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

Затверджую
Декан факультету комп'ютерних інформаційних технологій

_____ Ігор ЯКИМЕНКО
"_28_" ___08___ 2025р.

Затверджую
Проректор з науково-педагогічної роботи

_____ Віктор ОСТРОВЕРХОВ
"_29_" _____ 2025 р.

РОБОЧА ПРОГРАМА

з дисципліни

«ОЦІНКА ТА УПРАВЛІННЯ РИЗИКАМИ»

ступінь вищої освіти – **бакалавр**

галузь знань – 12 Інформаційні технології

спеціальність – **125 «Кібербезпека та захист інформації»**

освітньо-професійна програма – **Кібербезпека**

Кафедра кібербезпеки

Форма навчання	Курс	Семестри	Лекції (год.)	Лабораторні роботи (год.)	ІРС (год.)	Тренінг (год)	СРС, (год)	Разом (год.)	Екзамен, семестр
Денна	3	5	30	30	4	8	78	150	5

29.08.2025

Тернопіль - 2025

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

Робочу програму склав доктор технічних наук, професор, професор кафедри кібербезпеки Роман ПАСІЧНИК

Робоча програма затверджена на засіданні кафедри кібербезпеки, протокол №1 від 26. 08. 2025 р.

Завідувач кафедри кібербезпеки _____ Василь ЯЦКІВ

Гарант освітньо-професійної програми _____ Михайло КАСЯНЧУК

СТРУКТУРА РОБОЧОЇ ПРОГРАМИ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

1. Опис дисципліни “Оцінка та управління ризиками ”

Дисципліна “Оцінка та управління ризиками”	**Галузь знань, спеціальність, СВО**	**Характеристика навчальної дисципліни**
Кількість кредитів – 5	галузь знань – 12 Інформаційні технології	**Статус дисципліни** Обов’язкова **Мова навчання** українська
Кількість залікових модулів – 5	5	Рік підготовки: *3* Семестр: *5*
Кількість змістових модулів – 2	ступінь вищої освіти – бакалавр	Лекції (год): *30* Лабораторні заняття (год): 30
Загальна кількість годин – 150		Самостійна робота (год): 78 Тренінг (год.): денна – 8 год. Індивідуальна робота (год): 4.
Тижневих годин –10, з них аудиторних – 4		Вид підсумкового контролю – екзамен

2. Мета й завдання вивчення дисципліни “Оцінка та управління ризиками”

2.1. Мета вивчення дисципліни

Мета вивчення дисципліни “Оцінка та управління ризиками” полягає у формуванні у майбутніх спеціалістів умінь та компетенцій для забезпечення ефективної оцінки ризиків та управління ними у кібербезпеці, необхідних для подальшої роботи, навчити їх застосуванню методів та засобів оцінки ризиків та управління ними у кібербезпеці в умовах широкого використання сучасних інформаційних технологій.

Вивчення курсу “Оцінка та управління ризиками» передбачає наявність систематичних та ґрунтовних знань із суміжних курсів («Теорія ймовірностей та математична статистика», „Основи кібербезпеки”, «Дискретна математика», «Математичний аналіз»), а також цілеспрямованої роботи на лекційних та лабораторних заняттях, самостійної роботи студентів.

2.2. Завдання вивчення дисципліни

В результаті вивчення курсу „Оцінка та управління ризиками ” студенти повинні:

– засвоїти основні фундаментальні поняття і закони теорії ризиків для їх використання в сучасних кіберсистемах;

– знати принципи побудови алгоритмів оцінки ризиків та управління ними у кібербезпеці, основних стандартів оцінки ризиків та їх використання в задачах захисту інформації;

– використовувати основний математичний апарат та закони оцінки та управління ризиками у професійній діяльності;

– вміти використовувати програмні засоби, які реалізують основні функції оцінки та управління ризиками;

– програмно реалізовувати основні алгоритми оцінки та управління ризиками для вирішення типових задач захисту інформації;

– проектувати різного рівня системи оцінки та управління ризиками;

– вміння використовувати методи та засоби оцінки та управління ризиками у кібербезпеці.

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

– здатність застосовувати знання у практичних ситуаціях;

- здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики кібербезпеки та захисту інформації;

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

- здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.

2.4. Передумови для вивчення дисципліни

Вивчення курсу «Оцінка та управління ризиками» передбачає наявність систематичних та ґрунтовних знань із суміжних курсів, таких як «Вища математика», «Теорія ймовірності та математична статистика», «Дискретна математика», «Основи кібербезпеки», «Основи програмування».

2.5. Результати навчання

Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахування вимог до захисту інформації.

Забезпечувати функціонування системи управління кібербезпекою і захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків.

2.6. Завдання лекційних занять

Мета проведення лекцій полягає у тому, щоб ознайомити студентів із головними питаннями курсу «Оцінки та управління ризиками». Завдання проведення лекцій полягає у:

викладенні студентам у відповідності з програмою та робочим планом основних питань курсу «Оцінка та управління ризиками» та формуванні у студентів цілісної системи теоретичних знань з курсу «Оцінка та управління ризиками».

2.7. Завдання проведення лабораторних занять

Мета проведення лабораторних занять полягає у тому, щоб виробити у студентів практичні навички використання теоретичного матеріалу. Завдання проведення лабораторних занять полягає у глибшому засвоєнні та закріпленні теоретичних знань, одержаних на лекціях.

3. Програма навчальної дисципліни «Оцінка та управління ризиками»

Змістовий модуль 1. ***Кількісна оцінка ризиків у кібербезпеці.***

Тема 1. Концепції оцінки ризику.

Принципи підтримки кібербезпеки в бізнесі. Аудит загроз. Необхідність підтримки загальної стратегії забезпечення безперервності. Періодичний перегляд політик і процедур. Кібербезпека та інформаційна безпека. Конфіденційність, цілісність та доступність інформації. Актив. Атака. Експлойт. Поняття ризику. Схильність до ризику. Базові формули оцінки ризиків.

Тема 2. Види інформаційних систем. Активи та загрози.

Системи обробки транзакцій. Системи підтримки прийняття рішень. Системи управління знаннями. Виконавчі інформаційні системи. Системи планування ресурсів підприємства. Географічні інформаційні системи**.** Інформаційні системи моделювання ефективності ключових бізнес-процесів. Інформаційна система ігрового реалістичного захищеного моделювання. Види активів. Апаратні, програмні, інформаційні, нематеріальні активи та персонал. Реєстрація та ідентифікація активів. Автоматизовані системи інвентаризації активів. Ідентифікація загроз. Модель загрози STRIDE. Навколишнє середовище. Бізнес-ресурси. Ворожі суб'єкти. Спуфінг, фішинг, втручання, віцдмова від авторства, розголошення, відмова в обслуговуванні, Ddos- атаки, підвищення привілеїв. Типи загроз.

Тема 3. Системи безпеки та управління ризиками.

Мережева безпека. Міжмережеві екрани фаєрволи.Системи виявлення та запобігання вторгненням (IDS/IPS). Виявлення на основі сигнатур або аномальної поведінки. VPN віртуальні приватні мережі.Шифрування та приховування IP адреси. Безпека кінцевих точок. Антивірусне та антишпигунське програмне забезпечення. Сигнатури, евристичний аналіз, емуляція в пісочниці. EDR – моніторинг та захист кінцевих точок. SOC (Security Operations Center) центри моніторингу та реагування на загрози.

Тема 4. Розробка інноваційного проєкту інформаційної системи

Основні аспекти практичної цінності проєкту. Об'єкт дослідження.Ключові риси інноваційних проєктів. Виявлення протиріччя між існуючими знаннями та напрямком розвитку проєкту. Постановка задачі проєкту та гіпотетичний шлях її розв'язання. Уточнення постановки задачі та методів її розв'язання. Проведення тестових експериментів. Формулювання предмету дослідження із виділенням його наукової новизни. Публікація результатів проєктів.

Тема 5. Системна реалізація проекту розроблення інформаційної системи

Діаграма використання. Діаграма потоків даних (DFD). ER-діаграма бази даних. Фреймворки програмної реалізації систем. Використання Django для реалізації систем. Шаблонізатори Django. CSS фреймворки. Tailwind css. Реалізація інформаційних систем за допомогою Django

Змістовий модуль 2.Проект захищеної інформаційної системи

Тема 6. Моделювання системних подавачів даних

Навчальний проєкт. Середовище розробки pcharm. Інсталяція Django. Формування стартового проєкту. Формування додатку. Тестовий запуск проєкту. Моделі даних локальної бібліотеки. Повторна міграція та тестування моделей.

Тема 7. Системне управління даними

Адміністративна панель. Реєстрація моделей. Створення суперкористувача. Підключення адмінпанелі. Занесення даних у створені відношення. Реєстрація класу ModelAdmin. Налаштування відображення списків. Додавання фільтрів списку. Формування макету з детальним поданням.

Тема 8. Системна візуалізація

Структура проекту Django MVT. Налаштування шаблонів Django. Мова шаблонів Django. Змінні. Теги. Фільтри. Коментарі. Спадкування шаблонів. Структура домашньої сторінки. Базовий шаблон LocalLibrary. Шаблон індексного файлу. Посилання на статичні файли в шаблонах.

Тема 9. Засоби системної безпеки

Вбудовані механізми захисту Django. Захист від SQL-ін'єкцій. Захист від XSS (Cross-Site Scripting). Захист від CSRF (Cross-Site Request Forgery. Безпечне управління сесіями та паролями. Обмеження прав доступу. Валідація вхідних даних. Захист файлів. Ведення журналів та моніторинг. Методи аналізу стійкості. Аналіз вихідного коду. Динамічне тестування. Тестування на проникнення.

Тема 10. Підтримка безпеки інформаційних систем

Архітектура інформаційної системи моделювання із захистом від отруєння даних. Блок збору інформації. Блок вибору даних. Блок моделювання. Блок подання результатів. Реалізація моделі блокчейну. Генерація хеш кодів за допомогою бібліотеки hashlib. Генерація та поповнення ланцюга блоків. Перевірка ланцюга на валідність. Інтеграція з моделюючою системою. Моделююча функція. Додавання результатів моделювання до блокчейну. Контроль достовірності результатів.

4. Структура залікового кредиту дисципліни «Оцінка та управління ризиками»

	Кількість годин					
	Лекції	Практичні заняття	Самостійна робота	Індивідуальна робота	Тренінг	Контрольні заходи
Змістовий модуль 1. Кількісна оцінка ризиків у кібербезпеці						
Тема 1. Концепції оцінки ризику	2	2	8	1	2	Поточне опитування
Тема 2. Види інформаційних систем. Активи та загрози.	2	2	8			
Тема 3. Системи безпеки та управління ризиками.	3	3	8			
Тема 4. Розробка інноваційного проєкту інформаційної системи	3	3	8			
Тема 5. Системна реалізація проекту розроблення інформаційної системи.	3	3	8			
Змістовий модуль 2.Проект захищеної інформаційної системи						
Тема 6. Моделювання системних подавачів даних.	3	3	8	2	3	Поточне опитування
Тема 7. Системне управління даними.	3	3	8			
Тема 8. Системна візуалізація.	3	3	9			
Тема 9. Засоби системної безпеки	3	3	9			
Тема 10. Підтримка безпеки інформаційних систем.	3	3	9			
Разом	30	30	78	4	8	

5. Тематика лабораторних робіт.

Лабораторна робота №1

Тема: Інформаційні активи, атаки та інструментальні засоби.

Мета: Вивчення та дослідження видів інформаційних атак та оцінок ризиків.

Питання для обговорення:

1. Кібербезпека та інформаційна безпека. Конфіденційність, цілісність та доступність інформації.
2. Види активів.
3. Види інформаційних атак. Експлойти.
4. Поняття ризику. Базові формули оцінки ризиків.
5. Встановлення середовища IDLE Python
6. Встановлення середовища Pycharm

Лабораторна робота №2

Тема: Активи та загрози.

Мета: Вивчення, дослідження та моніторинг видів інформаційних загроз.

Питання для обговорення:

1. Ідентифікація загроз. Модель загрози STRIDE.
2. Навколишнє середовище. Бізнес-ресурси. Ворожі суб'єкти.
3. Спуфінг, фішинг, втручання, відмова від авторства, розголошення, відмова в обслуговуванні,
4. Ddos- атаки, підвищення привілеїв.

5. Шкідливе програмне забезпечення: віруси, хробаки, програми-вимагачі, спам, логічна бомба, троянський кінь, завантажувачі, інсталятори, флудери, зомбі, шпигуни, рекламники.
6. Маніпуляції людьми у розкритті конфіденційності, інфраструктурні атаки, внутрішні загрози від інсайдерів.
7. Системи моніторингу загроз: журнали подій, спеціальні державні служби, комерційні та відкриті джерела.

Лабораторна робота №3

Тема: Системи безпеки та управління ризиками.

Мета: Вивчення засобів підтримки інформаційної безпеки.

Питання для обговорення:

1. SIEM (Security Information and Event Management) технологія збору та аналізу гетерогенних даних у режимі реального часу.
2. Комплексна платформа SOAR оркестрації спостережень, автоматизації та реагування на загрози.
3. Системи симетричного та асиметричного шифруввання.
4. Системи управління доступом. Системи контролю версій коду Git.
5. Сканування на наявність вразливостей зовнішнього коду.
6. Управління залежностями. Ідентифікація загроз та визначення вразливостей на етапі проектування систем. Безпечна розробка (Secure Coding).

Лабораторна робота №4

Тема: Розробка інноваційного проєкту інформаційної системи

Мета: Вивчення методів проведення та публікації результатів інноваційного , дослідження .

Питання для обговорення:

1. Аналіз публікації щодо інноваційного проєкту. Захищена модель урожайності зернових культур на основі максимальних значень кумулятивних вегетаційних індексів.
2. Практична цінність дослідження. Джерело вхідної інформації.
3. Протиріччя існуючого підходу щодо моделювання значень вегетаційних індексів. Огляд літератури.
4. Архітектура інформаційної системи моделювання урожайності зернових із захистом від отруєння даних.
5. Модель динаміки із прогностичними властивостями. Адаптивна модель динаміки вегетаційних індексів.
6. Ідентифікація моделі Моно. Адаптація моделі до специфіки поточних даних.

Лабораторна робота №5

Тема: Системна реалізація проекту розроблення інформаційної системи

Мета: Вивчення засобів проєктування та реалізації розроблених інформаційних систем.

Питання для обговорення:

1. Побудова діаграми використання.
2. Діаграма потоків даних (DFD).
3. ER-діаграма бази даних.
4. Використання Django для реалізації систем.
5. Шаблонізатори Django.
6. CSS фреймворки. Tailwind css.

Лабораторна робота №6

Тема: Моделювання системних подавачів даних

Мета: Вивчення засобів структурування сховищ даних.

Питання для обговорення:

1. Навчальний проєкт. Середовище розробки pcharm.
2. Інсталяція Django. Формування стартового проєкту.
3. Формування додатку проєкту. Тестовий запуск проєкту.
4. Моделі даних локальної бібліотеки.
5. Повторна міграція та тестування моделей.

Лабораторна робота №7

Тема: Системне управління даними

Мета: Вивчення засобів наповнення сховищ та подання даних

Питання для обговорення:

1. Адміністративна панель.
2. Реєстрація моделей. Створення суперкористувача.
3. Підключення адмінпанелі. Занесення даних у створені відношення.
4. Реєстрація класу ModelAdmin.
5. Налаштування відображення списків.
6. Додавання фільтрів списку.
7. Формування макету з детальним поданням.

Лабораторна робота №8

Тема: Системна візуалізація

Мета: Вивчення засобів подання даних у веб-інтерфейсах

Питання для обговорення:

1. Структура проекту Django MVT. Налаштування шаблонів Django.
2. Мова шаблонів Django. Змінні. Теги. Фільтри. Коментарі. Спадкування шаблонів.
3. Структура домашньої сторінки.
4. Базовий шаблон LocalLibrary. Шаблон індексного файлу.
5. Посилання на статичні файли в шаблонах.

Лабораторна робота №9

Тема: Засоби системної безпеки

Мета: Вивчення засобів захисту даних

Питання для обговорення:

1. Вбудовані механізми захисту Django. Захист від SQL-ін'єкцій.
2. Захист від XSS (Cross-Site Scripting).
3. Захист від CSRF (Cross-Site Request Forgery.
4. Безпечне управління сесіями та паролями.
5. Валідація вхідних даних. Захист файлів. Ведення журналів та моніторинг.
6. Методи аналізу стійкості до кібератак. Аналіз вихідного коду.
7. Динамічне тестування. Тестування на проникнення.
8. Система моніторингу потенційних кібернетичних загроз для інформаційних систем.

Лабораторна робота №10

Тема: Підтримка безпеки інформаційних систем

Мета: Програмна реалізація захисту даних засобами блокчейн

Питання для обговорення:

1. Архітектура інформаційної системи із захистом від отруєння даних.
2. Реалізація моделі блокчейну. Генерація хеш кодів за допомогою бібліотеки hashlib.
3. Генерація та поповнення ланцюга блоків.
4. Перевірка ланцюга на валідність.
5. Інтеграція з моделюючою системою.
6. Моделююча функція.
7. Додавання результатів моделювання до блокчейну.
8. Контроль достовірності результатів.

6. Тематика самостійної роботи студентів

Самостійна робота "Розробка захищеної моделюючої інформаційної системи"

Мета роботи: Розробити та реалізувати за допомогою фреймворків захищену моделюючу інформаційну систему

Завдання:

1. Кожен студент вибирає тему своїх проектів самостійно або із запропонованого переліку.
2. На основі обраної теми студент розробляє Веб-проект, який включає:

…- Аналіз актуальності досліджень
- Огляд пов'язаної літератури
….- Постановка задачі проекту
- Аналіз завдань проекту
- Вибір програмних засобів для реалізації проекту
- Ескіз інтерфейсу проекту
- Навчання та тестування моделей спеціалізованого проекту
- Розробка системи захисту інформаційного та програмного забезпечення проекту засобами блокчейн
- Реалізація системи захисту проекту
- Тестування системи захисту
- Висновки та рекомендації для користувачів

3. Студент повинен підготувати звіт, який містить:

- Опис особливостей обраних проектних завдань
- Опис ескізу інтерфейсу проекту
- Детальний опис структури моделей спеціалізованого проекту
- Опис результатів навчання та тестування моделей
- Опис результатів випробовувань системи захисту проекту
- Висновки і рекомендацій для користувачів

Роботу необхідно здати викладачу у вигляді письмового звіту та презентації розробленого додатку. Захист роботи відбувається у формі усної презентації з демонстрацією функціоналу додатку.

Орієнтовна тематика проектів:

1. Система виявлення сонливості водія на основі комп'ютерного зору.
2. Реалізація веб-додатку для визначення захворювання рослин
3. Вебсервіс для підтримки людей із психологічними проблемами.
4. Модель автоматичного виявлення фейкових новин
5. Система бронювання туристичних турів.
6. Система колоризації зображень за допомогою моделі глибокого навчання.
7. Система лінгвістичного аналізу спеціальних термінів
8. Розробка моделі класифікації грального карт за допомогою глибокого навчання.
9. Реалізація веб-додатку для визначення стану розвитку рослин
10. Вебсервіс для підтримки людей із серцево-судинними захворюваннями.
11. Модель автоматичного виявлення повідомлень шкідливого психологічного впливу
12. Система бронювання готельних номерів.
13. Система усунення дефектів зображень за допомогою моделі глибокого навчання.
14. Система лінгвістичного аналізу текстів на історичну тематику
15. Розробка моделі класифікації зображень спеціальної техніки за допомогою глибокого навчання
16. Реалізація веб-додатку для визначення фази розвитку рослин
17. Вебсервіс для підтримки людей із захворюваннями ендокринної системи.
18. Модель автоматичного виявлення повідомлень недобросовісного рекламування продукції
19. Система бронювання відпочинкових об'єктів.
20. Система лінгвістичного аналізу текстів на військову тематику

7. Організація та проведення тренінгу з дисципліни «Оцінка та управління ризиками»

Тематика тренінгу: реалізація інформаційних систем

Цей тренінг охоплює ключові аспекти реалізації веб-проектів із використанням фреймворків на посилення проектів самостійної роботи. Учасники отримають досвід роботи із методологіями проектування та реалізації інформаційних систем.

Мета тренінгу: Забезпечити учасників теоретичними знаннями та практичними навичками в галузі реалізації Веб-проектів.

Перелік завдань для тренінгу:

1. Аналіз особливостей розроблюваних проектів
2. Відбір програмних засобів для підтримки процесу реалізації проекту.
3. Аналіз переваг та недоліків використання фреймворку Django у реалізації загальних проектів
4. Аналіз переваг та недоліків використання фреймворку Tensor Flow у реалізації проектів із розпізнавання зображень
5. Програмна реалізація завдання на посилення розроблюванрго проекту із самостійної роботи

Ці завдання дозволять студентам отримати практичний досвід формування проектів інформаційних систем із використанням фреймворків.

Порядок проведення тренінгу:

Вступна частина проводиться з метою ознайомлення студентів із запропонованими завданнями тренінгу.

Організаційна частина полягає у створенні робочого настрою у колективі студентів.
Практична частина реалізується шляхом виконання завдання на посилення проекту із самостійної роботи.

Підведення підсумків. Обговорення результатів виконаних завдань. Обмін думками з питань, що виносились на тренінг.

8. Методи навчання.

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

9. Засоби оцінювання та методи демонстрування результатів навчання

У процесі вивчення дисципліни “Оцінка та управління ризиками” використовуються наступні методи оцінювання навчальної роботи студента:

– поточне опитування;
– підсумковий модульний контроль за кожним змістовним модулем;
– оцінювання лабораторних завдань;
– оцінювання тренінгів;
– оцінювання результатів самостійної роботи;
– підсумковий екзамен.

10. Політика оцінювання

Політика щодо дедлайнів і перескладання. Для виконання усіх видів завдань студентами 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 студент може користуватися лише дозволеними допоміжними матеріалами або засобами, йому забороняється в будь-якій формі обмінюватися інформацією з іншими студентами, 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 "Оцінка та управління ризиками" визначається як середньозважена величина, в залежності 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 результати отримані у ході виконання даборатор-них робіт №1-5.	Підсумкова письмова робота за темами №1-5.	Оцінка за даний модуль визначається як середнє за результати отримані у ході виконання даборатор-них робіт №6-10.	Підсумкова письмова робота за темами №6-10.	Визначається як середнє арифметичне за виконання завдань №1-5 тренінгу.	Оцінка за виконаний і представлений звіт із оброблення отриманих даних	1. Теоре-тична частина: 2 запи-тання по 20 балів (максимум40 балів) 2. Прак-тична частина 2 задачі по 30 балів кожна (60 балів).

Поточне оцінювання під час заняття:

90–100 балів – у повному обсязі володіє навчальним матеріалом, вільно, самостійно та аргументовано його викладає під час відповідей, глибоко та всебічно розкриває зміст теоретичних питань;

75–89 балів – достатньо повно володіє навчальним матеріалом, але при викладанні деяких питань не вистачає достатньої глибини та аргументації, допускаються при цьому окремі несуттєві неточності та незначні помилки;

65–74 бали – в цілому володіє навчальним матеріалом та викладає його основний зміст, але без глибокого всебічного аналізу, обґрунтування та аргументації, допускаючи при цьому окремі суттєві неточності та помилки;

60–64 бали – не в повному обсязі володіє навчальним матеріалом, фрагментарно (без аргументації та обґрунтування) його викладає, недостатньо розкриває зміст теоретичних питань, допускаючи при цьому суттєві неточності;

1–59 балів – не володіє навчальним матеріалом, не розкриває зміст теоретичних питань. Підсумкова оцінка за поточне опитування кожного модуля визначається як середнє арифметичне оцінок, отриманих під час занять в межах кожного модуля.

Тренінг:

90–100 балів – у повному обсязі володіє навчальним матеріалом, вільно самостійно та аргументовано його використовує під час розв'язування задач тренінгу;

75–89 балів – достатньо повно володіє навчальним матеріалом, але при розв'язуванні окремих задач тренінгу не вистачає достатньої глибини та аргументації його використання, допускаються при цьому окремі несуттєві неточності та незначні помилки;

65–74 бали – в цілому володіє навчальним матеріалом та загалом його використовує при розв'язування задач тренінгу, але без глибокого всебічного аналізу, обґрунтування та аргументації, допускаючи при цьому суттєві неточності та помилки;

60–64 бали – не в повному обсязі володіє навчальним матеріалом, фрагментарно (без аргументації та обґрунтування) його використовує, частково розв'язуючи задачі тренінгу, допускаючи при цьому суттєві неточності;

1–59 – не володіє навчальним матеріалом, не розв'язує задачі тренінгу, не бере участі у колективних завданнях підчас проведення тренінгу.

Самостійна робота:

90–100 балів – зміст та захист звіту свідчить про високий рівень опанування навчального матеріалу, реферат містить елементи самостійного дослідження, студент на високому рівні виявляє творчий підхід до виконання завдань;

75–89 балів – зміст та захист звіту загалом свідчить про належний рівень опанування навчального матеріалу, можуть бути несуттєві недопрацювання, студент належно виявляє творчий підхід до виконання завдань;

60–74 балів – поставлені завдання виконані на недостатньому рівні; наведені авторські напрацювання є загальними і слабко обґрунтованими, свідчать про недостатній рівень опанування навчального матеріалу; студент припускається значних помилок у виконанні завдань, в окремих моментах виявляє творчий підхід до виконання завдань;

1–59 балів – завдання практично не виконані; відсутні авторські напрацювання; грубі помилки у вирішенні завдань роботи, що свідчать про низький рівень опанування навчального матеріалу; студент не виявляє творчого підходу до виконання завдань.

Модульна робота, екзамен – види контролю, при яких засвоєння студентом теоретичного та практичного матеріалу оцінюється від 0 до 100 балів як сума балів за виконані завдання. Екзаменаційний білет складається з двох теоретичних питань, за кожне з яких можна отримати від 0 до 20 балів, що в підсумку дає максимально 40 балів, та двох практичних задач, за які можна отримати від 0 до 60 балів. За теоретичне питання студент отримує 10–20 балів, якщо у повному обсязі володіє навчальним матеріалом, всебічно, самостійно та аргументовано його викладає під час відповіді, глибоко та всебічно розкриває зміст завдання, і 1–10 балів – якщо в цілому володіє навчальним матеріалом, але не в повному обсязі, фрагментарно (без аргументації та обґрунтування) його викладає, недостатньо розкриває зміст завдання, допускаючи при цьому суттєві неточності, відповіді на запитання нечіткі. За практичні задачі студент отримує 20–30 балів, якщо у повному обсязі володіє навчальним матеріалом, правильно розв'язує практичну задачу і інтерпретує отримані результати, демонструє самостійність виконання; 10–20 балів – у достатньому обсязі володіє навчальним матеріалом, правильно розв'язує практичну задачу, але на додаткові контрольні запитання відсутня повна відповідь, допускає несуттєві неточності та фрагментарно (без аргументації) інтерпретує отримані результати, демонструє самостійність виконання; 1–9 балів – не в повному обсязі володіє матеріалом, фрагментарно розв'язує практичне завдання, допускає суттєві неточності, поверхнево його викладає, недостатньо розкриває зміст поставлених питань.

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	Електронний варіант лекцій	1 - 10
2	Методичні вказівки до виконання лабораторних робіт (електронний варіант)	1 - 10
3	Мультимедійний проектор	1 - 10
4	Проекційний екран	1 - 10
5	Комунікаційне програмне забезпечення (Internet Explorer, Google Chrome, Firefox).	1 - 10
6	Наявність доступу до мережі Internet	1 - 10
7	Комунікаційне програмне забезпечення (Zoom) для проведення занять у режимі он-лайн (за необхідності).	1 - 10
8	ПК Intel Core i3-540; монітор 19 Samsung; принтер лазерний Canon MF4570.	1 - 10
9	IDLE Python, Pycharm, спеціалізовані бібліотеки Python, фреймворк Django	1-10

РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

1. Лісовська Ю. Кібербезпека. Ризики та заходи. – К.: Кондор, 2019. – 272 с.
2. Курс мережевої академії Cisco: Управління загрозами у кібербезпеці 2024. Режим доступу: https://www.netacad.com/courses/cyber-threat-management?courseLang=uk-UA
3. Stallings, W. Effective Cybersecurity: Understanding and Using Standards and Best Practices. Addison-Wesley. 2019. – 893 p.
4. NIST. Framework for Improving Critical Infrastructure Cybersecurity. April 16, 2018. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST. CSWP.04162018.pdf
5. Fagan M, Marron, J, Brady KG, Jr, Cuthill BB, Megas KN, Herold R (2021) IoT Device Cybersecurity Guidance for the Federal Government: IoT Device Cybersecurity Requirement Catalog. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-213A. https://doi.org/10.6028/NIST.SP.800-213A
6. Stine K, Quinn S, Witte G, Gardner R (2020) Integrating Cybersecurity and Enterprise Risk Management (ERM). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8286. https://doi.org/10.6028/NIST.IR.8286

7. Soni, Arun. The Cybersecurity Self-Help Guide. CRC Press, 2021.
8. Ulven, J.B.; Wangen, G. A Systematic Review of Cybersecurity Risks in Higher Education. Future Internet, 2021,13,39. https://doi.org/ 10.3390/fi13020039
9. ISO 31010 2019. Risk management -Risk assessment techniques. Management du risque -Techniques. – 268 p.
10. Wangen, G. Quantifying and Analyzing Information Security Risk from Incident Data; Graphical Models for Security; Albanese, M., Horne, R., Probst, C.W., Eds.; Springer International. Publishing: Cham, Switzerland, 2019, pp. 129–154.
11. Radanliev P., et al. "Cyber Risk in IoT Systems." (2019).
12. Lee, In. "Internet of Things (IoT) cybersecurity: Literature review and IoT cyber risk management." Future Internet 12.9, 2020: 157.
13. Wilhelmsen, Cheryl A., and Lee T. Ostrom. Risk assessment: tools, techniques, and their applications. John Wiley & Sons, 2019.
14. Fagan, Michael, et al. "IoT Device Cybersecurity Guidance for the Federal Government." NIST Special Publication 800 (2021): 213.
15. Burnap, Pete. "Risk Management & Governance Knowledge Area Issue." (2021). Version 1.1.1. https://www.cybok.org/media/downloads/Risk_Management_Governance_v1.1.1.pdf
16. Django. Tutorials Point. 2015. // https://www.tutorialspoint.com/django/django_tutorial.pdf.
17. Django Tutorial: The Local Library website // https://developer.mozilla.org/en-US/docs/Learn/Server-side/Django/Tutorial_local_library_website
18. Roman Pasichnyk, Ludmila Babala, Mykhaylo Machulyak, Yurii Yakymenko. Modeling Vegetation Index Dynamics in GIS Based on Remote Observations. 2025. 7pp., https://ceur-ws.org/Vol-3974/short03.pdf
19.