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.

ЗАТВЕРДЖУЮ:
Директор Навчально-наукового інституту новітніх освітніх технологій
_____ Святослав ПИТЕЛЬ
«29» 08 2025 р.

РОБОЧА ПРОГРАМА

з дисципліни «Безпека хмарних сервісів»
ступінь вищої освіти – бакалавр
галузь знань – 12 Інформаційні технології
спеціальність – 123 Комп'ютерна інженерія
освітньо-професійна програма – Комп'ютерна інженерія

Кафедра кібербезпеки

Форма навчання	Курс	Семестр	Лекції (год.)	Лабор. заняття (год.)	ІРС (год.)	Тренінг (год.)	СРС (год.)	Разом (год.)	Залік (семестр)
Денна	4	7	30	14	3	6	97	150	7
Заочна	4	7,8	8	4	-	-	138	150	8

29.08.2025

Тернопіль – 2025

Робочу програму склала доцент кафедри кібербезпеки, к.е.н., Людмила БАБАЛА.

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

Завідувач кафедри  Василь ЯЦКІВ

Гарант ООП  Леся ДУБЧАК

СТРУКТУРА РОБОЧОЇ ПРОГРАМИ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«Безпека хмарних сервісів»

1. Опис дисципліни «Безпека хмарних сервісів»

Дисципліна – Безпека хмарних сервісів	Галузь знань, спеціальність, СВО	Характеристика навчальної дисципліни
Кількість кредитів ECTS 5	**Галузь знань –** 12 «Інформаційні технології»	Вибіркова дисципліна, мова навчання - *українська*
Кількість залікових модулів - 3	**Спеціальність –** 125 «Кібербезпека»	*Денна:* Рік підготовки:4 Семестр – 7 *Заочна:* Рік підготовки:4 Семестр – 7,8
Кількість змістових модулів - 2	Ступінь вищої освіти – бакалавр	*Денна:* лекції – 30 год.; лабор.- 14 год; *Заочна:* лекції – 8 год.; лабор.- 4 год;
Загальна кількість годин - 150		*Денна:* Самостійна робота: 97 *год.,* Тренінг – 6 год. Індивідуальна робота : 3 *год.* *Заочна:* Самостійна робота: 138 *год*
Тижневих годин: 10 год., з них аудиторних – 3 год		Вид підсумкового контролю – *залік*

2. **Мета й завдання вивчення дисципліни** «Безпека хмарних сервісів»

1.1. Мета вивчення дисципліни:

Метою викладання дисципліни «Безпека хмарних сервісів» є формування у здобувачів комплексного розуміння сучасних методів та технологій забезпечення кібербезпеки, з особливим акцентом на хмарні технології, методи розвідки відкритих джерел (OSINT) та практичний аналіз державних реєстрів для забезпечення інформаційної безпеки.

1.2. Завдання вивчення дисципліни:

В результаті вивчення курсу «Безпека хмарних сервісів» здобувачі повинні:

знати:

- Основні концепції кібербезпеки та типи сучасних кіберзагроз;
- Принципи роботи та архітектуру хмарних технологій з точки зору безпеки;
- Методи виявлення та запобігання вторгненням у хмарних середовищах;
- Концепції управління ідентифікацією та доступом у хмарних сервісах;
- Основи криптографії та методи шифрування даних у хмарних сховищах;
- Методології та інструменти розвідки відкритих джерел (OSINT);
- Структуру та принципи роботи державних електронних реєстрів України;
- Методології тестування на проникнення та аналізу вразливостей хмарних систем;
- Процеси реагування на інциденти та управління безпекою в хмарному середовищі;
- Ключові нормативні вимоги та стандарти у сфері кібербезпеки;

- Техніки аналізу та верифікації інформації з відкритих джерел для задач кібербезпеки.

вміти:

- Аналізувати та оцінювати кіберзагрози в сучасному цифровому середовищі;
- Налаштовувати та управляти системами виявлення та запобігання вторгнень у хмарних інфраструктурах;
- Впроваджувати ефективні стратегії управління ідентифікацією та доступом;
- Застосовувати методи шифрування та управління ключами для захисту даних у хмарі;
- Проводити OSINT-дослідження для виявлення кіберзагроз та збору інформації;
- Здійснювати аналіз державних електронних реєстрів для забезпечення безпеки та верифікації даних;
- Проводити аналіз вразливостей та тестування на проникнення в хмарних системах;
- Розробляти та впроваджувати плани реагування на інциденти кібербезпеки;
- Забезпечувати відповідність хмарних сервісів нормативним вимогам та проводити аудит безпеки;
- Використовувати результати аналізу державних реєстрів та OSINT-даних для моніторингу та прогнозування кіберзагроз.

3. **Програма дисципліни «Безпека хмарних сервісів»**

Змістовий модуль 1 – Основи кібербезпеки та захист даних у хмарних середовищах

Тема 1. Сучасні загрози в хмарному середовищі

- Типи загроз в хмарному середовищі(віруси, фішинг, ransomware тощо);
- Вектори атак та методи їх виявлення у хмарному середовищі;
- Базові принципи захисту інформації у хмарному середовищі;
- Роль людського фактору в кібербезпеці.

Тема 2. Хмарні технології та їх роль у забезпеченні кібербезпеки підприємств

- Огляд моделей хмарних послуг (IaaS, PaaS, SaaS);
- Переваги та ризики використання хмарних технологій;
- Архітектура безпеки в хмарі;
- Розподіл відповідальності між провайдером та клієнтом;
- Стратегії мінімізації ризиків у хмарному середовищі.

Тема 3. Системи виявлення та запобігання вторгнень (IDS/IPS) в хмарних інфраструктурах

- Принципи роботи IDS/IPS;
- Особливості впровадження IDS/IPS у хмарному середовищі;
- Аналіз мережевого трафіку та виявлення аномалій;
- Налаштування та управління правилами IDS/IPS;
- Інтеграція з іншими системами безпеки.

Тема 4. Управління ідентифікацією та доступом (IAM) у хмарних середовищах

- Концепції IAM у хмарних сервісах;
- Методи автентифікації та авторизації;
- Управління привілеями та ролями;
- Федеративний доступ та Single Sign-On (SSO);
- Моніторинг та аудит доступу.

Тема 5. Шифрування даних та управління ключами в хмарних сховищах

- Основи криптографії у хмарних середовищах;
- Шифрування даних у стані спокою та під час передачі;
- Управління життєвим циклом ключів;
- Технології захисту ключів (HSM, KMS);
- Відповідність регуляторним вимогам щодо шифрування.

Змістовий модуль 2 – Розробка, безпека та управління хмарними додатками

Тема 6. Розвідка відкритих джерел (OSINT) у кібербезпеці

- Основи методології OSINT та її застосування в кібербезпеці;
- Інструменти та техніки збору інформації з відкритих джерел;

- Аналіз соціальних мереж та цифрових слідів для виявлення загроз;
- Верифікація та валідація інформації з відкритих джерел;
- Етичні та правові аспекти OSINT-діяльності.

Тема 7. Аналіз державних електронних реєстрів України

- Структура та функціонування державних електронних реєстрів;
- Методи доступу до публічної інформації реєстрів (API, веб-інтерфейси);
- Аналіз даних ЄДРПОУ, реєстру нерухомості, судових рішень;
- Виявлення аномалій та підозрілих активностей через аналіз реєстрів;
- Інтеграція даних з різних державних джерел для комплексного аналізу.

Тема 8. Реагування на інциденти та управління безпекою в хмарних середовищах

- Створення плану реагування на інциденти для хмарних систем;
- Виявлення та класифікація інцидентів безпеки;
- Процеси розслідування та аналізу інцидентів у хмарі;
- Інструменти та платформи для управління безпекою в хмарі.

Тема 9. Відповідність нормативним вимогам та аудит безпеки хмарних сервісів

- Огляд ключових стандартів та регуляторних вимог (GDPR, український закон про персональні дані);
- Проведення аудиту безпеки хмарних сервісів;
- Управління ризиками та відповідністю;
- Документування та звітність з питань безпеки;
- Співпраця з хмарними провайдерами щодо відповідності вимогам.

Тема 10. Практичний аналіз кіберзагроз через державні реєстри та OSINT

- Побудова профілів потенційних зловмисників через публічні дані;
- Відстеження фінансових операцій та корпоративних зв'язків;
- Створення інструментів моніторингу на основі аналізу реєстрів;
- Автоматизація збору та аналізу даних з державних джерел;
- Розробка звітів та дашбордів для візуалізації результатів аналізу

4. Структура залікового кредиту дисципліни «Безпека хмарних сервісів»

4.1. Структура залікового кредиту дисципліни «Безпека хмарних сервісів» для ДФН

Кількість годин						
Тематика	Лекції	Лабор. заняття	Самост.робота	Індив. робота	Тренінг	Контр. заходи
Змістовий модуль 1 – Основи кібербезпеки та захист даних у хмарних середовищах						
Тема 1. Сучасні загрози в хмарному середовищі	3	1	9	1	3	Поточне опитува-ння
Тема 2. Хмарні технології та їх роль у забезпеченні кібербезпеки підприємств	3	2	10			
Тема 3. Системи виявлення та запобігання вторгнень (IDS/IPS) в хмарних інфраструктурах	3	1	10			
Тема 4. Управління ідентифікацією та доступом (IAM) у хмарних середовищах	3	1	9			
Тема 5. Шифрування даних та управління ключами в хмарних сховищах	3	2	10			
Змістовий модуль 2 – Розробка, безпека та управління хмарними додатками						
Тема 6. Розвідка відкритих джерел (OSINT) у	3	1	10			

кібербезпеці				2	3	Поточне опитува-ння
Тема 7. Аналіз державних електронних реєстрів України	3	2	9			
Тема 8. Реагування на інциденти та управління безпекою в хмарних середовищах	3	1	10			
Тема 9. Відповідність нормативним вимогам та аудит безпеки хмарних сервісів	3	2	10			
Тема 10. Практичний аналіз кіберзагроз через державні реєстри та OSINT	3	1	10			
Разом	**30**	**14**	**97**	**3**	**6**	

4.2. Структура залікового кредиту дисципліни «Безпека хмарних сервісів» для ЗФН

	Кількість годин			
	Лекції	Практи-чні заняття	Самостій-на робота	Контро-льні заходи
Тема 1. Сучасні загрози в хмарному середовищі. Хмарні технології та їх роль у забезпеченні кібербезпеки підприємств. Системи виявлення та запобігання вторгнень (IDS/IPS) в хмарних інфраструктурах	2	1	35	Поточне опитування
Тема 2. Управління ідентифікацією та доступом (IAM) у хмарних середовищах. Шифрування даних та управління ключами в хмарних сховищах	2	1	34	
Тема 3. Розвідка відкритих джерел (OSINT) у кібербезпеці. Аналіз державних електронних реєстрів України. Реагування на інциденти та управління безпекою в хмарних середовищах	2	1	35	
Тема 4. Відповідність нормативним вимогам та аудит безпеки хмарних сервісів. Практичний аналіз кіберзагроз через державні реєстри та OSINT	2	1	34	
Разом	**8**	**4**	**138**	

5. Тематика лабораторних занять

Тематика лабораторних занять для ДНФ

Лабораторне робота 1: Аналіз та оцінка ризиків у хмарному середовищі

- Проведення аналізу потенційних загроз для конкретного хмарного сценарію;
- Оцінка вразливостей та їх потенційного впливу;
- Розробка стратегії мінімізації ризиків.

Лабораторне робота 2: Налаштування та тестування IDS/IPS у хмарній інфраструктурі

- Встановлення та конфігурація IDS/IPS у хмарному середовищі;

- Створення та налаштування правил виявлення;
- Проведення симуляції атак та аналіз ефективності системи.

Лабораторне робота 3: Управління ідентифікацією та доступом у хмарі

- Налаштування IAM-політик у хмарному сервісі;
- Впровадження багатофакторної автентифікації;
- Створення та управління ролями з різними рівнями доступу.

Лабораторне робота 4: Основи OSINT та збір інформації з відкритих джерел

- Використання базових OSINT-інструментів (Maltego, Shodan, Google Dorking);
- Аналіз соціальних мереж для виявлення інформаційних витоків;
- Складання профілю організації через публічно доступні дані.

Лабораторне робота 5: Аналіз державних електронних реєстрів України

- Робота з API державних реєстрів (ЄДРПОУ, OpenDataBot);
- Пошук та аналіз корпоративних зв'язків через реєстр юридичних осіб;
- Виявлення аномальних фінансових операцій через відкриті дані.

Лабораторне робота 6: Комплексне OSINT-розслідування кіберзагроз

- Побудова карти зв'язків потенційних кіберзлочинців;
- Аналіз цифрових слідів через поєднання державних реєстрів та соціальних мереж;
- Створення звіту про результати розслідування з рекомендаціями.

5.2. Тематика лабораторних занять для ЗНФ

. **Лабораторна робота 1: Комплексний аналіз безпеки хмарного середовища та основи OSINT**

- Проведення аналізу потенційних загроз для конкретного хмарного сценарію;
- Оцінка вразливостей та їх потенційного впливу;
- Розробка стратегії мінімізації ризиків;
- Використання базових OSINT-інструментів (Google Dorking, Shodan, соціальні мережі);
- Аналіз соціальних мереж для виявлення інформаційних витоків;
- Складання профілю організації через публічно доступні дані.

Лабораторна робота 2: Управління безпекою в хмарі та аналіз українських державних реєстрів

- Налаштування IAM-політик у хмарному сервісі;
- Впровадження багатофакторної автентифікації;
- Створення та управління ролями з різними рівнями доступу;
- Робота з API державних реєстрів (ЄДРПОУ, OpenDataBot);
- Пошук та аналіз корпоративних зв'язків через реєстр юридичних осіб;
- Виявлення аномальних фінансових операцій через відкриті дані;
- Побудова карти зв'язків потенційних кіберзлочинців;
- Аналіз цифрових слідів через поєднання державних реєстрів та соціальних мереж;
- Створення звіту про результати розслідування з рекомендаціями.

6. Самостійна робота

«Комплексний OSINT-аналіз кіберзагроз для підприємства з використанням державних реєстрів»

Мета роботи: Провести комплексний аналіз кіберзагроз для конкретного підприємства з використанням методів OSINT та аналізу державних електронних реєстрів України.

Завдання:

Вибір об'єкта дослідження Кожен здобувач обирає реальне українське підприємство (з публічно доступною інформацією) для проведення OSINT-аналізу.

Проведення комплексного аналізу:

- Збір базової інформації про підприємство через державні реєстри (ЄДРПОУ, відкриті дані);
- Аналіз корпоративної структури та бенефіціарних власників;
- Дослідження цифрового сліду компанії в мережі Інтернет;
- Виявлення потенційних точок вразливості через публічно доступну інформацію;
- Аналіз IT-інфраструктури та технологічного стеку компанії.

Підготовка звіту, який містить:

- Профіль підприємства на основі даних з державних реєстрів;
- Карту цифрового присутності компанії (домени, соціальні мережі, публічні API);
- Виявлені потенційні вразливості та витоки інформації;
- Аналіз можливих векторів атак на основі зібраної інформації;
- Рекомендації щодо підвищення рівня інформаційної безпеки;
- Методологію проведеного дослідження з переліком використаних інструментів;
- Етичні міркування та обмеження дослідження.

Вимоги до виконання:

Технічні інструменти (обов'язкові):

- Робота з API державних реєстрів або веб-скрапінг;
- Використання мінімум 3 OSINT-інструментів (Maltego, Shodan, Google Dorking, соціальні мережі);
- Документування всіх кроків дослідження.

Звіт повинен включати:

- Детальний опис методології (5-7 сторінок)
- Результати аналізу з скріншотами (10-15 сторінок)
- Візуалізацію зв'язків та структури даних
- Практичні рекомендації для підприємства

Форма подання:

Письмовий звіт обсягом 15-20 сторінок + презентація на 10-12 слайдів з демонстрацією ключових знахідок та методології дослідження.

Критерії оцінювання:

- Використання державних реєстрів (25%)
- Застосування OSINT-методів (25%)
- Якість аналізу та висновків (25%)
- Практична цінність рекомендацій (25%)

7. Організація та проведення тренінгу з дисципліни Безпека хмарних сервісів «Комплексна безпека хмарних технологій та OSINT-аналіз кіберзагроз»

Провести комплексний OSINT-аналіз обраного українського підприємства для виявлення потенційних кіберзагроз та вразливостей, використовуючи виключно легальні відкриті джерела інформації. На основі зібраних даних створити детальний звіт з оцінкою рівня кіберризиків, рекомендаціями щодо підвищення безпеки та планом моніторингу цифрового сліду організації.

Мета тренінгу:

Забезпечити учасників комплексними теоретичними знаннями та практичними навичками в галузі безпеки хмарних технологій та OSINT-методів, підготувавши їх до ефективного виявлення та аналізу кіберзагроз у сучасному цифровому середовищі.

Перелік задач для тренінгу:

1. Аналіз кіберзагроз підприємства через державні реєстри. Проведіть комплексний аналіз конкретного підприємства, використовуючи дані ЄДРПОУ, виявіть потенційні ризики через корпоративні зв'язки та фінансовий стан.
2. Дослідження цифрового сліду організації. Створіть профіль кіберзагроз для обраної компанії, аналізуючи її присутність у соціальних мережах, доменну структуру та публічну ІТ-інфраструктуру.
3. Моніторинг витоків корпоративних даних. Розробіть методологію відстеження появи конфіденційної інформації компанії у відкритих джерелах та даркнеті.
4. Аналіз інцидентів кібербезпеки через публічні дані. Дослідіть конкретний кіберінцидент, використовуючи тільки відкриті джерела, та складіть хронологію подій з ідентифікацією учасників.
5. Побудова карти загроз для галузі. Створіть аналітичну карту кіберзагроз для конкретної галузі економіки, використовуючи дані державних реєстрів та галузевих звітів.
6. OSINT-розслідування підозрілих фінансових операцій. Проведіть аналіз підозрілих транзакцій через публічні реєстри та виявіть можливі схеми відмивання коштів або фінансування

кіберзлочинності.

7. Аналіз вразливостей через публічні дані про ІТ-системи. Використайте «Shodan» та інші інструменти для виявлення потенційних вразливостей у публічно доступних системах української організації.

8. Моніторинг репутаційних загроз в онлайн-просторі. Створіть систему відстеження негативних публікацій та фейкової інформації про компанію у соціальних мережах та ЗМІ.

9. Дослідження APT-груп через відкриті джерела. Проаналізуйте діяльність конкретної APT-групи, використовуючи публічні звіти, соціальні мережі та технічну документацію.

10. Створення профілю кіберзлочинця. Складіть детальний профіль підозрюваного у кіберзлочинах, використовуючи тільки легально доступну інформацію з державних реєстрів та соціальних мереж.

Порядок проведення тренінгу:

1. Збір базової інформації - аналіз даних ЄДРПОУ, корпоративних зв'язків, фінансового стану через державні реєстри;
2. Дослідження цифрового сліду - картування доменів, субдоменів, IP-адрес, соціальних мереж організації;
3. Технічний аналіз - використання Shodan, Censys для виявлення публічно доступних сервісів та потенційних вразливостей;
4. Моніторинг витоків даних - пошук згадок компанії у витоках, форумах, даркнеті;
5. Репутаційний аналіз - відстеження публікацій, відгуків, можливої дезінформації;
6. Документування результатів - створення структурованого звіту з висновками та рекомендаціями.

Очікуваний результат: Презентація з аналізом кіберзагроз, профіль ризиків організації та практичні рекомендації щодо покращення кібербезпеки на основі виявлених уразливостей.

8. Методи навчання

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

9. Засоби оцінювання та методи демонстрування результатів навчання

У процесі вивчення дисципліни «Безпека хмарних сервісів» використовуються наступні засоби оцінювання та методи демонстрування результатів навчання:

- поточне опитування;
- модульне тестування та опитування;
- оцінювання лабораторних робіт;
- оцінювання тренінгів;
- оцінювання результатів самостійної роботи.

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 "Безпека хмарних сервісів"

визначається як середньозважена величина, в залежності від питомої ваги кожної складової залікового кредиту:

Модуль 1		**Модуль 2**	**Модуль 3**
40%	40%	5%	15%
Поточне оцінювання	Модульний контроль	Тренінги	Самостійна робота
Загальна оцінка за лабораторні роботи розраховується як середнє арифметичне з виконання 6 лабораторних робіт.	1. Теоретичні питання: 2 пита-ння по 30 балів - max 60 балів. 2. Тестові питання:10 тестів - max 40 балів.	Оцінюється виконання індивідуального завдання тренінгу (виконання роботи - max 60 балів, захист роботи - max 40 балів)	Оцінюється якість розробки, відповідність потребам підприємства, повнота реалізації функціоналу. (виконання роботи - max 60 балів, захист роботи - max 40 балів)

Виконання лабораторних робіт:

90-100 балів (Відмінно) - здобувач самостійно, без помилок, виконав усі кроки лабораторної роботи, правильно задокументував етапи та вільно оперує поняттями та принципами хмарної безпеки, управління ідентифікацією та доступом, а також методами OSINT-аналізу.

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

60-74 балів (Задовільно) - здобувач виконав завдання, але з суттєвими помилками, наприклад, не з першого разу. Розуміння поставлених у лабораторній роботі завдань є поверхневим.

1-59 балів (Незадовільно) - здобувач не зміг виконати завдання або результати були повністю невірними. Не продемонстрував базових навичок роботи з хмарними платформами, IDS/IPS системами або OSINT-інструментами.

Оцінювання модульного контролю:

90-100 балів (Відмінно) - здобувач демонструє повне і глибоке знання теоретичного матеріалу, а також практичних аспектів, вільно оперує поняттями та принципами безпеки хмарних сервісів та методів OSINT. Здатний не просто відповідати на тестові запитання, а й аналізувати складні ситуації, знаходити неочевидні рішення, аргументовано висловлювати власну позицію. Виявляє ініціативу в опануванні матеріалу, що виходить за межі навчальної програми.

75-89 балів (Добре) - здобувач має ґрунтовні знання з усіх основних розділів дисципліни. Демонструє вміння застосовувати теоретичні знання, що обговорюються на занятті, бере участь у обговореннях, відповідає на запитання викладача.

60-74 балів (Задовільно) - здобувач володіє мінімально необхідним обсягом знань. Відповіді переважно на тестові запитання, можуть містити неточності, може плутатися в термінах і поняттях. Не виявляє ініціативи в опрацюванні матеріалу, а лише відтворює інформацію, отриману на лекціях.

1-59 балів (Незадовільно) - здобувач не володіє або володіє лише фрагментарними знаннями з дисципліни. Відповіді переважно неправильні, що свідчить про повну відсутність розуміння матеріалу.

Тренінг:

90-100 балів (Відмінно) - здобувач самостійно, без помилок, виконав усі етапи завдання, правильно задокументував усі етапи роботи, та вільно оперує поняттями та принципами кібербезпеки хмарних середовищ та OSINT-методології.

75-89 балів (Добре) - 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 (Задовільно) - здобувач виконав завдання, але з суттєвими помилками, наприклад, не

з первого разу. Розуміння поставлених у тренінгу завдань є поверхневим.
1-59 балів (Незадовільно) - здобувач не зміг виконати завдання або результати були повністю невірними. Не продемонстрував базових навичок роботи з хмарними технологіями безпеки або OSINT-платформами.

Самостійна робота:

90–100 балів (Відмінно) - доповідь охоплює всі ключові аспекти обраної теми, демонструючи глибоке розуміння предмета. Дослідження містить не лише опис, але й глибокий аналіз, порівняння різних підходів та методів, а також обґрунтовані висновки. Використані сучасні та актуальні джерела інформації, що свідчить про обізнаність здобувач а з останніми тенденціями у сфері безпеки хмарних сервісів та OSINT-аналітиці. Здобувач вільно володіє матеріалом, виступає впевнено та відповідає на всі запитання.
75–89 балів (Добре) - доповідь розкриває основні питання теми, але може бути менш деталізованою. В роботі є аналітичні елементи, але вони можуть бути не достатньо глибокими. Використані джерела інформації є релевантними, але можуть бути не найновішими. Здобувач демонструє знання матеріалу, але може мати незначні труднощі з відповідями на додаткові питання.
60–74 балів (Задовільно) - доповідь охоплює лише основні аспекти теми. Можуть бути пропущені важливі деталі. Робота має описовий характер, аналіз та висновки є поверхневими. Здобувач не завжди впевнено відповідає на запитання. 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.

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.	Проєктор	1-10
2.	Персональний комп'ютер	1-10
3.	Електронний варіант лекцій	1-10
4.	Методичні вказівки до виконання лабораторних робіт (електронний варіант)	1-10
3.	Хмарна платформа (наприклад, AWS, Azure або Google Cloud)	1-3, 7-9
4	OSINT-інструменти (Maltego Community Edition, Shodan, Google Dorking)	4, 6, 10
5	Доступ до державних електронних реєстрів України (API або веб-інтерфейси)	5, 7, 10

РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

1. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. Дата оновлення: 28.12.2023. URL: https://zakon.rada.gov.ua/laws/show/2163-19
2. Про затвердження Стратегії кібербезпеки України : Указ Президента України від 26.08.2021 № 447/2021. URL: https://www.president.gov.ua/documents/4472021-40013
3. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу : НД ТЗІ 1.1-003-99. Київ : ДССЗЗІ України, 1999. 62 с.
4. Системи управління якістю. Вимоги: ДСТУ ISO 9001:2015. Київ: ДП «УкрНДНЦ», 2016. 22 с.
5. Оцінювання економічної ефективності проектних рішень у будівництві: ДСТУ-Н Б А.3.1-23:2013. Київ: Мінрегіон України, 2014. 16 с.
6. Архипов А. Є., Архипова Н. І. Кібербезпека критичних інфраструктур: теорія і практика: навчальний посібник. Київ: НАУ, 2020. 284 с.
7. Бабала Л. В. Економічні основи проектування систем автоматизації: навчальний посібник. Київ: НТУУ «КПІ», 2023. 284 с.
8. Бабала Л. В., Бойчук А. В. Інформаційна система підтримки управлінської діяльності підприємства. Modern problems of science, education and society: Proceedings of the 8th International scientific and practical conference. Kyiv: SPC «Sci-conf.com.ua», 2023. С. 228-232.
9. Грищук Р. В., Данилюк В. А. Основи кібербезпеки: навчальний посібник. Житомир: ЖНАЕУ, 2021. 544 с.
10. Ковальчук О., Бабала Л., Іваницький Р. Інтелектуальна модель виявлення асоціативних правил у базах даних кримінальних правопорушень. Herald of Khmelnytskyi National University. Technical sciences. 2025. Vol. 03-27. DOI: 10.31891/2307-5732-2025-349-27.
11. Корченко О. Г., Казмірчук С. В. Системи виявлення вторгнень : навчальний посібник. Київ: КПІ ім. Ігоря Сікорського, 2022. 312 с.
12. Лахно В. А., Касаткіна Н. В. Захист інформації в комп'ютерних системах і мережах : навчальний посібник. Суми : СумДПУ імені А. С. Макаренка, 2021. 268 с.
13. Бабала Л. В., Данилюк І. В. Проектування та реалізація комп'ютеризованої системи контролю дотримання вимог безпеки. The 7th International scientific and practical conference "Perspectives of contemporary science: theory and practice" (August 19-21, 2024). Lviv: SPC «Sci-conf.com.ua», 2024. С. 183-186.
14. Basta, A., & Halton, W. Computer Security and Penetration Testing. 3rd ed. Boston: Cengage Learning, 2019. 576 p.
15. Bazzell, M. Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information. 8th ed. North Charleston: Intel Techniques, 2021. 784 p.
16. Brown, A. K. Investment Evaluation Methods for Smart Manufacturing. London: Springer-Verlag, 2023. 356 p.
17. Chen, L., Patel, K., Mueller, S. Cost-Benefit Analysis in Manufacturing Automation. International Journal of Production Economics. 2024. Vol. 267. P. 108-125.
18. Conklin, W. A., White, G., Williams, D., Davis, R. L., & Cothren, C. CompTIA Security+ All-in-One Exam Guide, Sixth Edition (Exam SY0-601). 6th ed. New York: McGraw Hill, 2021. 896 p.
19. Diogenes, Y., & Dmitrenko, M. Cybersecurity – Azure Security: Get to grips with building and maintaining cloud security solutions for your Azure environment. Birmingham: Packt Publishing, 2019. 456 p.
20. Stallings, W., & Brown, L. Computer Security: Principles and Practice. 4th ed. London: Pearson, 2022. 912 p.
21. Sullivan, N. Cloud Security: A Comprehensive Guide to Secure Cloud Computing. Hoboken: Wiley, 2022. 528 p.
22. Vacca, J. R. Cloud Computing Security: Foundations and Challenges. Boca Raton: CRC Press, 2021. 584 p.
23. Yoon, H. J. Cybersecurity in the Digital Age: Tools, Techniques & Best Practices. New York: Business Expert Press, 2020. 298 p.
24. CERT-UA: офіційний веб-сайт. URL: https://cert.gov.ua
25. Державна служба спеціального зв'язку та захисту інформації України: офіційний веб-сайт. URL: https://cip.gov.ua

26. Державна служба статистики України: офіційний веб-сайт. URL: http://www.ukrstat.gov.ua
27. Міністерство економіки України: офіційний веб-сайт. URL: https://www.me.gov.ua
28. Національний банк України: офіційний веб-сайт. URL: https://bank.gov.ua
29. NIST Cybersecurity Framework: офіційний веб-сайт. URL: https://nist.gov/cyberframework
30. OWASP (Open Web Application Security Project): офіційний веб-сайт. URL: https://owasp.org
31. Shodan Search Engine : веб-сервіс. URL: https://shodan.io