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

ЗАТВЕРДЖУЮ
Декан факультету комп'ютерних інформаційних технологій
_____ Ігор ЯКИМЕНКО
«_29_» _____ 2025 р.

ЗАТВЕРДЖУЮ
Проректор з науково-педагогічної роботи
_____ Віктор ОСТРОВЕРХОВ
«_30_» _____ 2025 р.

РОБОЧА ПРОГРАМА

з дисципліни «Практикум зі спеціальності»
ступінь вищої освіти – бакалавр
галузь знань - 12 Інформаційні технології
спеціальність – 125 Кібербезпека
освітньо-професійна програма – Кібербезпека

Кафедра кібербезпеки

Форма навчання	Курс	Семестр	Лекції (год.)	Лабор. роботи (год.)	ІРС (год.)	Тренінг (год.)	СРС (год.)	Разом (год.)	Залік / екзамен (семестр)
Денна	4	8	30	30	4	6	110	180	Екзамен (8)

29.08.2025

Тернопіль – 2025

Робоча програма складена на основі освітньо-професійної програми підготовки бакалавра галузі знань 12 Інформаційні технології спеціальності 125 Кібербезпека, затвердженої Вченою радою ЗУНУ (протокол № 9 від 15.06.2022 р.).

Робочу програму склав доцент кафедри кібербезпеки, доктор філософії (Кібербезпека та захист інформації) Сергій КУЛИНА.

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 «Практикум зі спеціальності»

Дисципліна «Кібернетична безпека»	**Галузь знань, спеціальність, СВО**	**Характеристика навчальної дисципліни**
Кількість кредитів ECTS – 6	Галузь знань 12 Інформаційні технології	Статус дисципліни – обов'язкова. Мова навчання – українська.
Кількість залікових модулів – 5	Спеціальність 125 «Кібербезпека»	Рік підготовки: Денна – 4. Семестр: Денна – 8.
Кількість змістових модулів – 2	Ступінь вищої освіти – бакалавр	Лекції (год): Денна – 30. Лабораторні заняття (год): Денна – 30.
Загальна кількість годин – 180		Самостійна робота (год): 110. Тренінг (год): 6. Індивідуальна робота (год): 4.
Тижневих годин – 18, з них аудиторних – 6		Вид підсумкового контролю – екзамен.

2. Мета і завдання дисципліни «Практикум зі спеціальності»

2.1. Мета вивчення дисципліни

Метою дисципліни «**Практикум зі спеціальності**» є – здобуття компетентностей, які формуються під час вивчення комплексу обов'язкових освітніх компонент упродовж всього терміну навчання та підготовки до успішного складання ЄДКІ.

2.2. Завдання вивчення дисципліни

Основне завдання дисципліни: дати достатній рівень знань, умінь та компетентностей у галузі забезпечення інформаційної безпеки і/або кібербезпеки; мати здатності до застосовування отриманих знань у практичних ситуаціях; знати та розуміти предметну область, розуміти професію; вміти виявляти, ставити та вирішувати проблеми у галузі кібербезпеки.

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

- Знання та розуміння предметної області та розуміння професії.
- Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.
- Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.
- Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.

2.4. Передумови для вивчення дисципліни

Вивчення курсу «Практикум зі спеціальності» передбачає наявність систематичних та ґрунтовних знань із суміжних дисциплін («Тестування на проникнення», «Комплексні системи захисту інформації», «Управління інформаційною безпекою», «Нормативно-правове забезпечення»), а також цілеспрямованої роботи на лекційних та практичних заняттях, самостійної роботи здобувачів освіти.

2.5. Результати навчання

- Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки.
- Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно телекомунікаційних систем.
- Вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації.
- Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації.
- Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах.
- Вирішувати задачі захисту інформації, що обробляється в інформаційно телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації.
- Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно телекомунікаційних системах.
- Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно телекомунікаційних системах.
- Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно телекомунікаційних системах.
- Використовувати інструментарій для моніторингу процесів в інформаційно телекомунікаційних системах.
- Здійснювати оцінку можливості проникнення в інформаційні системи та мережі шляхом виявлення та експлуатації наявних вразливостей.

3. Програма навчальної дисципліни: «Практикум зі спеціальності»

Змістовий модуль 1. Інформаційні технології в інформаційній та/або кібербезпеці.

Тема 1. Законодавча та нормативно-правова база, державні та міжнародні вимоги, практики і стандарти в галузі інформаційної та/або кібербезпеки.

1.1 Законодавча та нормативно-правова база України в галузі інформаційної та /або кібербезпеки. ЗУ «Про інформацію», «Про науково-технічну інформацію». ЗУ «Про захист інформації в інформаційно-телекомунікаційних системах», «Про основні засади забезпечення

кібербезпеки України». ЗУ «Про державну таємницю». «Про захист персональних даних». Постанова КМУ від 19 червня 2019 року No 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури».

1.2 Державні Стандарти України в галузі інформаційної та/або кібербезпеки: ДСТУ 3396.0,1,2-97; ДСТУ ISO/IEC 15408-1:2017. Нормативні документи з технічного захисту інформації. НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу». НД ТЗІ 2.5-004-99. «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу».

1.3 Міжнародні стандарти в галузі інформаційної та /або кібербезпеки. Регламенти ЄС в галузі кібербезпеки. Регламент Європейського Парламенту і Ради (ЄС) 2019/881 від 17 квітня 2019 року «Про Агентство Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA) та про сертифікацію кібербезпеки інформаційно-комунікаційних технологій» ISO 27001, ISO 27002, ISO 27003; ISO/IEC 15408- 2, ISO/IEC 15408-3.

Тема 2. Інформаційні технології в інформаційній та/або кібербезпеці

2.1 Інструментальні та прикладні застосунки в інформаційній та/або кібербезпеці. Мережева модель OSI. Основні протоколи стеку TCP/IP. Віртуалізація (принципи, гіпервізори). Архітектура комп'ютерів.

2.2 Методи і засоби обробки інформації. Алгоритмізація та програмування (без прив'язки до конкретної мови програмування). Основи об'єктно-орієнтованого програмування (Класи, Методи, Перевантаження, Наслідування, Узагальнення). Методи сортування та пошуку даних.

2.3 Операційні системи. Архітектура операційних систем. Процеси і потоки в операційних системах. Керування пам'яттю в операційних системах. Файлові системи. Захисні механізми операційних систем.

Тема 3. Безпека інформаційно-комунікаційних систем

3.1 Захист інформації, що обробляється та зберігається в ІКС. Процедури ідентифікації, автентифікації, авторизації користувачів. Резервування інформації та компонентів ІКС.

3.2 Програмні та програмно-апаратні комплекси ЗЗІ. Антивіруси, міжмережеві екрани (призначення, архітектура, функції). IPS, IDS (призначення, архітектура, функції). Системи контролю та управління доступом в ІКС (Active Directory, ACL).

3.3 Відновлення функціонування ІКС після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження. Організаційно-технічні заходи відновлення функціонування ІКС.

3.4 Моніторинг процесів функціонування ІКС. Журнал аудиту подій. Політики резервного копіювання даних. Джерела інформації про події та типи подій, що аналізуються в системах моніторінгу Система візуалізації та управління подіями (SIEM).

3.5 Механізми безпеки комп'ютерних мереж. Протоколи безпеки на канальному рівні. Протоколи безпеки на мережному рівні (IPSec). Протоколи безпеки на транспортному/сеансовому рівні (SSL/TLS). Протоколи безпеки прикладного рівня (HTTPS). Протоколи автентифікації прикладного рівня (RADIUS). Віртуальні приватні мережі (VPN).

Тема 4. Комплексні системи захисту інформації

4.1 Проєктування, створення, супровід КСЗІ.

Дослідження середовищ функціонування. Вибір методів та засобів забезпечення необхідного рівня ІБ.

4.2 Моделі загроз та моделі порушника. Загрози цілісності. Загрози доступності. Загрози конфіденційності. Загрози через технічні канали. Загрози автентичності.

4.3 Оцінка захищеності інформації в ІКС

Змістовий модуль 2. Управління інформаційною та / або кібербезпекою

Тема 5. Управління інформаційною та / або кібербезпекою

5.1 Управління кіберінцидентами. Поняття кіберінцидента / кібератаки. Розслідування кіберінцидентів / кібератак.

5.2 Управління ризиками в інформаційній та / або кібербезпеці. Ризики інформаційної безпеки. Аналіз та оцінка ризику. Прийняття ризику. Зменшення ризику. Страхування (перекладання) ризику.

5.3 Політика інформаційної безпеки. Розробка політик ІБ під час забезпечення бізнес-процесів. Дотримання політик ІБ під час забезпечення бізнес-процесів.

Тема 6. Криптографічний захист інформації

6.1 Математичні основи криптографії та стеганографії. Модулярні обчислення. Елементи теорії чисел. Алгоритм Евкліда. Теорема Ейлера. Теореми Ферма. Обчислення у скінченних полях. Умови стійкості шифрів. Однонаправлені функції, функції гешування. Псевдовипадкові послідовності в криптосистемах. Обчислення в системі чисел з плаваючою точкою.

6.2 Симетричні криптосистеми. Модель симетричної криптосистеми. Класичні методи шифрування. Шифр Цезаря, Вернама. Квадрат Полібія. Шифр гамування. Блокові шифри. DES, AES, ДСТУ ГОСТ 28147-2009, ДСТУ 7624:2014 (довжина ключів, довжина блоку вхідного тексту, кількість раундів, крипостійкість, режими роботи згідно з ДСТУ ISO/IEC 10116:2019). Потокові шифри. RC4, STRUMOK. (довжина ключів, крипостійкість).

6.3 Асиметричні криптосистеми. Модель асиметричної криптосистеми. Шифри RSA, Ель Гамаля (EG). Генерація спільних секретних ключів Діффі-Хеллмана (DH). Електронний цифровий підпис DSA.

6.4 Цифрова стеганографія. Поняття цифрової стеганографії. Модель стеганосистеми. Основні вимоги до стеганосистеми. Відкриті, напівзакриті, закриті стеганосистеми. Поняття ЦВЗ, класифікація. Метод модифікації найменшого значущого біта.

Тема 7. Технічний захист інформації.

7.1 Технічні канали витоку інформації. Вібро-акустичний канал витоку інформації. Електричний канал витоку інформації. Електромагнітний канал витоку інформації. Оптичний та оптоелектронний канал витоку інформації. Параметричний канал витоку інформації.

7.2 Методи та засоби технічного захисту інформації. Пасивні методи та засоби захисту інформації від витоку технічними каналами. Активні методи та засоби захисту інформації від витоку технічними каналами. Методи пошуку та блокування засобів негласного отримання інформації. Методи та засоби технічного захисту інформації від витоку вібро-акустичними каналами. Методи та засоби технічного захисту інформації від витоку електромагнітними та електричними каналами. Методи та засоби технічного захисту інформації від витоку оптичними та оптоелектронними каналами. Методи та засоби технічного захисту інформації від витоку параметричними каналами. Системи відеоспостереження, охоронних сигналізацій, контролю доступу.

4. Структура залікового кредиту з дисципліни «Практикум зі спеціальності»

	Кількість годин					
	Лекції	Лабор. заняття	Інд. робота	Тренінг	Самост. робота	Контр. заходи
Змістовий модуль 1. Інформаційні технології в інформаційній та/або кібербезпеці						
Тема 1. Законодавча та нормативно-правова база, державні та міжнародні вимоги, практики і стандарти в галузі інформаційної та/або кібербезпеки	6	4	2	4	16	Поточне опитування
Тема 2. Інформаційні технології в інформаційній та/або кібербезпеці	6	6			16	
Тема 3. Безпека інформаційно-комунікаційн их систем	4	6			14	
Тема 4. Комплексні системи захисту інформації	2	2			16	
Змістовий модуль 2. Управління інформаційною та / або кібербезпекою						
Тема 5. Управління інформаційною та / або кібербезпекою	4	4	2	2	16	Поточне опитування
Тема 6. Криптографічний захист інформації	6	6			16	
Тема 7. Технічний захист інформації	2	2			16	
Разом	30	30	4	6	110	

5. Тематика лабораторних робіт

Лабораторна робота №1.

Тема: Вивчення процесів, потоків, дескрипторів і реєстру Windows

Мета: вивчення процесів, потоків і дескриптори за допомогою засобу Process Explorer, що входить до складу SysInternals Suite.

Питання для обговорення:

1. Вивчення процесів
2. Вивчення потоків і дескрипторів
3. Вивчення реєстру Windows

Лабораторна робота №2

Тема: Аналіз трафіку HTTP і HTTPS за допомогою програми Wireshark

Мета: навчитися аналізувати і перехоплювати трафік HTTP і HTTPS за допомогою програми Wireshark.

Питання для обговорення:

1. Перехоплення і перегляд HTTP-трафіку
2. Перехоплення і перегляд HTTPS-трафіку

Лабораторна робота №3

Тема: Packet Tracer. Наочне подання роботи списку контролю доступу

Мета: навчитися використовувати список контролю доступу (ACL) для заборони ехозапитів, відправлених на вузли віддалених мереж.

Питання для обговорення:

1. Перевірка локального підключення і тестування роботи списку контролю доступу
2. Видалення списку контролю доступу та перевірка підключення

Лабораторна робота №4

Тема: Packet Tracer. Визначення потоку пакетів

Мета: спостереження за потоком пакетів в топології локальної та глобальної мережі а також спостереження за змінами потоку пакетів при зміні топології мережі.

Питання для обговорення:

1. Перевірка зв'язку
2. Топологія віддаленої локальної мережі
3. Топологія глобальної мережі

Лабораторна робота №5

Тема: Packet Tracer. Ведення журналу мережевої активності

Мета: навчитися використовувати Packet Tracer для аналізу і реєстрації мережевого трафіку. Ви розглянете вразливість в одному мережевому додатку, а також перегляньте трафік ICMP за допомогою системного журналу.

Питання для обговорення:

1. Створення трафіку FTP
2. Вивчення трафіку FTP
3. Перегляд повідомлень системного журналу

Лабораторна робота №6

Тема: Вивчення трафіку DNS

Мета: навчитися використовувати програму Wireshark в системі Windows для фільтрації пакетів DNS і перегляду інформації як про пакети запитів, так і відповідей DNS.

Питання для обговорення:

1. Перехоплення трафіку DNS
2. Вивчення трафіку DNS-запиту
3. Вивчення трафіку DNS-відповіді

Лабораторна робота №7

Тема: Читання журналів сервера

Мета: вивчення журналів сервера

Питання для обговорення:

1. Читання файлів журналів з використанням програм Cat, More і Less
2. Файли журналів і Syslog
3. Файли журналів і Journalctl

Лабораторна робота №8

Тема: Вивчення сеансів зв'язку за протоколами Telnet і SSH за допомогою програми Wireshark

Мета: навчитися налаштовувати маршрутизатор для підключень по протоколу SSH і використовувати програму Wireshark для перехоплення і перегляду даних, що передаються під час сеансів Telnet і SSH.

Питання для обговорення:

1. Вивчення сеансу Telnet за допомогою програми Wireshark
2. Вивчення сеансу SSH за допомогою програми Wireshark

Лабораторна робота №9

Тема: Дослідження реалізації NetFlow

Мета: використання Packet Tracer для створення мережевого трафіку і спостереження за відповідними записами потоків NetFlow в засобі збору даних NetFlow..

Питання для обговорення:

1. Спостереження за записом потоків NetFlow (один напрямок).
2. Спостереження за записом потоків NetFlow для сеансу, який входить в засіб збору даних і виходить з нього.

Лабораторна робота №10

Тема: Packet Tracer. Ведення журналів з декількох джерел

завдання

Мета: навчитися використовувати Packet Tracer для перегляду даних, сформованих системним журналом, AAA і NetFlow.

Питання для обговорення:

1. Використання системного журналу для перехоплення файлів з декількох мережевих пристроїв
2. Спостереження за доступом користувача AAA
3. Ознайомлення з інформацією про NetFlow.

Лабораторна робота №11

Тема: Налаштування середовища з кількома ВМ

Мета: навчитися налаштовувати середовище віртуальної мережі шляхом підключення один до одної декількох віртуальних машин в Virtualbox.

Питання для обговорення:

1. Імпорт пристрою віртуальної машини в VirtualBox
2. Об'єднайте в мережу віртуальні машини для створення віртуальної лабораторної середовища
3. Завершення роботи віртуальних машин.

Лабораторна робота №12

Тема: Правила Snort і міжмережевого екрану

Мета: Ознайомлення з принципами написання правил Snort і міжмережевого екрану

Питання для обговорення:

1. Підготовка віртуального середовища
2. Брандмауер і журнали IDS
3. Завершення і очищення процесу Mininet

6. Організація і проведення тренінгу з дисципліни «Практикум зі спеціальності»

Тематика: Розробка системи виявлення та запобігання вторгнень на основі open source рішень.

Мета тренінгу з дисципліни «Практикум зі спеціальності» – поглиблення та закріплення теоретичних знань з дисципліни, отриманих на лекційних та лабораторних заняттях, а також формування у здобувачів освіти:

- практичних навичок ключових професійних дій та операцій, які є невід'ємною частиною майбутньої роботи у сфері кіберзахисту;
- уміння використовувати теоретичні знання для вирішення реальних, практичних завдань у сфері кіберзахисту;
- навичок аналізу професійних ситуацій, пошуку ефективних рішень та оцінки їхніх результатів;
- усвідомлення важливості дотримання стандартів у сфері кіберзахисту.

Порядок проведення:

1. Вступна частина проводиться з метою ознайомлення учасників з темою та основними завданнями тренінгу, ключовими поняттями та принципами, що будуть використані в процесі роботи.
2. Організаційна частина полягає у формуванні робочих груп та поясненні правил роботи. Учасники групою обирають open source рішення із рекомендованого переліку.
3. Практична частина реалізується шляхом виконання завдань тренінгу, а саме розгортанні та налаштуванні системи виявлення та запобігання вторгненням з подальшим оформленням звіту про виконану роботу.
4. Підведення підсумків. Обговорення результатів виконаних завдань. Обмін думками з питань, що виносились на тренінг.

Завдання тренінгу полягає в розробці системи виявлення та запобігання вторгнень на основі наступного переліку рекомендованих open source рішень:

1. Snort
2. Suricata
3. Zeek (раніше Bro)
4. OSSEC
5. Wazuh
6. OpenWIPS-NG
7. Security Onion
8. Fail2Ban
9. ClamAV
10. Elastic Stack (ELK)

Оцінка за тренінг виставляється на основі представленого та захищеного звіту про розгортання та налаштування системи виявлення та запобігання вторгненням. Максимальна кількість балів за завдання самостійної роботи становить 100 балів.

7. Самостійна робота

Здобувачі освіти мають самостійно опрацьовувати відповідний обсяг інформації, оскільки це є обов'язковим компонентом їхньої навчальної діяльності у вищій школі. Самостійна робота полягає у проведенні дослідження та підготовці звіту згідно однієї вибраної здобувачем освіти теми із запропонованих орієнтованих тематик:

Орієнтована 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). База вразливостей CVE
12	Стандарт безпеки даних індустрії платіжних карт (PCI DSS).
13	Управління ризиками.
14	Політики безпеки
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.

Метою виконання самостійного завдання з дисципліни «Практикум зі спеціальності» є оволодіння навиками самостійно, без сторонньої допомоги, вирішувати типові та нестандартні завдання, з якими здобувач освіти зіткнеться в майбутній професії.

Загальні вимоги до оформлення результатів виконаних завдань самостійної роботи: шрифт − Times New Roman; розмір шрифту − 14 кегель; інтервал між рядками – 1,5; абзац – 1,25 см, поля: верхнє і нижнє – 20 мм, ліве – 25 мм, праве – 15 мм; нумерація сторінок − у правому нижньому куті; обсяг звіту – 10-12 сторінок друкованого тексту. Максимальна кількість балів за завдання самостійної роботи становить 100 балів.

8. Методи навчання

У процесі навчання використовуються: лекції, в тому числі із використання мультимедійного проектора, лабораторні та індивідуальні заняття, робота в групі, реферування, а також методи опитування, тестування тощо.

9. Засоби оцінювання та методи демонстрування результатів навчання

У процесі вивчення дисципліни «Практикум зі спеціальності» використовуються наступні засоби оцінювання та методи демонстрування результатів навчання:

- поточне тестування та поточне опитування;
- підсумкове модульне тестування та опитування за кожним заліковим модулем;
- оцінювання виконання лабораторних робіт;
- оцінювання самостійної роботи;
- оцінювання завдань виконаних на тренінгу;
- екзамен.

10. Критерії, форми поточного та підсумкового контролю

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

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 2	Тренінги	Самостійна робота	Екзамен
Оцінка за даний модуль визначається як середнє арифметичне за захист лабораторних робіт №1-6.	Підсумкове модульне тестування за темами № 1-4.	Оцінка за даний модуль визначається як середнє арифметичне за захист лабораторних робіт № 7-12.	Підсумкове модульне тестування за темами № 5-7.	Оцінка за представлення та захист звіту згідно одного із завдань тренінгу.	Оцінка за звіт про виконаного завдання самостійної роботи.	1. Теоретичні питання: 3 питання по 10 балів. 2. 35 тестів по 2 бали.

Виконання лабораторних робіт:

90-100 балів (Відмінно) - здобувач освіти самостійно, без помилок, виконав усі кроки в рамках лабораторної роботи, правильно задокументував етапи та вільно оперує поняттями та принципами, що відносяться до теми дисципліни.

75-89 балів (Добре) - здобувач освіти виконав завдання лабораторної роботи, проте в процесі виконання допустив кілька дрібних помилок, які не вплинули на кінцевий результат (наприклад, неточна послідовність дій), в процесі роботи виникали додаткові запитання.

60-74 балів (Задовільно) - здобувач освіти виконав завдання лабораторної роботи, але з суттєвими помилками, наприклад, не з першого разу чи не до кінця. Розуміння поставлених у лабораторній роботі завдань є поверхневим та неповним.

1-59 балів (Незадовільно) - здобувач освіти не зміг виконати завдання або результати були повністю невірними. Не продемонстрував базових навичок роботи з програмним забезпеченням.

Підсумкове модульне тестування - вид контролю, при якому засвоєний здобувачем освіти теоретичний та практичний матеріал оцінюється у форматі тестування. Тестування містить 50 запитань кожна правильна відповідь дає 2 бали, максимум 100 балів.

Тренінг:

90-100 балів (Відмінно) - здобувач освіти самостійно, без помилок, виконав завдання, а саме розгорнув обрану систему виявлення та запобігання вторгненням, правильно задокументував усі етапи роботи, та вільно оперує поняттями та принципами дисципліни.

75-89 балів (Добре) - здобувач освіти виконав завдання, а саме розгорнув обрану систему виявлення та запобігання вторгненням, але з дрібними помилками, які не вплинули на результат, в процесі роботи виникали додаткові запитання. Здобувач успішно оформив звіт, який не містить помилок і свідчить про розуміння основних понять та принципів дисципліни.

60-74 балів (Задовільно) - здобувач освіти виконав завдання, а саме розгорнув обрану систему виявлення та запобігання вторгненням, але з суттєвими помилками, наприклад, не з першого разу. Здобувач освіти оформив звіт, який містить незначні помилки, розуміння поставлених у тренінгу завдань є поверхневим.

1-59 балів (Незадовільно) - здобувач освіти не зміг виконати завдання або результати були повністю невірними. Не продемонстрував достатній рівень навичок роботи з програмним забезпеченням, не розуміє основні поняття та принципи дисципліни.

Самостійна робота:

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

75–89 балів (Добре) - 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 (Задовільно) - 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 (Незадовільно) - 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 «Практикум зі спеціальності». Екзаменаційний білет складається з двох блоків.

Перший блок містить три теоретичних запитання, за кожне з яких можна отримати від 0 до 10 балів, що в підсумку дає 30 балів. За відповідь на питання здобувач освіти отримує 6–10 балів, якщо у повному обсязі володіє навчальним матеріалом, всебічно, самостійно та аргументовано відповідає на питання білету і 1–5 балів – якщо володіє навчальним матеріалом не в повному обсязі, доповідає його фрагментарно, допускаючи при цьому неточності.

Другий блок містить 35 тестових завдань. За кожну правильну відповідь тестування здобувач освіти отримує 2 бали, максимум 70 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.	Електронний варіант лекцій	1 - 7
2.	Методичні вказівки до виконання лабораторних робіт (електронний варіант)	1 - 7
3.	Мультимедійний проектор. Комп'ютерна лабораторія. Доступ до Інтернету. Курс мережевої академії Cisco CCNA Cybersecurity Operations.	1 - 7
4.	Oracle VirtualBox, віртуальні машини: CyberOps, Security Onion, Kali Linux, Metasploitable; Cisco Packet Tracer 8.0, Ubuntu Server, OpenSSH, OpenVAS, Wireshark, Nmap, John the Ripper, Snort, Suricata, Zeek, OSSEC, Wazuh, OpenWIPS-NG, Security Onion, Fail2Ban, ClamAV, Elastic Stack (ELK).	1 - 7

Рекомендовані джерела інформації

1. Опорний конспект лекцій з дисципліни «Практикум зі спеціальності» для здобувачів освітньо-професійної програми «Кібербезпека» першого (бакалаврського) рівня вищої освіти спеціальності «Кібербезпека та захист інформації»/ Укл.: Яцків В.В., Кулина С.В. Тернопіль : ЗУНУ, 2025. 41 с.
2. Anu, Vaibhav. Information security governance metrics: A survey and taxonomy. Information Security Journal: A Global Perspective31. 4, 2022. – pp. 466-478.
3. Breaking Down the OSI Model: A Cybersecurity Perspective - DEV ..., – URL: https://dev.to/aditya8raj/breaking-down-the-osi-model-a-cybersecurity-perspective-22ni
4. Cybersecurity Algorithms - Meegle, – URL: https://www.meegle.com/en_us/topics/algorithm/cybersecurity-algorithms
5. Grimes, Roger A. *Hacking Multifactor Authentication*. John Wiley & Sons, 2020.
6. Grubb S. How Cybersecurity Really Works. 2021. – 219 p.
7. 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.
8. ISO 27001 Implementation Phase - Iseo Blue, – URL: https://iseoblue.com/post/iso-27001-implementation-phase/
9. Possible attacks on the TCP/IP protocol stack and countermeasures, – URL: https://securityaffairs.com/117635/security/tcp-ip-protocol-stack-attacks.html
10. Santos, Henrique MD. Cybersecurity: A Practical Engineering Approach. CRC Press, 2022. 341 p.
11. 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
12. Курс мережевої академії Cisco: CCNA Cybersecurity Operations. 2020. Режим доступу. https://www.netacad.com/courses/security/ccna-cybersecurity-operations
13. Про захист інформації в інформаційно-комунікаційних системах - НТФ "Інтес", – URL: https://qdpro.com.ua/document/18462

14. Указ президента України №447/2021 — Офіційне інтернет ..., – URL: https://www.president.gov.ua/documents/4472021-40013