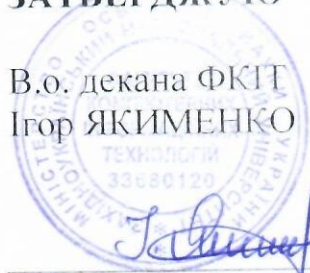


МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

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 «Основи кібербезпеки»
ступінь вищої освіти – бакалавр
галузь знань – 12 Інформаційні технології
спеціальність – 125 Кібербезпека та захист інформації
освітньо-професійна програма – Кібербезпека

Кафедра кібербезпеки

Форма навчання	Курс	Семестр	Лекції (год.)	Лабор. роботи (год.)	ІРС (год.)	Тренінг, КПЗ (год.)	Самост. робота студ. (год.)	Разом (год.)	Екз. (сем.)
Денна	1	1	45	60	6	14	85	210	1

11.01.2023 р.

Тернопіль – 2023

Робоча програма розроблена на основі освітньо-професійної програми підготовки бакалавра галузі знань 12 «Інформаційні технології» спеціальності 125 «Кібербезпека та захист інформації», затвердженої Вченою радою ЗУНУ (протокол № 10 від 23.06.2023 р.).

Робочу програму склав завідувач кафедри кібербезпеки, д.т.н., професор Василь Яцків

Робоча програма затверджена на засіданні кафедри кібербезпеки, протокол № 1 від 28.08.2023 р.

Завідувач кафедри



Василь ЯЦКІВ

Розглянуто та схвалено групою забезпечення спеціальності 125 «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

1. Опис дисципліни «Основи кібербезпеки»

Дисципліна «Основи кібербезпеки»	Галузь знань, спеціальність, СВО	Характеристика навчальної дисципліни
Кількість кредитів ECTS – 7	Галузь знань 12 Інформаційні технології	Статус дисципліни: обов'язкова Мова навчання: українська
Кількість залікових модулів – 4	Спеціальність 125 «Кібербезпека та захист інформації»	Рік підготовки: Денна – 1 Семестр: Денна – 1
Кількість змістових модулів – 2	Ступінь вищої освіти – бакалавр	Лекції (год.): 45 Практичні заняття (год.): 60
Загальна кількість годин – 210		Самостійна робота (год.): 85 Тренінг, КППЗ (год.): 14 Індивідуальна робота (год.): 6
Тижневих годин – 14, з них аудиторних – 7		Вид підсумкового контролю – екзамен

2. Мета і завдання дисципліни «Основи кібербезпеки»

2.1. Мета вивчення дисципліни.

Метою дисципліни «Основи кібербезпеки» є формування у студентів цілісного уявлення про спеціальність кібербезпека та базових знань в даній галузі.

2.2. Завдання вивчення дисципліни

Основне завдання курсу дати студентам теоретичну та практичну підготовку з основ кібербезпеки, зокрема: тактику, методи та процедури, які використовуються кіберзлочинцями; принципи конфіденційності, цілісності і доступності, оскільки вони відносяться до станів даних і контрзаходів в області кібербезпеки; технології, продукти і процедури, які використовуються для захисту конфіденційності, цілісності та доступності; розуміння, як професіонали кібербезпеки використовують технології, процеси та процедури для захисту всіх компонентів мережі.

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

Знання та розуміння предметної області та розуміння професії.

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 до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.

Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.

2.4. Передумови для вивчення дисципліни.

Перелік дисциплін, які мають бути вивчені раніше: шкільний курс інформатики.

2.5. Результати навчання.

Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності.

Діяти на основі законодавчої та нормативно правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки.

Розробляти моделі загроз та порушника.

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

3. Зміст дисципліни «Основи кібербезпеки»

Змістовий модуль 1. Основи комп'ютерної безпеки.

Тема 1. Кібербезпека – Світ експертів і злочинців.

Світ кібербезпеки. Кіберзлочинці проти фахівців з кібербезпеки. Типові загрози. Розповсюдження загроз кібербезпеки.

Література: 1, 2, 3, 4.

Тема 2. Куб кібербезпеки.

Три виміри куба кібербезпеки. Тріада: конфіденційність, цілісність, доступність. Стани даних.

Література: 1, 2, 3, 4.

Тема 3. Засоби протидії кіберзлочинності.

Структура керування ІТ безпекою. Модель кібербезпеки ISO. Використання моделі ISO для кібербезпеки. Модель кібербезпеки ISO та тріада КЦД.

Література: 1, 4, 5.

Тема 4. Кібербезпека – загрози, вразливості та атаки.

Шкідливе програмне забезпечення та зловмисний код. Типи шкідливого ПЗ. Віруси, Інтернет-черв'яки та «Троянські коні». Логічні бомби (Logic Bombs). Програми – вимагачі.

Література: 1, 2, 4.

Тема 5. Обман.

Мистецтво обману. Соціальна інженерія. Тактики соціальної інженерії. Методи обману. "Серфінг через плече" і "Дайвінг у смітнику". Уособлення і розіграш. Несанкціоноване проникнення. Шахрайство в Інтернеті та по електронній пошті

Література: 1, 2, 4.

Тема 6. Атаки.

Типи кібератак. Відмова в обслуговуванні. Аналіз трафіку (Sniffing). Підміна. Man-in-the-middle (людина посередині). Атаки нульового дня.

Література: 1, 2, 4.

Тема 7. Мистецтво захисту таємниць.

Криптографія. Шифрування за допомогою закритого ключа. Шифрування з відкритим ключем. Порівняння симетричного та асиметричного шифрування.

Література: 1, 2, 4.

Тема 8. Контроль доступу.

Типи контролю доступу. Стратегії контролю доступу. Ідентифікація. Методи аутентифікації. Авторизація. Звітність. Типи засобів контролю безпеки.

Література: 1, 2, 4.

Тема 9. Приховування даних.

Маскування даних. Стеганографія. Обфускація даних.

Література: 1, 2, 5.

Змістовий модуль 2. Захист організації.

Тема 10. Мистецтво забезпечення цілісності.

Типи засобів контролю цілісності даних. Алгоритми хешування. Додавання солі. HMAC.

Література: 1, 4, 5.

Тема 11. Цифрові підписи. Сертифікати.

Підписи та законодавство. Як працює технологія цифрового підпису. Основні відомості про цифрові сертифікати. Створення цифрового сертифіката.

Література: 1, 4, 5.

Тема 12. Забезпечення цілісності баз даних.

Цілісність баз даних. Перевірка баз даних. Вимоги до цілісності баз даних.

Література: 1, 4, 5.

Тема 13. Концепція п'яти дев'яток.

Висока доступність. П'ять дев'яток. Заходи для поліпшення доступності. Керування активами. Захист в глибину. Надмірність. Системна стійкість.

Література: 1, 5, 7

Тема 14. Реагування на інциденти.

Фази реагування на інциденти. Підготовка. Виявлення та аналіз. Стримування і викорінення, а також відновлення. Спостереження за системою після інциденту.

Технології реагування на інциденти. Контроль доступу до мережі. Системи виявлення вторгнень. Системи запобігання вторгнень. NetFlow і IPFIX. Розширений аналіз загроз.

Література: 1, 5, 7.

Тема 15. Відновлення після катастроф.

Планування відновлення після катастроф. План відновлення після стихійних лих. Впровадження заходів аварійного відновлення.

Література: 1, 5, 7.

Тема 16. Захист домену кібербезпеки.

Захист систем та пристроїв. Укріплення хоста. Захист бездротових та мобільних пристроїв. Захист даних на хостах. Керування вмістом і образами. Фізичний захист робочих станцій.

Література: 1, 3, 6.

Тема 17. Укріплення захисту серверів.

Безпечний віддалений доступ. Адміністративні заходи. Фізичний захист серверів.

Література: 1, 3, 6.

Тема 18. Укріплення захисту мережі.

Захист мережевих пристроїв. Оперативні центри. Комутатори, маршрутизатори і мережеві пристрої. Бездротові та мобільні пристрої. Мережеві служби та служби маршрутизації.

Література: 1, 3, 6.

Тема 19. Фізична безпека.

Фізичний контроль доступу. Огородження та барикади. Біометрія. Перепустки та журнали доступу. Спостереження. Відеоспостереження і спостереження з використанням електронних засобів. RFID та бездротовий нагляд.

Література: 1, 3, 6.

Тема 20. Як стати спеціалістом з кібербезпеки.

Домен кібербезпеки. Домен користувача. Домен пристроїв. Домен локальної мережі. Домен приватної хмари. Розуміння етики роботи у кібербезпеці. Етика та керівні принципи. Кіберзакони та відповідальність. Зброя кібербезпеки.

Література: 1, 2, 4.

4. Структура залікового кредиту з дисципліни «Основи кібербезпеки»

4.1 Денна форма навчання

	Кількість годин					
	Лекції	Практичні заняття	СРС	ІРС	Тренінг, КПІЗ	Контрольні заходи
Змістовий модуль 1. Основи комп'ютерної безпеки.						
Тема 1. Кібербезпека - Світ експертів і злочинців	2	3	3		7	Опитування під час заняття, оцінювання практ. занять
Тема 2. Куб кібербезпеки	2	3	4			
Тема 3. Засоби протидії кіберзлочинності	2	3	4			
Тема 4 Кібербезпека – загрози, вразливості та атаки	2	3	6			
Тема 5. Обман	2	3	4			
Тема 6. Атаки	2	3	6			
Тема 7. Мистецтво захисту таємниць	3	3	4	2		
Тема 8. Контроль доступу	2	3	6			
Тема 9. Приховування даних	2	3	4			
Змістовий модуль 2. Захист організації						
Тема 10. Мистецтво забезпечення цілісності	2	3	4	2	7	Опитування під час заняття, оцінювання практ. занять
Тема 11. Цифрові підписи. Сертифікати	2	3	4			
Тема 12. Забезпечення цілісності баз даних	2	3	4	2		
Тема 13. Концепція п'яти дев'яток	2	3	4			
Тема 14. Реагування на інциденти	4	3	4			
Тема 15. Відновлення після катастроф	2	3	4			
Тема 16. Захист домену кібербезпеки	4	3	4			
Тема 17. Укріплення захисту серверів	2	3	4			
Тема 18. Укріплення захисту мережі	2	3	4			
Тема 19. Фізична безпека	2	3	4			
Тема 20. Як стати спеціалістом з кібербезпеки	2	3	4			
Разом	45	60	85	6	14	

5. Тематика лабораторних робіт

Лабораторна робота № 1

Тема: Встановлення віртуальної машини на персональний комп'ютер.

Мета: навчитися встановлювати та використовувати віртуальні машини.

Література: 1, 8

Лабораторна робота № 2

Тема: Packet Tracer - використання перевірок цілісності файлів і даних

Мета: навчитися перевіряти цілісність декількох файлів за допомогою хешів, щоб гарантувати, що файли не були змінені.

Література: 1, 2

Лабораторна робота № 3

Тема: Packet Tracer – WEP/WPA2 PSK/WPA2 RADIUS

Мета: використання WEP, WPA2 PSK і WPA2 RADIUS для демонстрації різних варіантів конфігурації мереж Wi-Fi і особливостей їх захисту

Література: 1, 8.

Лабораторна робота № 4

Тема: **Packet Tracer - Налаштування режиму VPN Transport**

Мета: навчитися налаштувати VPN-клієнт для підключення до об'єкту і відправляти зашифрований FTP-трафік.

Література: 1, 7.

Лабораторна робота № 5

Тема: Packet Tracer - Налаштування режиму тунелю VPN

Мета: навчитися налаштувати тунель VPN між двома об'єктами і відправити зашифрований FTP трафік.

Література: 2, 4.

Лабораторна робота № 6

Тема: Packet Tracer - Резервування маршрутизаторів та комутаторів

Мета: навчитися використовувати декілька маршрутизаторів для забезпечення резервного шлюзу за замовчуванням.

Література: 1, 2.

Лабораторна робота № 7

Тема: Packet Tracer - Стійкість маршрутизаторів і комутаторів

Мета: навчитися захищати конфігурацію IOS маршрутизатора.

Література: 1, 2.

Лабораторна робота № 8

Тема: Packet Tracer - Брандмауери на сервері та ACL на маршрутизаторі

Мета: протестувати підключення до віддаленого веб-сервера.

Література: 1, 3, 4.

Лабораторна робота № 9

Тема: Аутентифікація, авторизація та облік

Мета: навчитися налаштувати елементи керування безпекою під час управління обліковим записом

Література: 1, 2.

Лабораторна робота № 10

Тема: Виявлення загроз і вразливостей

Мета: виявлення загроз та вразливостей в системі за допомогою Nmap, сканеру портів і інструменту для аналізу топології мережної інфраструктури.

Література: 1, 9.

Лабораторна робота № 11

Тема: Використання стеганографії.

Мета: навчитися використовувати стенографію, для приховування документів в файлі JPEG.

Література: 1, 10.

Лабораторна робота № 12

Тема: Дослідження надійності паролів.

Мета: Виявлення паролю користувача з використанням утиліти для зламу пароля.

Література: 1, 3.

Лабораторна робота № 13

Тема: Використання цифрових підписів.

Мета: Зрозуміти концепції цифрового підпису.

Література: 1, 5.

Лабораторна робота №14.

Тема: Віддалений доступ

Мета: Порівняйте використання SSH і Telnet для доступу до віддаленого хосту.

Література: 1, 10

Лабораторна робота №15.

Тема: Захист Linux систем

Мета: Вивчення інструментів аудиту безпеки (security auditing) для захисту системи Linux.

Література: 1, 8

6. Комплексне практичне індивідуальне завдання

Тематика КПЗ: Це підсумкове завдання поєднує багато навичок, які ви здобули протягом вивчення цього курсу.

Завдання.

1. Необхідно налаштувати бездротовий маршрутизатор.
2. Завантажити данні використовуючи FTP.
3. Підключитись безпечно до віддаленого сайту використовуючи VPN.
4. Забезпечити захист для Cisco IOS маршрутизатора.

7. Самостійна робота та дуальна освіта

№ п/п	Тематика
1	Основні поняття кібербезпеки
2	Властивості інформація
3	Види і основні принципи забезпечення кібербезпеки
4	Види захисту інформації
5	Види сучасних комп'ютерних загроз
6	Шкідливе програмне забезпечення (Malware)
7	Комп'ютерні віруси
8	Мережеві хробаки (networm)
9	Троянські програми (trojan)
10	Руткіти (rootkit)
11	Інтернет-шахрайство
12	Несанкціонований доступ до інформаційних ресурсів та інформаційно-телекомунікаційних систем
13	Бот-мережі (botnet)
14	DDoS-атаки (Distributed Denial of Service)
15	Крадіжка коштів
16	«Крадіжка особистості» (Identity Theft)
17	Клавіатурні шпигуни (keylogger)
18	Рекламні системи (adware)
19	Спеціалізовані пошукові системи
20	Анонімність в Інтернеті

8. Організація та проведення тренінгу з дисципліни «Основи кібербезпеки»

№ п/п	Вид роботи	Порядок проведення тренінгу
1	Підключення до Web Server	1. Встановіть доступ до серверу Web HQ Internet з ПК Sally, використовуючи HTTP 2. Встановіть доступ до серверу Web HQ Internet з ПК Sally, використовуючи HTTPS
2	Запобігання незашифрованих HTTP - сесій	1. Налаштування HQ_Router 2. Встановіть доступ до серверу Web HQ Internet з ПК Sally, використовуючи HTTP 3. Встановіть доступ до серверу Web HQ Internet з ПК Sally, використовуючи HTTPS
3	Доступ до брандмауера на сервері	1. На ділянці Metropolis Bank HQ натисніть на сервер Email. 2. Перейдіть на вкладку Desktop та натисніть Firewall.

9. Засоби оцінювання та методи демонстрування результатів навчання

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

- поточне опитування;
- залікове модульне тестування та опитування;
- оцінювання виконання лабораторних робіт;
- оцінювання результатів КПЗ;
- ректорська контрольна робота;
- екзамен.

10. Критерії, форми поточного та підсумкового контролю

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

Для екзамену

Заліковий модуль 1	Заліковий модуль 2	Заліковий модуль 3	Заліковий модуль 4
20%	20%	20%	40%
1. Усне опитування на заняттях – мах 20 балів. 2. Письмова робота – мах 56 балів. 3. Практичне завдання – мах 24 балів	1. Усне опитування на заняттях – мах 20 балів. 2. Письмова робота – мах 52 балів. 3. Практичне завдання – мах 28 балів	1. Підготовка КПЗ – мах 30 балів. 2. Захист КПЗ – мах 40 балів. 3. Оцінка за тренінг – мах 30 балів	1. Розв'язання 20 тестів по 3 бали = мах 60 балів. 2. Практичне завдання = мах 40 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 – 20
2.	Комп'ютерна лабораторія. Доступ до Інтернету.	1 – 20
3.	Методичні вказівки до виконання лабораторних робіт (електронний варіант)	1 – 20
4.	Віртуальна машина Ubuntu CyberEss 1	1 – 20

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Курс мережевої академії Cisco: Cybersecurity Essentials, 2020. Режим доступу. <https://www.netacad.com/courses/cybersecurity/cybersecurity-essentials>
2. Методичні вказівки до виконання лабораторних робіт з курсу “Основи кібербезпеки” для студентів спеціальностей “Кібербезпека” / Укл.: Яцків В. В. – Тернопіль: Економічна думка, 2018. – 44 с.
3. Закон України «Про основні засади забезпечення кібербезпеки України» зі змінами. Відомості Верховної Ради (ВВР), 2017, № 45, ст.403, зі змінами від 28.07.2022 року. Режим доступу: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>
4. Інформаційна безпека. Яковенко Є., Журавель І., Горбатий І., Бондарев А. Видавництво Львівська політехніка, 2019. – 580 с.
5. Вишня В. Б. Основи інформаційної безпеки : навч. посібник / В. Б. Вишня, О. С. Гавриш, Е. В. Рижков. Дніпро : Дніпроп. держ. ун-т внутріш. справ, 2020. – 128 с.
6. Stallings, W. Effective Cybersecurity: Understanding and Using Standards and Best Practices. Addison-Wesley. 2019. – 893 p.
7. Messier Ric. CEH v10 Certified Ethical Hacker Study Guide. John Wiley & Sons, 2019. – 584 p.
8. Yaacoub, Jean-Paul A., et al. A Survey on Ethical Hacking: Issues and Challenges. arXiv preprint arXiv:2103.15072, 2021.
9. Priyadarshini I. Introduction on cybersecurity. Cyber security in parallel and distributed computing: Concepts, techniques, applications and case studies, 2019.– P. 1-37
10. Brooks C. J., Grow, C., Craig Jr, P. A., & Short, D. Cybersecurity essentials. John Wiley & Sons. – 2018. – 784 p.