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

ЗАТВЕРДЖУЮ

Декан факультету комп'ютерних інформаційних технологій
Ігор ЯКИМЕНКО

«29» 08 2025 р.

ЗАТВЕРДЖУЮ

Проректор з науково-педагогічної роботи
Віктор ОСТРОВЕРХОВ

«__» _____ 2025 р.

РОБОЧА ПРОГРАМА

з дисципліни «Основи кібербезпеки»
ступінь вищої освіти – бакалавр
галузь знань – F Інформаційні технології
спеціальність – F5 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

29.08.2025

Тернопіль – 2025

Робоча програма розроблена на основі освітньо-професійної програми підготовки бакалавра галузі знань F «Інформаційні технології» спеціальності F5 «Кібербезпека та захист інформації», затвердженої Вченою радою ЗУНУ (протокол № 8 від 26.06.2025 р.).

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

Робоча програма затверджена на засіданні кафедри кібербезпеки,
протокол № 1 від 26.08.2025 р.

Завідувач кафедри  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 F Інформаційні технології	**Статус дисципліни**: обов'язкова **Мова навчання:** українська
Кількість залікових модулів – 5	Спеціальність F5 «Кібербезпека та захист інформації»	Рік підготовки: Денна – 1 Семестр: Денна – 1
Кількість змістових модулів – 2	Ступінь вищої освіти – бакалавр	Лекції (год.): 46 Лабораторні роботи (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 здобувачів цілісного уявлення про спеціальність кібербезпека та базових знань в даній галузі.

2.2. Завдання вивчення дисципліни

Основне завдання курсу дати здобувачам 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.

ЗКІ. Здатність застосовувати знання у практичних ситуаціях.

ЗК2. Знання та розуміння предметної області і розуміння професійної діяльності.

СК2. Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації.

СКЗ. Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики кібербезпеки та захисту інформації.

СК 4. Здатність забезпечувати захист інформації в інформаційних та інформаційно-комунікаційних системах згідно встановленої політики кібербезпеки й захисту інформації.

СК5. Здатність відновлювати функціонування інформаційних та інформаційно-комунікаційних систем після реалізації загроз, здійснення кібератак, збоїв і відмов різних класів та походження.

2.4. Передумови для вивчення дисципліни.

Вивчення курсу передбачає наявність знань отриманих при вивченні шкільного курсу інформатики, пов'язаних з матеріалами суміжних курсів: «Основи програмування», «Вища математика».

2.5. Результати навчання.

РН4. Організовувати власну професійну діяльність, обирати й використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність.

РН5. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.

РН6. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат.

РН10. Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.

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.

Тема 2. Куб кібербезпеки.

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

Тема 3. Засоби протидії кіберзлочинності.

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

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.

Тема 5. 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

Тема 6. Типи кібератак.

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

Тема 7. Мистецтво захисту таємниць.

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

Тема 8. Контроль доступу.

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

Тема 9. Приховування даних.
Маскування даних. Стеганографія. Обфускація даних.

Змістовий модуль *2.* Захист організації.
Тема 10. Мистецтво забезпечення цілісності.
Типи засобів контролю цілісності даних. Алгоритми хешування. Додавання солі. HMAC.

Тема 11. Цифрові підписи. Сертифікати.
Підписи та законодавство. Як працює технологія цифрового підпису. Основні відомості про цифрові сертифікати. Створення цифрового сертифіката.

Тема 12. Забезпечення цілісності баз даних.
Цілісність баз даних. Перевірка баз даних. Вимоги до цілісності баз даних.

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.

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.

Тема 15. Відновлення після катастроф.
Планування відновлення після катастроф. План відновлення після стихійних лих. Впровадження заходів аварійного відновлення.

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.

Тема 17. Укріплення захисту серверів.
Безпечний віддалений доступ. Адміністративні заходи. Фізичний захист серверів.

Тема 18. Укріплення захисту мережі.
Захист мережевих пристроїв. Оперативні центри. Комутатори, маршрутизатори і мережеві пристрої. Бездротові та мобільні пристрої. Мережеві служби та служби маршрутизації.

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.

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.

4. Структура залікового кредиту з дисципліни «Основи кібербезпеки»
4.1 Денна форма навчання

	Кількість годин					
	Лекції	Лабор. роботи	ІРС	Тренінг	СРС	Контрольні заходи
Змістовий модуль 1. Основи комп'ютерної безпеки.						
Тема 1. Кібербезпека - Світ експертів і злочинців	2	3	3	7	4	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. Мистецтво обману	2	3			4	
Тема 6. Типи кібератак	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	3	7	6	Поточне опитування
Тема 11. Цифрові підписи. Сертифікати	3	3			8	
Тема 12. Забезпечення цілісності баз даних	2	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	6	14	114	

5. Тематика лабораторних робіт

Лабораторна робота № 1

Тема: Встановлення віртуальної машину на персональний комп'ютер.
Мета: навчитися встановлювати та використовувати віртуальні машини.

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.

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

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.

Лабораторна робота № 5

Тема: Packet Tracer - Налаштування режиму тунелю VPN

Мета: навчитися налаштовувати тунель VPN між двома об'єктами і відправите зашифрований FTP трафік.

Лабораторна робота № 6

Тема: Packet Tracer - Резервування маршрутизаторів та комутаторів

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

Лабораторна робота № 7

Тема: Packet Tracer - Стійкість маршрутизаторів і комутаторів

Мета: навчитися захищати конфігурацію IOS маршрутизатора.

Лабораторна робота № 8

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

Мета: протестувати підключення до віддаленого веб-сервера.

Лабораторна робота № 9

Тема: Аутентифікація, авторизація та облік

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

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.

Лабораторна робота № 11

Тема: Використання стеганографії.

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

Лабораторна робота № 12

Тема: Дослідження надійності паролів.

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

Лабораторна робота № 13

Тема: Використання цифрових підписів.

Мета: Зрозуміти концепції цифрового підпису.

Лабораторна робота №14.

Тема: Віддалений доступ

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

Лабораторна робота №15.

Тема: Захист Linux систем

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

Лабораторна робота №16.

Тема: Порівняння трафіку веб-браузера ,Telnet і SSH

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

Лабораторна робота №17.

Тема: Дослідження MITER CVE

Мета: Визначення релевантних даних про загрози

Лабораторна робота №18.

Тема: Збір системної інформації після інциденту.

Мета: Вивчення системної інформації після того, як стався інцидент

Лабораторна робота №19.

Тема: Аналіз атак

Мета: Дослідження індикаторів компрометації (Indicators of Compromise – IOCs

Лабораторна робота №20.

Тема: Дослідження аварійного відновлення.

Мета: Виконання резервного копіювання на TFTP-сервер

6. Самостійна робота

Для самостійної роботи кожному здобувачу пропонується виконання вибраного 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 освітньому процесі застосовуються: лекції, в тому числі з використання мультимедійного проектора та інших ТЗН; лабораторні роботи, індивідуальні заняття; самостійна робота здобувачів, 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;
– оцінювання виконання лабораторних робіт;
– підсумковий модульний контроль за кожним змістовним модулем;
– оцінювання тренінгів;
– оцінювання результатів самостійної роботи;
– підсумковий екзамен.

10. Політика оцінювання

Політика щодо дедлайнів і перескладання. Для виконання усіх видів завдань здобувачами і проведення контрольних заходів встановлюються конкретні терміни. Перескладання модулів проводиться в установленому порядку.

Політика щодо академічної доброчесності. Списування під час проведення контрольних заходів заборонені. Під час контрольного заходу здобувач може користуватися лише дозволеними допоміжними матеріалами або засобами, йому забороняється в будь-якій формі обмінюватися інформацією з іншими здобувачами, використовувати, розповсюджувати, збирати варіанти контрольних завдань.

Політика щодо відвідування. За об'єктивних причин (наприклад, карантин, воєнний стан, хвороба, закордонне стажування) навчання може відбуватись в дистанційній формі за погодженням із керівником курсу з дозволу дирекції факультету.

11. 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 %	15 %	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.	Підсумкове тестування за темами №1-10.	Оцінка за даний модуль визначається як середнє арифметичне за захист лабораторних робіт №11-20.	Підсумкове тестування за темами №11-20	Визначається як середнє арифметичне з оцінок за виконання двох завдань тренінгу.	Оцінка за даний модуль виставляється за виконання вибраного наскрізного завдання.	1. Теоретичні питання: 2 питання по 20 балів. 2. 30 тестів по 2 бали.

Виконання лабораторних робіт:

90-100 балів: здобувач демонструє глибоке розуміння теми й чітко пояснює застосовані принципи, виконує всі етапи лабораторної роботи без помилок, обґрунтовує вибір інструментів та методів, перевіряє результати перехресною валідацією. Звіт повний і структурований: містить цілі, методику, відтворювані кроки (команди/скрипти), докази (логи/скріншоти), схему топології або потоку даних, аналіз отриманих артефактів, чіткі рекомендації (із посиланням на критерії критичності). Дотримано етики, правових обмежень і завдання, роботу виконано самостійно, результат легко відтворити іншими.

75-89 балів: здобувач коректно виконує більшість завдань і демонструє загалом правильне розуміння теорії, але припускається поодиноких неточностей або пропускає другорядні кроки (наприклад, неповна валідація чи не всі негативні/граничні тести). Вибір інструментів і методів здебільшого обґрунтований, однак місцями бракує глибини аналізу або альтернатив. Звіт містить основні розділи, є достатньо докладним (кроки, скріншоти, коротка схема), проте місцями не вистачає чіткої аргументації або повноти доказів; рекомендації релевантні, але частково узагальнені або без пріоритизації. Етичні вимоги й завдання витримано, відтворюваність у цілому можлива, інколи потрібні додаткові уточнення.

60-74 балів: здобувач виконує мінімально необхідні кроки для досягнення базових результатів, але помітні прогалини у розумінні (теорія викладена поверхово, інструменти застосовано за шаблоном). Аналіз обмежується описом кроків без достатнього обґрунтування; перевірка результатів слабка або відсутня (немає перехресної перевірки, граничні випадки не розглянуто). Звіт неповний: бракує частини доказів (логи/скріншоти), схема або відсутня, або формальна; рекомендації загальні та без пріоритизації. Етичні та правові аспекти зазвичай дотримано, але потребують нагадувань; відтворюваність часткова, вимагає суттєвої допомоги викладача.

1-59 балів: здобувач не досягає цілей лабораторної роботи: демонструє суттєві непорозуміння базових принципів, обирає або застосовує інструменти некоректно, не отримує коректних результатів чи наводить неперевірені/сумнівні дані. Звіт відсутній або має фрагментарний характер (немає кроків, доказів, аналізу, схем), рекомендації відсутні або нерелевантні; відтворюваність неможлива. Порушуються етичні норми, межі завдання чи інструкції з безпечної роботи, або виявлено ознаки академічної недоброчесності (плагіат/фальсифікація).

Підсумкове тестування за темами: вид контролю, при якому засвоєний здобувачем теоретичний та практичний матеріал оцінюється у форматі тестування. Тестування містить 20 запитань кожна правильна відповідь дає 5 бали, максимум 100 балів.

Тренінг:

90-100 балів: здобувач самостійно, без помилок, виконав усі етапи завдання, правильно задокументував усі етапи роботи, та вільно оперує поняттями та принципами тестування на проникнення.

75-89 балів: здобувач виконав завдання, але з кількома дрібними помилками, які не вплинули на кінцевий результат (наприклад, неточна послідовність дій), виникали питання під час роботи.

60-74 балів: здобувач виконав завдання, але з суттєвими помилками, наприклад, не з першого разу. Розуміння поставлених завдань є поверхневим.

1-59 балів: здобувач не зміг виконати завдання або результати були повністю невірними. Не продемонстрував базових навичок роботи з наданим програмним забезпеченням.

Самостійна робота:

90–100 балів: доповідь охоплює всі ключові аспекти обраної теми, демонструючи глибоке розуміння предмету дисципліни. Дослідження містить не лише опис, але й глибокий аналіз, порівняння різних методів та засобів, висновки обґрунтовані. У процесі написання звіту використані сучасні та актуальні джерела інформації, що свідчить про обізнаність здобувача з напрямом дослідження. Здобувач вільно володіє матеріалом, доповідає впевнено та відповідає на всі запитання.

75–89 балів: доповідь розкриває основні питання теми, але може бути недостатньо деталізованою; є аналітичні елементи, але вони можуть бути не достатньо глибокими; використані джерела інформації є релевантними, але не найновішими. Здобувач демонструє знання матеріалу, але має незначні труднощі з відповідями на додаткові питання.

60–74 балів: доповідь охоплює лише основні аспекти теми, бути пропущені важливі деталі. Робота має описовий характер, аналіз та висновки є поверхневими. Здобувач не завжди впевнено відповідає на запитання, а сам виступ може бути нечітким.

1–59 балів: зміст доповіді не відповідає темі або є компіляцією застарілих даних. Робота є прямим копіюванням без самостійного опрацювання.

Екзамен - вид підсумкового контролю, який проводиться з метою оцінювання засвоєння здобувачем вищої освіти теоретичного та практичного матеріалу з дисципліни. Екзаменаційний білет складається з двох блоків.

Перший блок містить два теоретичних запитання, за кожне з яких можна отримати від **0 до 20 балів**, що в підсумку дає максимально 40 балів. За відповідь на питання здобувач освіти отримує **11–20 балів**, якщо у повному обсязі володіє навчальним матеріалом, всебічно, самостійно та аргументовано відповідає на питання білету і **1–10 балів** – якщо володіє навчальним матеріалом не в повному обсязі, викладає його фрагментарно, допускаючи при цьому суттєві неточності.

Другий блок містить 30 тестових завдань. За кожну правильну відповідь тестування здобувач освіти отримує 2 бали, максимум 60 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)

12. 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: 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