів) Письмова робота = 50 балів	Модуль 2 (теми 4-6) 1. Усне опитування під час заняття (3 теми по 10 балів = 30 балів) Письмова робота = 70 балів	1. Написання та захист КПІЗ = 80 балів. 2. Виконання завдань під час тренінгу = 20 балів	1. Тестові завдання (25 тестів по 2 бали за тест) – макс. 50 балів 2. Завдання. 1 – макс. 25 балів 3. Завдання. 2 – макс. 25 балів	100

Шкала оцінювання:

За шкалою Університету	За національною шкалою	За шкалою ECTS
90-100	відмінно	A (відмінно)
85-89	добре	B (дуже добре)
75-84		C (добре)
65-74	задовільно	D (задовільно)
60-64		E (достатньо)
35-59	незадовільно	FX (незадовільно з можливістю повторного складання)
1-34		F (незадовільно з обов'язковим повторним курсом)

11. Інструменти, обладнання та програмне забезпечення, використання яких передбачає навчальна дисципліна

№	Найменування	Номер теми
1.	Електронний варіант лекцій	1-6
2.	Вихідні дані для виконання практичних занять.	1-6

РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

1. Microsoft Security Development Lifecycle (SDL) – Process Guidance https://msdn.microsoft.com/en-us/library/windows/desktop/84aed186-1d75-4366-8e61-8d258746bopq.aspx

2. OWASP Foundation. OWASP Testing Guide v4.0. URL: https://www.owasp.org/index.php/Web_Application_Penetration_Testing.

3. J. Koo, Y. Kim and S. Lee, "Security Requirements for Cloud-based C4I Security Architecture", 2019 International Conference on Platform Technology and Service (PlatCon), pp. 1-4, 2019.

4. C. Bryce, "Security governance as a service on the cloud", J Cloud Comp, vol. 8, 2019.

5. G. Levitin, L. Xing and H.Z. Huang, "Security of separated data in cloud systems with competing attack detection and data theft processes", Risk Analysis, vol. 39, no. 4, pp. 846-858, 2019.

6. K. O'Loughlin, M. Neary, E.C. Adkins and S.M. Schueller, "Reviewing the data security and privacy policies of mobile apps for depression", Internet interventions, vol. 15, pp. 110-115, 2019.

7. B Ouyang and Y. Cui, "Research on Computer Network Security Prevention in the Era of Big Data[J]", Journal of Physics: Conference Series, vol. 1648, no. 2, pp. 022011, 2020.

8. C. Wang, S. Chen, Z. Feng, Y. Jiang and X. Xue, "Block Chain-Based Data Audit and Access Control Mechanism in Service Collaboration", 2019 IEEE International Conference on Web Services, pp. 214-218, 2019.

9. Кузнецов О. О. Захист інформації в інформаційних системах : навч. посіб. Х. : ХНЕУ, 2018. – 510 с.

10. Поляков А. О., Євсеєв С. П., Огурцов В. В. Лабораторний практикум з навчальної дисципліни "Захист інформації в інформаційних системах" : навч.-практ. посіб. - Х. : ХНЕУ, 2017. – 208 с.

11. Гуз А.М., Довгань О.Д., Марущак А.І. Організація захисту інформації з обмеженим доступом. - К. : Наук.-вид. відділ НА СБ України, 2015. - 378 с.

12. Закон України “Про захист інформації в автоматизованих системах” від 05.07.1994.

13. Загальні положення щодо захисту інформації в комп’ютерних системах від несанкціонованого доступу. – НД ТЗІ 1.1-001-98, ДСТТСЗІ СБ України, Київ, 1998.

14. Класифікація автоматизованих систем і стандартні профілі захищеності оброблюваної інформації від несанкціонованого доступу. – НД ТЗІ 2.2-002-98, ДСТТСЗІ СБ України, Київ, 1998.

15. Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу. – НД ТЗІ 1.1-002-98, ДСТТСЗІ СБ України, Київ, 1998.