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.

ЗАТВЕРДЖУЮ
Директор навчально-наукового інституту новітніх освітніх технологій
_____ Святослав ПИТЕЛЬ
"___"_____2023 р.

РОБОЧА ПРОГРАМА

з дисципліни «Безпека програм та даних»

Ступінь вищої освіти: бакалавр
Галузь знань – 12 «Інформаційні технології»
Спеціальність – 121 «Інженерія програмного забезпечення»
Освітньо-професійна програма – «Інженерія програмного забезпечення»

Кафедра комп'ютерних наук

Форма навчання	Курс	Семестр	Лекції (год.)	Лабор. (год.)	ІРС (год.)	Тренінг КПІЗ (год.)	СРС (год.)	Разом (год.)	Іспит. (сем.)
Денна	4	8	48	48	6	12	36	150	8
Заочна	4	8,9	4	2	-	-	144	150	9

31.08.2023

Тернопіль – ЗУНУ
2023

Робоча програма розроблена доцентом кафедри комп'ютерних наук, к.т.н., Русланом ШЕВЧУКОМ.

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 2023р.

Голова групи
забезпечення спеціальності,
д.т.н., професор _____ Микола ДИВАК

Гарант ОП
к.т.н., доцент _____ Світлана КРЕПИЧ

СТРУКТУРА РОБОЧОЇ ПРОГРАМИ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«Безпека програм та даних»
1 Опис дисципліни «Безпека програм та даних»

Дисципліна «Безпека програм та даних»	Галузь знань, спеціальність, ступінь вищої освіти	Характеристика навчальної дисципліни
Кількість кредитів - 5	Галузь знань - 12 Інформаційні технології	Статус дисципліни: нормативна Мова навчання: українська
Кількість залікових модулів - 4	Спеціальність: 121 Інженерія програмного забезпечення	Рік підготовки: *Денна – 4,* *Заочна – 4.* Семестр: *Денна – 8* *Заочна – 8,9.*
Кількість змістових модулів – 2	Ступінь вищої освіти – бакалавр	Лекції: *Денна* – 48 год, *Заочна* – 4 год. Лабораторні заняття: *Денна* – 48 год, *Заочна* – 2 год.
Загальна кількість годин – 150		Самостійна робота: *Денна* – 36 год, тренінг – 12 год. *Заочна* – 144 год. Індивідуальна робота: *Денна* – 6 год.
Тижневих годин – 12 год., з них аудиторних – 6 год		Вид підсумкового контролю – іспит

2. Мета й завдання вивчення дисципліни «Безпека програм та даних»

2.1. Мета вивчення дисципліни

Метою дисципліни «Безпека програм та даних» є надання студентам знань щодо сучасних стандартів, підходів, методів та засобів захисту інформаційних систем. Програма та тематичний план дисципліни орієнтовані на глибоке та ґрунтовне засвоєння студентами основних понять щодо програмно-апаратного захисту інформації, ідентифікації та аутентифікації користувачів комп'ютерних систем, засобів і методів обмеження доступу до програм, методів та засобів криптографічного захисту інформації, захисту програм від несанкціонованого копіювання, захисту програмних засобів від дослідження.

Ця дисципліна відноситься до дисциплін циклу професійної та практичної підготовки. Знання основ дисципліни «Безпека програм та даних» на даний час одним із важливих показників рівня кваліфікації фахівця з програмної інженерії.

Студенти при вивченні дисципліни повинні сформуватись вміння класифікувати, ідентифікувати і захищати засоби обробки інформації від несанкціонованого доступу та комп'ютерних вірусів, захищати інформацію

персонального комп’ютера та розроблене програмне забезпечення, розробляти індивідуальні системи управління доступом і захистом інформації.

Вивчення курсу "Безпека програм та даних" вимагає цілеспрямованої роботи над вивченням спеціальної літератури, активної роботи на лекціях та практичних заняттях, самостійної роботи та виконання індивідуальних завдань.

2.2. Завдання вивчення дисципліни

У результаті вивчення курсу "Безпека програм та даних" студенти повинні знати:

- загальні відомості про захист програм та даних;
- стандарти галузі інформаційної безпеки;
- алгоритми ідентифікації та аутентифікації користувачів;
- алгоритми криптографічного захисту інформації;
- методи та засоби обмеження доступу до програм та даних
- класифікацію загроз інформації та міри протидії;
- класифікацію та особливості комп’ютерних вірусів;
- особливості захисту програм від досліджень;

Мета проведення лекцій полягає у тому, щоб ознайомити студентів із основними відомостями щодо захисту інформації, потенційних загроз та проблем захисту програм та даних.

Мета проведення лекцій полягає у:

- викладенні студентам у відповідності з програмою та робочим планом основних понять захисту програм та даних;
- сформувати у студентів цілісну систему теоретичних знань з курсу "Безпека програм та даних".

Мета проведення практичних занять полягає у тому, щоб виробити у студентів практичні навички захисту програм та даних від різного роду загроз.

Завдання проведення практичних занять:

- ознайомити з методами захисту програм та даних;
- ознайомитись з сучасними засобами захисту програм та даних;
- отримання навиків програмуванні систем комплексного захисту інформації;
- глибше засвоїти та закріпити теоретичні знання, одержані на лекціях.

2.3 Найменування та опис компетентностей, формування котрих забезпечує вивчення дисципліни.

Здатність аналізувати, вибирати і застосовувати методи і засоби для забезпечення інформаційної безпеки (в тому числі кібербезпеки).

2.4. Передумови для вивчення дисципліни.

Дисципліни, які повинні бути вивчені попередньо:

- Якість програмного забезпечення та тестування;
- Аналіз вимог до програмного забезпечення;
- Основи інженерії програмного забезпечення.

2.5. Результати навчання

У результаті вивчення курсу "Безпека програм та даних" студенти повинні:

- Знати, аналізувати, вибирати, кваліфіковано застосовувати засоби забезпечення інформаційної безпеки (в тому числі кібербезпеки) і цілісності даних відповідно до розв'язуваних прикладних завдань та створюваних програмних систем.

3 Програма навчальної дисципліни «Безпека програм та даних»

Змістовний модуль 1. Принципи безпеки та захисту інформації в ПЗ.

Тема 1. ОСНОВНІ ПОНЯТТЯ БЕЗПЕКИ ПРОГРАМ ТА ДАНИХ

Предмет і задачі захисту програм і даних. Вразливість компютерних систем. Політика безпеки в комп'ютерних системах. Оцінка та механізми захисту програм та даних. Стандарти захисту даних.

Література: 1-5, 7-10

Тема 2. ІДЕНТИФІКАЦІЯ ТА АУТЕНИТИФІКАЦІЯ КОРИСТУВАЧІВ

Ідентифікація користувачів. Аутентифікація користувачів. Перевірка автентичності користувачів. Протоколи ідентифікації.

Література: 1,2,4

ТЕМА 3. МОДЕЛІ РОЗПОВСЮДЖЕННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Моделі безоштовного ПЗ. Моделі умовно-безоштовного ПЗ. Моделі комерційного ПЗ. Хмарні моделі.

Тема 4. КРИПТОГРАФІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ

Основні поняття та визначання криптографічного захисту інформації. Симетричне та асиметричне шифрування. Цифрові підписи. Хеш-функції. Цифрові сертифікати. Технологія Blockchain.

Література: 1,4,7,9

Змістовний модуль 2. Основи побудови систем захисту інформації в ПЗ.

Тема 5. МЕТОДИ ТА ЗАСОБИ ОБМЕЖЕННЯ ДОСТУПУ ДО ПРОГРАМ ТА ДАНИХ

Вразливість комп'ютерних систем. Способи проникнення до комп'ютерних систем. Спостереження за користувачами КС. Особливості обмеження доступу до програм та даних.

Література: 1,4

Тема 6. ЗАХИСТ ПРОГРАМ ВІД НЕСАНКЦІОНОВАНОГО ДОСЛІДЖЕННЯ

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

Література: 1,4,8

Тема 7. ВІРТУАЛЬНІ ПРИВАТНІ МЕРЕЖІ

Поняття про віртуальні захищені (приватні) мережі (VPN). Види віртуальних приватних мереж. Сервіси VPN. Способи утворення захищених тунелів. Рівні реалізації VPN. Протоколи: SSL, SOCKS, IPSec, PPTP, L2F, L2TF

Література: 1,4

4. Структура залікового кредиту дисципліни „Безпека програм та даних”

денна форма навчання	Кількість годин					
	Лекції	Лабораторна робота	СРС	ІРС	Тренінг КПІЗ	Контрольні заходи
Змістовий модуль 1. Принципи безпеки та захисту інформації в ПЗ.						
Тема 1. Основні поняття безпеки програм та даних	6	6	6	3	6	Усне опитування/ тестування
Тема 2. Ідентифікація та аутентифікація користувачів	8	8	6			Усне опитування/ тестування
Тема 3. Моделі розповсюдження програмного забезпечення	6	6	6			Усне опитування/ тестування
Тема 4. Криптографічний захист інформації	10	10	6			Усне опитування/ тестування
Змістовий модуль 2. Основи побудови систем захисту інформації в ПЗ.						
Тема 5. Методи та засоби обмеження доступу до програм та даних	6	6	4	3	6	Усне опитування/ тестування
Тема 6. Захист програм та даних від несанкціонованого копіювання	6	6	4			Усне опитування/ тестування
Тема 7. Віртуальні приватні мережі	6	6	4			Усне опитування/ тестування
Разом	**48**	**48**	**36**	**6**	**12**	

заочна форма навчання	Кількість годин		
	Лекції	Лабораторна робота	Самостійна робота
Тема 1. Основні поняття безпеки програм та даних	1	1	20
Тема 2. Ідентифікація та аутентифікація користувачів			22
Тема 3. Моделі розповсюдження програмного забезпечення	1		20
Тема 4. Криптографічний захист інформації			20
Тема 5. Методи та засоби обмеження доступу до програм та даних	1	1	22
Тема 6. Захист програм та даних від несанкціонованого копіювання	1		20
Тема 7. Віртуальні приватні мережі			20
Разом	**4**	**2**	**144**

5. Тематика лабораторних робіт

Лабораторна робота №1 (6 год.)

Тема: Розмежування повноважень користувачів на основі парольної аутентифікації
Мета: Розробка програми розмежування повноважень користувачів на основі парольного аутентифікації.
Лабораторна робота №2 (8 год.)
Тема: Логування дій користувачів у програмних системах.
Мета: Засвоїти методику та отримати практичні навики розробки процедур логування дій користувачів на прикладі підсистем ідентифікації та аутентифікації користувачів із важкооборотними однонапрямленими хеш-функціями.
Лабораторна робота №3 (8 год.)
Тема: Методи захисту програмного забезпечення.
Мета: Одержати практичні навики реалізації алгоритмів захисту програмного забезпечення для найпоширеніших моделей розповсюдження.
Лабораторна робота №4 (10 год.)
Тема: Захист веб-ресурсів від ботів та спаму за допомогою механізму CAPTCHA.
Мета: отримати практичні навики реалізації механізму CAPTCHA.
Лабораторна робота №5 (8 год.)
Тема: Аналіз захищеності веб-ресурсів
Мета: Отримати практичні навики аналізу захищеності веб-ресурсів, формування аналітичного звіту та рекомендацій щодо усунення виявлених вразливостей..
Лабораторна робота №6 (8 год.)
Тема: Особливості захисту даних за допомогою технології Blockchain
Мета: Формування вмінь і навиків реалізації Blockchain.

6. Комплексне практичне індивідуальне завдання

Індивідуальні завдання з дисципліни «Безпека програм та даних" виконується самостійно кожним студентом. КПІЗ охоплює усі основні теми дисципліни «Безпека програм та даних». 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 «Безпека програм та даних».

Варіанти КПІЗ з дисципліни "Безпека програм та даних":

1. Провести критичний аналіз систем резервного копіювання та відновлення даних (не менше 5 рішень). Надати рекомендації щодо особливостей резервного копіювання та відновлення даних.
2. Провести критичний аналіз засобів створення смарт-контрактів на базі блокчейну Ethereum, NXT, Bitcoin.
3. Розробити Incident Response Plan для реагування на програми – вимагачі (Ransomware)
4. Розробити Investigation Report на фішингову атаку типу нігерійські листи.
5. Розробити політику конфіденційності IT-компанії відповідно до вимог GDPR
6. Розробити положення про обробку персональних даних користувачів відповідно до вимог GDPR для будь-якого веб-сайту.
7. Провести функціональний аналіз хмарних ресурсів (не менше 5 рішень) для забезпечення безпеки даних у відповідності до GDPR.

8. Провести функціональний аналіз DLP – систем (Data Loss Prevention) (не менше 5 рішень).
9. Провести функціональний аналіз SIEM - систем (Security information and event management) (не менше 5 рішень).
10. Провести функціональний аналіз IDS - систем (Intrusion Detection System). (не менше 5 рішень).
11. Провести функціональний аналіз IDM – систем (Identity Management System). (не менше 5 рішень).
12. Провести функціональний аналіз інструментів для penetration test.
13. Провести критичний аналіз фаєрволів для ОС Android та iOS. Сформувати рекомендації для користувачів.
14. Провести критичний аналіз фаєрволів для ОС Windows. Сформувати рекомендації для користувачів.
15. Провести критичний аналіз антивірусів для ОС Android та iOS. Сформувати рекомендації для користувачів.
16. Провести критичний аналіз антивірусів для ОС Windows. Сформувати рекомендації для користувачів.
17. Розробити рекомендації для IT-компанії щодо використання wi-fi (корпоративний, гостьовий доступ) з точки зору безпеки даних.
18. Проаналізувати переваги створення DMZ (demilitarized zone) для IT-компанії з точки зору безпеки даних.
19. Розробити рекомендації щодо впровадження VLAN (Virtual Local Area Network) для IT-компанії
20. Розробити рекомендації щодо використання реєстру Windows фахівцями з інформаційої безпеки.
21. Провести критичний аналіз VPN- клієнтів для платформи Android (не менше 3 рішень). Сформувати рекомендації для користувачів

Індивідуальне завдання оцінюється за 100-бальною шкалою. Виконання індивідуального завдання є одним із обов'язкових складових модулів залікового кредиту з дисципліни «Безпека програм та даних».

7. Самостійна робота

1. Провести критичний аналіз VPN - сервісів для платформи Windows (не менше 3 рішень). Сформувати рекомендації для користувачів.
2. Провести критичний аналіз засобів дешифрування результатів роботи програм-вимагачів (не менше 3 рішень). Сформувати рекомендації для користувачів.
3. Розробити рекомендації для користувачів, що заразились adware.
4. Розробити рекомендації для користувачів що заразились троянськими вірусами.
5. Розробити рекомендації для запобігання телефонному та email – фішингу.
6. Розробити рекомендації для користувачів для безпечної роботи в мережі Інтернет.
7. Розробити рекомендації для користувачів для безпечного користування мобільними телефонами.
8. Безпека систем, що використовують NCSA HTTPD і Apache HTTPD
9. Безпека систем, що використовують скріпти в CGI-BIN
10. Класифікація систем виявлення мережевих атак

11. Класифікація систем контролю цілісності
12. Аналіз проблем безпеки Інтернету – речей
13. Аналіз проблем безпеки кіберфізичних систем
14. Аналіз проблем безпеки в хмарі
15. Аналіз проблем безпеки в NFC
16. Аналіз атак на Microsoft AD.
17. Аналіз задач SOC центру (Security operation center)
18. TOP-10 фінансових втрат українських підприємств від зловмисних атак за 2019 рік.
19. Актуальні тренди кібербезпеки 2022
20. Аналіз засобів захисту кінцевих терміналів
21. Сервіси і механізми захисту
22. Принципи побудови блочних шифрів та криптосистем з відкритим ключем
23. Сучасні алгоритми симетричного та асиметричного шифрування
24. Сучасні алгоритми хешування
25. Основні методи безпечного написання коду програм
26. Методи і засоби аналізу безпеки програмних засобів
27. Використовувати функції Microsoft CryptoAPI для розробки прикладного ПЗ
28. Оцінка та аналіз безпеки ПЗ
29. Протоколи автентифікації
30. Програмна реалізація криптографічних алгоритмів

8. Тренінг з дисципліни

Тематика тренінгу: Захист інформаційних систем від несанкціонованого копіювання

Завдання та структура тренінгу:

1. На базі розробленого програмного забезпечення на практичних заняттях, реалізувати метод захисту від несанкціонованого копіювання відповідно до варіанту, поданого нижче.
2. Варіанти завдання

№	Тип ПП	Обмеження	Шифр ключа
1	Demoware	Розмір файлів для відкриття не більший 100 КБ	Цезаря
2	Demoware	Відкриття файлів тільки формату BMP	Віженера
3	Demoware	Відкриття файлів тільки текстових форматів	Цезаря
4	Demoware	Відсутня функція збереження файлів	Віженера
5	Demoware	Файли відкриваються тільки з однієї директорії	Віженера
6	Demoware	Недоступна функція друку	Цезаря
7	Demoware	Недоступна функція перегляду параметрів файлу	Цезаря
8	Trialware	Блокування виконання програми після 30 днів після її встановлення	Віженера

9	Trialware	Блокування виконання програми після 10 запусків після її встановлення	Цезаря
10	Trialware	Блокування виконання програми після її відкриття 10 раз	Віженера
11	Trialware	Блокування виконання програми після 30 днів після її встановлення або 20 запусків	Віженера
12	Trialware	Блокування функцій програми після 10 днів після її встановлення	Цезаря
13	Trialware	Блокування функцій програми в останній день поточного року	Цезаря
14	Trialware	Блокування функцій програми в кінці поточно місяця	Віженера
15	Nagware	Діалогове вікно нагадування про реєстрацію програми через кожні 5 хвилин роботи з нею	Цезаря
16	Nagware	Діалогове вікно нагадування про реєстрацію програми після кожного запуску програми	Віженера
17	Nagware	Діалогове вікно нагадування про реєстрацію програми після кожного завершення програми	Віженера

9. Методи оцінювання

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

У процесі вивчення дисципліни «Безпека програм та даних» використовуються наступні методи оцінювання навчальної роботи студентів:

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

10. Критерії, форми поточного та підсумкового контролю

Підсумковий бал (за 100-бальної шкалою) з дисципліни «Безпека програм та даних» визначається як середньозважена величина, залежно від питомої ваги кожної складової залікового кредиту

Заліковий модуль 1	Заліковий модуль 2 (РКР)	Заліковий модуль 3 (КПІЗ)	Заліковий модуль 4 (іспит)	Разом
20%	20 %	20 %	40%	100%
Виконання лабораторних робіт (3 роботи по 20 балів – 60 балів) Написання модульної роботи –	Виконання лабораторних робіт (3 роботи по 10 балів – 30 балів) Написання ректорської	Написання та захист КПІЗ – 80 балів Виконання завдань під час тренінгу – 20	Тестові завдання (10 питань по 5 балів – 50 балів) Завдання по теорії (2 завдання по 10 балів – 20 балів)	100

40 балів	контрольної роботи – 70 балів	балів	Практичне завдання (два завдання по 15 балів)	

За шкалою ЗУНУ	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.	Мультимедійний проектор	1-7
2.	Проекційний екран	1-7
3.	Комунікаційне програмне забезпечення (Internet Explorer, Google Chrome, Firefox)	1-7
4.	Операційна система Windows, наявність доступу до мережі Internet	1-7
5.	Персональні комп’ютери	1-7
6.	Комунікаційне програмне забезпечення (Zoom) для проведення занять у режимі онлайн (за необхідності)	1-7
7.	Комунікаційна навчальна платформа (Moodle) для організації дистанційного навчання (за необхідності)	1-7
8.	Базове програмне забезпечення Microsoft Office	1-7
9.	Спеціалізоване програмне забезпечення: - Visual Studio	1-7

РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

1. Wenliang Du. Computer Security: A Hands-on Approach, 2022. – 543 p.
2. Luo, F.; Zhang, X.; Yang, Z.; Jiang, Y.; Wang, J.; Wu, M.; Feng, W. Cybersecurity Testing for Automotive Domain: A Survey. *Sensors* 2022, *22*, 9211. https://doi.org/10.3390/s22239211
3. Duane C. Wilson. Cybersecurity, MIT Press, 2021. - 161 p.
4. Joseph Steinberg. Cybersecurity For Dummies, John Wiley & Sons 2022. – 416 p
5. Kutub Thakur, Al-Sakib Khan Pathan. Cybersecurity Fundamentals: A Real-World Perspective, CRC Press, 2020. - 304 p
6. Quinn Kiser. Computer Networking and Cybersecurity: A Guide to Understanding

Communications Systems, Internet Connections, and Network Security Along with Protection from Hacking and Cyber Security Threats, Independently Published, 2020. – 240 p.

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

8. Поляков А. О., Євсеєв С. П., Огурцов В. В. Лабораторний практикум з навчальної дисципліни "Захист інформації в інформаційних системах" : навч.-практ. посіб. - Х. : ХНЕУ, 2018. – 208 с.

9. Терейковський, І. А. Інтелектуалізовані методи захисту інформації: нейронні мережі в захисті інформації [Електронний ресурс] : навчальний посібник для здобувачів ступеня бакалавр за освітньою програмою «Системне програмування та спеціалізовані комп'ютерні системи» спеціальності 123 Комп'ютерна інженерія / І. А. Терейковський, А. О. Корченко ; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 3,16 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2022. – 176 с. – Назва з екрана.

10. Згуровський М. Проблеми інформаційної безпеки в Україні, шляхи їх вирішення // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – Київ. – 2018. – С. 10 – 14.