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

ЗАТВЕРДЖУЮ

В.о. декана ФКІТ
Ігор ЯКИМЕНКО

«____» 2023 р.

ЗАТВЕРДЖУЮ

В.о. проректора з науково-педагогічної роботи
Віктор ОСТРОВЕРХОВ

«____» 2023 р.

РОБОЧА ПРОГРАМА

з дисципліни «Системи та технології кібербезпеки»
ступінь вищої освіти – бакалавр
галузь знань – 12 Інформаційні технології
спеціальність – 125 Кібербезпека
освітньо-професійна програма – Кібербезпека

Кафедра спеціалізованих комп'ютерних систем

Форма навчання	Курс	Семестр	Лекції (год.)	Практ. (год.)	ІРС (год.)	Тренінг, КПІЗ (год.)	Самост. робота студ. (год.)	Разом (год.)	Залік (сем.)
Денна	4	7	26	12	2	12	98	150	7

31.08.2023

Тернопіль – 2023

Робочу програму склала доцент кафедри спеціалізованих комп'ютерних систем, к.т.н., доцент Наталія ЯЦКІВ

Робоча програма затверджена на засіданні кафедри спеціалізованих комп'ютерних систем, протокол
№ 1 від 28.08.2023 р.

Завідувач кафедри
спеціалізованих комп'ютерних систем Андрій СЕГІН

Розглянуто та схвалено групою забезпечення спеціальності Кібербезпека та захист інформації, протокол №1 від 30.08.2023 р.

Голова групи
забезпечення спеціальності Василь ЯЦКІВ

Гарант ОП Ігор ЯКИМЕНКО

СТРУКТУРА РОБОЧОЇ ПРОГРАМИ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Опис дисципліни «Системи та технології кібербезпеки»

Дисципліна «Системи та технології кібербезпеки»	**Галузь знань, спеціальність, СВО**	**Характеристика навчальної дисципліни**
Кількість кредитів – 5	Галузь знань – 12 Інформаційні технології	**Статус дисципліни** вибіркова **Мова навчання** українська
Кількість залікових модулів – 3	спеціальність – 125 Кібербезпека	Рік підготовки: *Денна – 4* Семестр: *Денна – 7*
Кількість змістових модулів – 2	Ступінь вищої освіти – бакалавр	Лекції: *Денна – 26* Практичні заняття: *Денна – 12*
Загальна кількість годин – 150		Самостійна робота: *Денна – 98* Індивідуальна робота : *Денна – 2*
Тижневих годин – 11, з них аудиторних – 3		Вид підсумкового контролю – залік

2. Мета і завдання дисципліни «Системи та технології кібербезпеки»

2.1. Мета вивчення дисципліни.

Метою дисципліни «**Системи та технології кібербезпеки**» є - отримання знань та умінь, які необхідні для розробки та використання систем виявлення та запобігання вторгнень.

2.2. Завдання вивчення дисципліни

Основне завдання дисципліни дати студентам теоретичну та практичну підготовку з розгортання та використання систем та технологій кібербезпеки.

2.3. В результаті вивчення дисципліни студент повинен знати:

− структуру та функції центру моніторингу та управління безпекою;
− методи захисту і аналізу кінцевих пристроїв;
− поверхні вразливі до атак;
− системи управління безпекою;
− базу вразливостей CVE;
− джерела даних про безпеку;
− методи шифрування, інкапсуляція і тунеллювання.

2.4. В результаті вивчення дисципліни студент повинен уміти:

– забезпечувати впровадження та дотримання політики кіберзахисту в ІТС, процедур, і правил;

– приймати участь у розробці планів відновлення, неперервності процесів організації для забезпечення здатності організації продовжувати виконувати необхідну діяльність в період порушення ІТ;

–виконувати конфігурування систем виявлення вторгнень та використовувати компоненти захисту для забезпечення необхідного рівня захищеності ІТС;

– виконувати аналіз зловмисного програмного коду.

– впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти кібербезпеки.

3. Програма навчальної дисципліни: «Системи та технології кібербезпеки»

Змістовий модуль 1. **Криптографії в реальному світі.**

Тема 1. Криптографії в реальному світі.

1. Принцип Керкгофа: тільки ключ зберігається в таємниці
2. Симетрична та асиметрична криптографія
3. Дві цілі: конфіденційність і автентифікація

Література: 1, 2, 4.

Тема 2. Хеш-функції

1. Властивості безпеки хеш-функції
2. Стандартизовані хеш-функції
3. SHAKE і cSHAKE, дві розширювані функції виводу (XOF)
4. Хешування паролів

Література: 1, 2, 3.

Тема 3. Коди автентифікації повідомлень

1. Властивості безпеки коду автентифікації повідомлення
2. Коди автентифікації повідомлень на практиці
3. HMAC, код автентифікації повідомлення на основі хешу

Література: 1, 2, 6.

Тема 4. Автентифіковане шифрування

1. Алгоритм шифрування AES-CBC-HMAC
2. Автентифіковане шифрування з пов’язаними даними (AEAD)
3. Chacha20-Poly1305

Література: 1, 2, 5, 7.

Тема 5. Обмін ключами

1. Стандарти обміну ключами
2. Стандарти Діффі-Хеллмана
3. Еліптична крива Діффі-Хеллмана (ECDH)

Література: 1, 2, 5, 8

Тема 6. Асиметричне шифрування та гібридне шифрування

1. Стандарти асиметричного та гібридного шифрування
2. Асиметричне шифрування за допомогою RSA-OAEP
3. Гібридне шифрування з ECIES

Література: 1, 2, 7, 9

Змістовий модуль 2. **Криптографія в децентралізованих системах**

Тема 7. Підписи та докази з нульовим знанням

1. Докази з нульовим знанням
2. Підписи RSA
3. Алгоритм цифрового підпису кривої Едвардса (EdDSA)

Література: 1, 2, 10.

Тема 8. Захищені комунікації
1. Як працює TLS
2. Стан зашифрованого Інтернету сьогодні
3. Структура протоколу Noise: сучасна альтернатива TLS
Література: 1, 4, 10.

Тема9. Наскрізне шифрування.
1. Масштабування довіри між користувачами за допомогою мережі довіри
2. Безпечний обмін повідомленнями, сучасний погляд на наскрізне шифрування з Signal
3. Стан наскрізного шифрування
Література: 1, 3, 10.

Тема 10. Аутентифікація користувача
1. Заміна паролів асиметричними ключами
2. Спільні ключі
3. Симетричний обмін ключами з автентифікацією пароля з CPace
Література: 1, 2, 5.

Тема 11. Криптографія в децентралізованих системах
1. Проблема стійкості та довіри
2. Проблема цензури - мережі без дозволу
3. LibraBFT: візантійський відмовостійкий консенсусний протокол
Література: 1, 7, 8, 12.

Тема 12. Апаратна криптографія
1. Модель сучасного криптографічного зловмисника
2. Модулі надійної платформи (TPM): корисна стандартизація захищених елементів
3. Сучасні інтегровані рішення: довірене середовище виконання (TEE)
Література: 1, 2, 10.

Тема 13. Постквантова криптографія
1. Постквантова криптографія, захист від квантових комп'ютерів
2. Підписи на основі хешування: не потрібно нічого, крім хеш-функції
3. Коротші ключі та підписи з криптографією на основі решітки
4. Kyber, обмін ключами на основі решітки
5. Dilithium, схема підпису на основі решітки
Література: 1, 7, 8, 12.

4. Структура залікового кредиту
з дисципліни "Системи та технології кібербезпеки" (денна форма навчання)

	Кількість годин					
	Лекції	Практичні заняття	СРС	ІРС	Тренінг, КПІЗ	Контрольні заходи
Змістовий модуль 1. Криптографії в реальному світ						
Тема 1. Криптографії в реальному світі	2		6		6	Опитування під час заняття, оцінювання практ. занять
Тема 2. Хеш-функції	2	1	6			
Тема 3. Коди автентифікації повідомлень	2	1	6	1		
Тема 4. Автентифіковане шифрування	2	1	8			
Тема 5. Обмін ключами	2	1	8			
Тема 6. Асиметричне шифрування та гібридне шифрування	2	1	8			
Змістовий модуль 2. Криптографія в децентралізованих системах						
Тема 7. Підписи та докази з нульовим знанням.	2	1	8		6	Опитування під час заняття, оцінювання практ. занять
Тема 8. Захищені комунікації	2	1	8			
Тема 9. Наскрізне шифрування	2	1	8			
Тема 10. Аутентифікація користувача	2	1	8	1		
Тема 11. Криптографія в децентралізованих системах	2	1	8			
Тема 12. Криптографія на основі коду	2	1	8			
Тема 13. Апаратна криптографія	2	1	8			
Разом	**26**	**12**	**98**	**2**	**12**	

5. Тематика практичних (семінарських або <u>лабораторних</u>) занять

Лабораторна робота №1

Тема: Використання утиліти Nmap.

Мета: Вивчення Nmap.

Питання для обговорення:

1. Утиліта Nmap.
2. Перевірка на наявність відкритих портів.

Література: 1, 2.

Лабораторна робота №2

Тема: Спостереження за процесом тристороннього квитування протоколу TCP за допомогою програми Wireshark.

Мета: Вивчення тристороннього квитування протоколу TCP за допомогою програми Wireshark.

Питання для обговорення:

1. Підготовка хостів для перехоплення трафіку
2. Аналіз пакетів за допомогою програми Wireshark
3. Перегляд пакетів за допомогою програми tcpdum

Література: 1, 2

Лабораторна робота №3

Тема: Шифрування і розшифрування даних з допомогою OpenSSL

Мета: Вивчення алгоритмів шифрування і розшифрування даних з допомогою OpenSSL.

Питання для обговорення:
1. Шифрування повідомлень за допомогою OpenSS
2. Розшифрування повідомлень за допомогою OpenSS
Література: 1, 2.

Лабораторна робота №4
Тема: Шифрування і розшифрування даних з допомогою хакерських інструментів
Мета: Вивчення хакерських інструментів шифрування і розшифрування даних
Питання для обговорення:
1. Створення та шифрування файлів
2. Відновлення паролів зашифрованого ZIP-файл
Література: 1, 2

Лабораторна робота №5
Тема: Ведення журналу мережевої активності з використанням середовища Packet Tracer.
Мета: Вивчення процедур ведення журналу мережевої активності.
Питання для обговорення:
1. Створення трафіку FTP. Вивчення трафіку FTP
3. Перегляд повідомлень системного журналу
Література: 1, 2.

Лабораторна робота №6
Тема: Сховища центрів сертифікації
Мета: Вивчення принципів роботи сховищ центрів сертифікації
Питання для обговорення:
1. Сертифікати, яким довіряє ваш браузер
2. Виявлення атаки через посередника
Література: 1, 2.

6. Комплексне практичне індивідуальне завдання
Варіанти КПІЗ з дисципліни «**Системи та технології кібербезпеки**»
Розробка системи виявлення та запобігання вторгнень.
1.1 Постановка задачі.
1.2 Збір інформації та пошук цілей.
1.3 Визначення структури системи
1.4 Розробка правил
1.5 Дослідження роботи системи.
1.6 Висновки.

7. Самостійна робота та дуальна освіта

№ п/п	Тематика
1	Елементи центру моніторингу та управління безпекою. SOC
2	Технології в SOC
3	Корпоративний SOC і послуги з управління інформаційною безпекою
4	Безпека кінцевих пристроїв.
5	Захист від шкідливого ПЗ на рівні хоста.
6	Захист від шкідливого ПЗ на рівні мережі.
7	Рішення для захисту від складного шкідливого програмного забезпечення Cisco AMP.
8	Міжмережеві екрани на рівні хоста.
9	Виявлення аномалій мережі
10	Перевірка мережі на уразливості
11	Загальна система оцінки вразливостей (Common Vulnerability Scoring System, CVSS).
12	База вразливостей CVE.
13	Стандарт безпеки даних індустрії платіжних карт (PCI DSS).
14	Управління ризиками.
15	Контроль вразливостей
16	Моніторинг безпеки
17	Протоколи HTTP, HTTPS, ICMP
18	Протоколи електронної пошти
19	Технології перетворення мережевих адрес (NAT) і перетворення адрес портів (PAT)
20	Реагування на інциденти і їх обробка
21	Структура правила Snort.
22	Робота в Sguil. Запити в Sguil.
23	Обробка подій в Sguil.
24	Реагування на інциденти і їх обробка
25	Життєвий цикл реагування на інциденти NIST.
26	Етапи виявлення та аналізу інцидентів.

8. 8. Організація та проведення тренінгу з дисципліни з дисципліни «Системи та технології кібербезпеки»

№ п/п	Вид роботи	Порядок проведення тренінгу
1	Аналіз трафіку з Snort	Використання Snort для аналізу трасування мережі за допомогою автономної системи фільтрації. Для цього необхідно запустити Snort з файлом правил і трасуванням: snort -c 1.rules -l log -r newtrace.pcap Потім переглянути у фільтрі журналу файл журналу та alert.ids.
2	Використання аналізу Snort.	Вилучіть свої артефакти в трасуванні HTTP за допомогою: File-> Export Objects -> HTTP
3	Використання аналізу Snort.	Використовуйте файли PCAP виявіть активність: 1) виявити неправильний вхід на FTP; 2) визначити вхід через Telnet; 3) виявлення сканування портів; 4) виявлення SYN flood; 5) виявлення FIN flood; 6) виявлення вкладених файлів; 7) визначати адреси електронної пошти.

9. Засоби оцінювання та методи демонстрування результатів навчання

У процесі вивчення дисципліни «Системи та технології кібербезпеки» використовуються наступні засоби оцінювання та методи демонстрування результатів навчання:

– поточне опитування;
– залікове модульне тестування та опитування;
– оцінювання виконання лабораторних робіт;
– оцінювання результатів КПІЗ;
– ректорська контрольна робота.

10. Критерії, форми поточного та підсумкового контролю

Підсумковий бал (за 100-бальною шкалою) з дисципліни «Системи та технології кібербезпеки» визначається як середньозважена величина, залежно від питомої ваги кожної складової залікового кредиту:

Для заліку

Заліковий модуль 1	Заліковий модуль 2	Заліковий модуль 3
30 %	40 %	30 %
1. Усне опитування на заняттях – max 7*3=21 бали. 2. Письмова робота – max 55 балів. 3. Практичне завдання – max 3*8=24 балів	1. Усне опитування на заняттях – max 5*4=20 балів. 2. Письмова робота – max 56 балів. 3. Практичне завдання – max 3*8=24 бали	1. Підготовка КПІЗ – max 30 балів. 2. Захист КПІЗ – max 40 балів. 3. Оцінка за тренінг – max 30 балів

Шкала оцінювання:

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 - 12
2.	Комп'ютерна лабораторія. Доступ до Інтернету.	1 - 12
3.	Віртуальна машина CyberOps	1 - 12

РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

1. Курс мережевої академії Cisco: CCNA Cybersecurity Operations. 2020. Режим доступу. https://www.netacad.com/courses/security/ccna-cybersecurity-operations
2. Інформаційна безпека. // Яковенко Є., Журавель І., Горбатий І., Бондарєв А. Видавництво Львівська політехніка, 2019. – 580.
3. Anu, Vaibhav. Information security governance metrics: A survey and taxonomy. Information Security Journal: A Global Perspective31. 4, 2022. – pp. 466-478.
4. Hamdani, Syed Wasif Abbas, et al. "Cybersecurity Standards in the Context of Operating System: Practical Aspects, Analysis, and Comparisons." *ACM Computing Surveys (CSUR)* 54.3, 2021. – pp.1-36
5. Santos, Henrique MD. Cybersecurity: A Practical Engineering Approach. CRC Press, 2022. – 341 p.
6. Grubb S. How Cybersecurity Really Works. 2021. – 219 p.
7. Grimes, Roger A. *Hacking Multifactor Authentication*. John Wiley & Sons, 2020.
8. Maurushat, Alana. *Ethical hacking*. University of Ottawa Press, 2019.
9. Cisar, P., & Pinter, R. Some ethical hacking possibilities in Kali Linux environment. *Journal of Applied Technical and Educational Sciences*, *9*(4), 2019, pp.129-149.
10. Stallings, W. Effective Cybersecurity: Understanding and Using Standards and Best Practices. Addison-Wesley. 2019. – 893 p.
11. Warsinske, J., Graff, M., Henry, K., Hoover, C., Malisow, B., Murphy, S., & Vasquez, M. The Official (ISC) 2 Guide to the CISSP CBK Reference. John Wiley & Sons. 2019. – 928 c.