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

ЗАТВЕРДЖУЮ

Декан ФКІТ
Ігор ЯКИМЕНКО

«30» 08 2024 р.

ЗАТВЕРДЖУЮ

Проректор з науково-
педагогічної роботи
Віктор ОСТРОВЕРХОВ

«__» _____ 2024 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, (год.)	Самост. робота студ. (год.)	Разом (год.)	Екз. (сем.)
Денна	1	1	46	60	6	14	114	240	1

30.08.2024

Тернопіль – 2024

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 № 11 від 26.06.2024 р.).

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

Робоча програма затверджена на засіданні кафедри кібербезпеки, протокол № 1 від 26.08.2024 р.

Завідувач кафедри Василь ЯЦКІВ

Розглянуто та схвалено групою забезпечення спеціальності 125 «Кібербезпека та захист інформації», протокол №1 від 30.08.2024 р.

Голова групи забезпечення спеціальності Василь ЯЦКІВ

Гарант освітньо-професійної програми Михайло КАСЯНЧУК

СТРУКТУРА РОБОЧОЇ ПРОГРАМИ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

1. Опис дисципліни «Основи кібербезпеки»

Дисципліна «Основи кібербезпеки»	**Галузь знань, спеціальність, СВО**	**Характеристика навчальної дисципліни**
Кількість кредитів ECTS – 8	Галузь знань 12 Інформаційні технології	**Статус дисципліни**: обов'язкова **Мова навчання:** українська
Кількість залікових модулів – 5	Спеціальність 125 «Кібербезпека та захист інформації»	Рік підготовки: Денна – 1 Семестр: Денна – 1
Кількість змістових модулів – 2	Ступінь вищої освіти – бакалавр	Лекції (год.): 46 Практичні заняття (год.): 60
Загальна кількість годин – 240		Самостійна робота (год.): 114 Тренінг (год): 14 Індивідуальна робота (год): 6
Тижневих годин – 16, 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 IT 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. Конторолль 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.

Домени 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	Лабор. роботи	СРС	ІРС	Тренінг	Контрольні заходи
Змістовий модуль 1. Основи комп'ютерної безпеки.						
Тема 1. Кібербезпека - Світ експертів і злочинців	2	3	4	3	7	Поточне опитування
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	8			
Тема 8. Контроль доступу	2	3	6			
Тема 9. Приховування даних	2	3	6			
Змістовий модуль 2. Захист організації						
Тема 10. Мистецтво забезпечення цілісності	2	3	6	3	7	Поточне опитування
Тема 11. Цифрові підписи. Сертифікати	2	3	8			
Тема 12. Забезпечення цілісності баз даних	3	3	8			
Тема 13. Концепція п’яти дев’яток	2	3	6			
Тема 14. Реагування на інциденти	4	3	6			
Тема 15. Відновлення після катастроф	2	3	6			
Тема 16. Захист домену кібербезпеки	4	3	6			
Тема 17. Укріплення захисту серверів	2	3	6			
Тема 18. Укріплення захисту мережі	2	3	6			
Тема 19. Фізична безпека	2	3	4			
Тема 20. Як стати спеціалістом з кібербезпеки	2	3	4			
Разом	46	60	114	6	14	

5. Тематика лабораторних робіт

Лабораторна робота № 1

Тема: Встановлення віртуальної машину 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 - Настройка режиму VPN Transport**

Мета: навчитися налаштовувати 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 налаштовувати тунель VPN між двома об'єктами і відправите 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 налаштовувати 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: Вияснення 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

Лабораторна робота №16.

Тема: Порівняння трафіку веб-браузера ,Telnet і SSH

Мета: Використання Wireshark для захоплення трафіку веб-браузера, Telnet та SSH.

Література: 1

Лабораторна робота №17.

Тема: Дослідження MITER CVE

Мета: Визначення релевантних даних про загрози

Література: 1

Лабораторна робота №18.

Тема: Збір системної інформації після інциденту.

Мета: Вивчення системної інформації після того, як стався інцидент

Література: 1

Лабораторна робота №19.

Тема: Аналіз атак

Мета: Дослідження індикаторів компрометації (Indicators of Compromise – IOCs

Література: 1

Лабораторна робота №20.

Тема: Дослідження аварійного відновлення.

Мета: Виконання резервного копіювання на TFTP-сервер

Література: 1

6. Самостійна робота

Для самостійної роботи кожному студенту пропонується виконання вибраного наскрізного завдання. Орієнтовна тематика наскрізних завдань:

1. Дослідження методів соціальної інженерії
2. Дослідження DNS-трафіку
3. Читання журналів подій сервера
4. Налаштування базових функцій безпеки бездротової мережі
5. Рекомендовані заходи щодо зменшення загроз
6. Дослідження процесів, потоків, дескрипторів і реєстру Windows
7. Створення облікових записів користувачів
8. Використання Windows PowerShell
9. Диспетчер завдань Windows
10. Моніторинг і керування системними ресурсами в Windows
11. Робота з текстовими файлами в CLI
12. Використання сканеру портів для виявлення відкритих портів
13. Навігація у файловій системі Linux та встановлення дозволів.
14. Налаштування функцій безпеки в Windows і Linux
15. Посилення захисту системи Linux
16. Відновлення паролів
17. Рекомендації щодо заходу безпеки кінцевої точки
18. Онлайн-інструменти для дослідження шкідливих програм
19. Налаштування автентифікації та авторизації в Linux.

20. Використання класичних та сучасних алгоритмів шифрування
21. Шифрування і розшифрування даних за допомогою OpenSSL

7. 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

8. Методи навчання.

У навчальному процесі застосовуються: лекції, в тому числі з використання мультимедійного проектора та інших ТЗН; лабораторні роботи, індивідуальні заняття; самостійна робота студентів, робота в Інтернет.

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;
– підсумковий модульний контроль за кожним змістовним модулем;
– оцінювання виконання лабораторних робіт;
– оцінювання тренінгів;
– оцінювання результатів самостійної роботи;
– підсумковий письмовий 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:

Модуль 1		Модуль 2		Модуль 3	Модуль 4	Модуль 5
10 %	10 %	10 %	10 %	5 %	10 %	40 %
Поточне оцінювання	Модульний контроль 1	Поточне оцінювання	Модульний контроль 1	Тренінги	Самостійна робота	Екзамен
Оцінка за даний модуль визначається як середнє арифметичне за захист лабораторних робіт №1-10.	Підсумкова письмова робота за темами №1-13.	Оцінка за даний модуль визначається як середнє арифметичне за захист лабораторних робіт №11-20.	Підсумкова письмова робота за темами №14-27	Визначається як середнє арифметичне з оцінок за виконання двох завдань тренінгу.	Оцінка за даний модуль виставляється за виконання вибраного наскрізного завдання.	1. 20 тестів по 3 бали - max 60 балів. 2.Практичне завдання - max 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 – 27
2.	Комп'ютерна лабораторія. Доступ до Інтернету.	1 – 27
3.	Методичні вказівки до виконання лабораторних робіт (електронний варіант)	1 – 27
4.	Віртуальна машина Ubuntu_CyberEss_1	1 – 27

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Курс мережевої академії Cisco: Основи кібербезпеки, 2024. Режим доступу: https://www.netacad.com/courses/cybersecurity-essentials?courseLang=uk-UA
2. 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
3. Інформаційна безпека. Яковенко Є., Журавель І., Горбатий І., Бондарєв А. Видавництво Львівська політехніка, 2019. – 580 с.
4. 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.
5. Stallings, W. Effective Cybersecurity: Understanding and Using Standards and Best Practices. Addison-Wesley. 2019. – 893 p.
6. Messier Ric. CEH v10 Certified Ethical Hacker Study Guide. John Wiley & Sons, 2019. – 584 p.
7. Yaacoub, Jean-Paul A., et al. A Survey on Ethical Hacking: Issues and Challenges. arXiv preprint arXiv:2103.15072, 2021.
8. Priyadarshini I. Introduction on cybersecurity. Cyber security in parallel and distributed computing: Concepts, techniques, applications and case studies, 2019.– P. 1-37
9. The NIST Cybersecurity Framework (CSF) 2.0 National Institute of Standards and Technology. This publication is available free of charge from: https://doi.org/10.6028/NIST.CSWP.29. February 26, 2024
10. National Institute of Standards and Technology Special Publication 800-53A Revision 5 Natl. Inst. Stand. Technol. Spec. Publ. 800-53A, Rev. 5, 733 pages (January 2022) CODEN: NSPUE2. This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-53Ar5