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 «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, КПІЗ (год.)	Самост. робота студ. (год.)	Разом (год.)	Екз. (сем.)
Денна	4	8	30	30	4	12	104	180	8

31.08.2023

Тернопіль – 2023

Робоча програма розроблена на основі освітньо-професійної програми підготовки бакалавра галузі знань 12 «Інформаційні технології» спеціальності 125 «Кібербезпека», затвердженої Вченою радою ЗУНУ (протокол № 10 від 24.06.2020 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 кібербезпеки 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 «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 – 4	Спеціальність 125 «Кібербезпека»	Рік підготовки: Денна: 4 Семестр: Денна: 8
Кількість змістових модулів – 2	Ступінь вищої освіти – бакалавр	Лекції: 30 год. Лабораторні заняття: 30 год.
Загальна кількість годин – 180		Самостійна робота: 104 год. Тренінг, КПІЗ (год.): 12 Індивідуальна робота: 3 год.
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.

Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.).

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

Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

2.4. Передумови для вивчення дисципліни

Перелік дисциплін, які мають бути вивчені раніше: програмування на мові Python; Основи кібернетичної безпеки; Операційні системи; Алгоритми та структури даних; Архітектура комп'ютерів та систем, Оцінка та управління ризиками, Управління інформаційною безпекою, Кібернетична безпека, Криптографія, Технічні засоби захисту інформації.

Перелік раніше здобутих результатів 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.

2.5. Результати навчання.

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

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

Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат.

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

Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації.

Застосовувати різні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик орієнтованому контролі доступу до інформаційних активів.

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».

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».

1.2 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.

Література: 1, 2, 4, 8.

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

Література: 1, 2, 6, 7

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.

Журнал аудиту подій. Політики резервного копіювання даних.

3.4 Моніторинг процесів функціонування ІКС

Джерела інформації про події та типи подій, що аналізуються в системах моніторінгу

Система візуалізації та управління подіями (SIEM)

Аналіз подій

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).

Література: 1, 2, 5, 7.

Тема 4. **Комплексні системи захисту інформації**

4.1 Проєктування, створення, супровід КСЗІ.

Дослідження середовищ функціонування ІС – середовища користувачів, обчислювальної системи, фізичного середовища, інформаційного середовища та побудова моделі загроз.

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

Література: 1, 2, 5, 9.

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.

Література: 1, 2, 7, 9.

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.

Література: 1, 2, 4, 10

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.

Література: 1, 4, 6.

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

		Кількість годин				
	Лекції	Прак-тичні заняття	СРС	ІРС	Тренінг, КПІЗ	Контрольні 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	2	2	12		6	Опитування під час заняття, оцінювання практ. занять
Тема 2. Інформаційні технології в інформаційній та/або кібербезпеці	4	4	12			
Тема 3. Безпека інформаційно-комунікаційних систем	6	6	20			
Тема 4. Комплексні системи захисту інформації	4	4	12	2		
Змістовий модуль 2. Управління інформаційною та / або кібербезпекою						
Тема 5. Управління інформаційною та / або кібербезпекою	4	4	14		6	Опитування під час заняття, оцінювання практ. занять
Тема 6. Криптографічний захист інформації	6	6	20	2		
Тема 7. Технічний захист інформації	4	4	14			
Разом	30	30	104	4	12	

5. Тематика практичних (семінарських або лабораторних) занять

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

Література: 1, 2.

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

Література: 1, 2.

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

Література: 1, 2.

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

Література: 1, 2.

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

Література: 1, 2.

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

Література: 1, 2.

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

Література: 1, 2.

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

Література: 1, 2.

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.

Література: 1, 2.

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.

Література: 1, 2.

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.

Література: 1, 2.

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

Література: 1, 2.

6. Комплексне практичне індивідуальне завдання

Варіанти КПІЗ з дисципліни «**Кібернетична безпека**»

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

1.1 Постановка задачі.
1.2 Збір інформації та пошук цілей.
1.3 Визначення структури системи
1.4 Розробка правил
1.5 Дослідження роботи системи.
1.6 Висновки.

7. Самостійна робота

№ п/п	Тематика
1	Елементи центру моніторингу та управління безпекою. SOC
2	Технології в SOC
3	Корпоративний SOC і послуги з управління інформаційною безпекою
4	Безпека кінцевих пристроїв.
5	Захист від шкідливого ПЗ на рівні хоста.
6	Захист від шкідливого ПЗ на рівні мережі.
7	Рішення для захисту від складного шкідливого програмного забезпечення Cisco AMP.
8	Міжмережеві екрани на рівні хоста.
9	Виявлення аномалій мережі
10	Перевірка мережі на уразливості
11	Загальна система оцінки вразливостей (Common Vulnerability Scoring System, CVSS). 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.

8. Організація та проведення тренінгу з дисципліни

№ п/п	Вид роботи	Порядок проведення тренінгу
1	Підготовка обладнання та ПЗ	Встановлення програмного забезпечення
2	Налаштування програмного забезпечення	Налаштуйте syslog на брандмауері PfSense Налаштування Windows 2003 Server для аудиту
3	Виявлення атак на сервер	Налаштування Snort для виявлення атак на веб-сервер. Налаштуйте Splunk у Windows 2008 для отримання журнали аудиту 2003, сповіщення Snort і системний журнал PfSense

9. Засоби оцінювання та методи демонстрування результатів навчання

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

- стандартизовані тести;
- поточне опитування;
- залікове модульне тестування та опитування;
- презентації результатів виконаних завдань та досліджень;
- оцінювання результатів КПІЗ;
- завдання на лабораторному обладнанні, тренажерах, реальних об'єктах тощо;
- ректорська контрольна робота;
- 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:

Для екзамену

Заліковий модуль 1	Заліковий модуль 2	Заліковий модуль 3	Заліковий модуль 4
20%	20%	20%	40%
1. Усне опитування на заняттях – max 4*6=24 бали. 2. Письмова робота – max 52 балів. 3. Практичне завдання – max 6*4=24 бали	1. Усне опитування на заняттях – max 2*10=20 балів. 2. Письмова робота – max 56 балів. 3. Практичне завдання – max 6*4=24 бали	1. Підготовка КПІЗ – max 30 балів. 2. Захист КПІЗ – max 40 балів. 3. Оцінка за тренінг – max 30 балів	1. Розв'язання 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 - 14
2.	Комп'ютерна лабораторія. Доступ до Інтернету. Курс мережевої академії Cisco CCNA Cybersecurity Operations.	1 - 14
3.	Oracle VirtualBox, віртуальні машини: CyberOps, Security Onion, Kali Linux, Metasploitable; Cisco Packet Tracer 8.0, Ubuntu Server, OpenSSH, OpenVAS, Wireshark, Nmap, John the Ripper.	1 - 14

РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

1. 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
2. Курс мережевої академії Cisco: CCNA Cybersecurity Operations. 2020. Режим доступу. https://www.netacad.com/courses/security/ccna-cybersecurity-operations
3. Інформаційна безпека. // Яковенко Є., Журавель І., Горбатий І., Бондарєв А. Видавництво Львівська політехніка, 2019. – 580.
4. Anu, Vaibhav. Information security governance metrics: A survey and taxonomy. Information Security Journal: A Global Perspective31. 4, 2022. – pp. 466-478.
5. 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
6. Santos, Henrique MD. Cybersecurity: A Practical Engineering Approach. CRC Press, 2022. – 341 p.
7. Grubb S. How Cybersecurity Really Works. 2021. – 219 p.
8. Grimes, Roger A. *Hacking Multifactor Authentication*. John Wiley & Sons, 2020.
9. Maurushat, Alana. *Ethical hacking*. University of Ottawa Press, 2019.
10. Cisar, P., & Pinter, R. Some ethical hacking possibilities in Kali Linux environment. *Journal of Applied Technical and Educational Sciences*, *9*(4), 2019, pp.129-149.
11. Teixeira, D. Metasploit Penetration Testing Cookbook - Third Edition. Packt Publishing Ltd. 2018.
12. Stallings, W. Effective Cybersecurity: Understanding and Using Standards and Best Practices. Addison-Wesley. 2019. – 893 p.
13. Warsinske, J., Graff, M., Henry, K., Hoover, C., Malisow, B., Murphy, S., & Vasquez, M. The Official (ISC) 2 Guide to the CISSP CBK Reference. John Wiley & Sons. 2019. – 928 c.