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

ЗАТВЕРДЖУЮ
Декан факультету комп'ютерних інформаційних технологій
_____Ігор ЯКИМЕНКО
«30» _____ 2025р.

ЗАТВЕРДЖУЮ
Проректор з науково-педагогічної роботи
_____Віктор ОСТРОВЕРХОВ
«___» _____ 2025р.

ЗАТВЕРДЖУЮ:
Директор навчально-наукового інституту новітніх освітніх технологій
_____Святослав ПИТЕЛЬ
«___» _____ 2025р.

РОБОЧА ПРОГРАМА

з дисципліни

«УПРАВЛІННЯ ТА ЗАХИСТ ХМАРНИХ ІНФРАСТРУКТУР»

Ступінь вищої освіти – магістр
Галузь знань – F Інформаційні технології
Спеціальність – F5 Кібербезпека та захист інформації
Освітньо-професійна програма – Кібербезпека

Кафедра кібербезпеки

Форма навчання	Курс	Семестр	Лекції (год.)	Практ. (год.)	ІРС (год.)	Тренінг (год)	СРС (год.)	Разом (год.)	Залік/ екзамен. (семестр)
Денна	1	2	32	14	5	6	93	150	Екзамен (2)
Заочна	1	2	8	4	---	---	138	150	Екзамен (2)

Тернопіль – 2025

Робочу програму склав доцент кафедри кібербезпеки, к.т.н., доцент Цаволик Тарас Григорович.

Робоча програма затверджена на засіданні кафедри кібербезпеки,
протокол № 3 від 25.09.25 р.

Завідувач кафедри Василь ЯЦКІВ

Гарант освітньо-професійної програми Василь ЯЦКІВ

СТРУКТУРА РОБОЧОЇ ПРОГРАМИ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

1. Опис дисципліни «Управління та захист хмарних інфраструктур»

Дисципліна – «Управління та захист хмарних інфраструктур»	**Галузь знань, спеціальність, СВО**	**Характеристика навчальної дисципліни**
Кількість кредитів – 5	Галузь знань F Інформаційні технології	Статус дисципліни – вибіркова Мова навчання - українська
Кількість залікових модулів – 4	Спеціальність F5 – Кібербезпека та захист інформації	Рік підготовки: ДФН - 1; ЗФН - 1 Семестр: ДФН – 2; ЗФН – 2
Кількість змістових модулів –2	Освітній ступінь – магістр	Лекції: ДФН – 32 год.; ЗФН: - 8 год. Лабораторні роботи: ДФН – 14 год.; ЗФН – 4 год.
Загальна кількість годин – 150		Самостійна робота: ДФН –93 год. ЗФН – 138. Тренінг: ДФН – 6 год. Індивідуальна робота: ДФН - 5 год.
Тижневих годин:10 год., з них аудиторних –3 год.		Вид підсумкового контролю – екзамен

2. Мета й завдання вивчення дисципліни

2.1. Мета вивчення дисципліни

Метою вивчення дисципліни “Управління та захист хмарних інфраструктур” полягає у формуванні знань та навичок, для протидії сучасним кіберзагрозам через стрімке зростання використання хмарних технологій у всіх сферах бізнесу, державного управління та освіти. Хмарні сервіси стають основною інфраструктурою для зберігання, обробки та передачі даних, що супроводжується зростанням ризиків кіберзагроз, втрат даних, витоків інформації та атак на хмарні середовища.

2.2 Завдання вивчення дисципліни

Основне завдання курсу полягає у формуванні у здобувачів освітньо-професійної програми комплексних знань та практичних навичок щодо управління безпекою хмарних інформаційних систем та захисту хмарних інфраструктур від сучасних кіберзагроз. Дисципліна спрямована на розвиток умінь застосовувати сучасні методи та технології забезпечення безпеки в хмарних середовищах, що базуються на принципах комплексного підходу до управління безпекою та інтегрованих рішеннях захисту.

У результаті вивчення навчальної дисципліни здобувач повинен:

знати:

- Фундаментальні принципи хмарних обчислень та основи безпеки хмарних інфраструктур, включаючи моделі розгортання (IaaS, PaaS, SaaS) та моделі розподілу відповідальності між постачальником та клієнтом;
- Архітектурні компоненты хмарних інфраструктур, їх взаємодію та специфічні вимоги безпеки для кожного компонента;
- Принципи та механізми управління ідентифікацією та доступом (IAM), включаючи аутентифікацію, авторизацію, федеративне управління ідентичністю та принцип найменших привілеїв;
- Технології мережевої безпеки у хмарі, включаючи сегментацію мережі, віртуальні приватні хмари (VPC), брандмауери наступного покоління та захист від DDoS-атак;

- Методи захисту даних, включаючи симетричне та асиметричне шифрування, управління ключами, технології BYOK (Bring Your Own Key), HYOK (Hold Your Own Key) та BYOE (Bring Your Own Encryption);
- Принципи безпеки обчислювальних ресурсів, включаючи захист віртуальних машин, контейнерів, функцій без сервера та мікросервісів;
- Технології моніторингу, логування та виявлення загроз у хмарних середовищах, включаючи SIEM, SOAR, машинне навчання та поведінкову аналітику;
- Принципи інтеграції безпеки в процеси розробки та експлуатації (DevSecOps), включаючи безперервну інтеграцію безпеки, автоматизацію тестування безпеки та управління вразливостями;
- Методології реагування на інциденти у хмарних середовищах, включаючи специфіку розслідування хмарних інцидентів, збір та аналіз цифрових доказів;
- Вимоги комплаєнсу та управління політиками безпеки у хмарі, включаючи GDPR, HIPAA, SOC 2, ISO 27001 та галузеві стандарти;
- Принципи автоматизації безпеки та управління станом безпеки хмари (CSPM), включаючи автоматичне виявлення неправильних конфігурацій та їх усунення;
- Стратегії відновлення після збоїв та забезпечення безперервності бізнесу у хмарних середовищах, включаючи DRaaS, резервне копіювання та високу доступність;
- Сучасні загрози хмарним інфраструктурам та передові методи захисту, включаючи zero-trust архітектуру, поведінкову аналітику та штучний інтелект у безпеці;
- Особливості забезпечення безпеки у мультихмарних та гібридних середовищах, включаючи централізоване управління політиками та уніфіковану видимість.

вміти:

- Проектувати та впроваджувати комплексні системи безпеки хмарних інфраструктур з урахуванням специфіки різних хмарних сервісів та моделей розгортання;
- Налаштовувати та управляти системами IAM, включаючи створення політик доступу, налаштування багатофакторної аутентифікації та впровадження рольової моделі доступу;
- Проектувати та впроваджувати мережеву архітектуру безпеки у хмарі, включаючи налаштування VPC, підмереж, групи безпеки та мережевих ACL;
- Впроваджувати комплексні рішення шифрування даних, включаючи вибір відповідних алгоритмів, налаштування систем управління ключами та забезпечення шифрування в стані спокою, при передачі та під час обробки;
- Налаштовувати та експлуатувати системи моніторингу безпеки та виявлення загроз, включаючи створення правил кореляції, налаштування алертів та аналіз журналів безпеки;
- Інтегрувати практики DevSecOps у процеси розробки, включаючи автоматизацію тестування безпеки, сканування вразливостей та управління секретами;
- Розробляти та впроваджувати плани реагування на інциденти у хмарних середовищах, включаючи процедури ізоляції, збору доказів та відновлення;
- Проводити аудит комплаєнсу та впроваджувати політики управління у відповідності з регуляторними вимогами;
- Автоматизувати процеси управління станом безпеки хмари, включаючи використання CSPM-інструментів та Infrastructure as Code;
- Розробляти та тестувати стратегії відновлення після збоїв та забезпечення безперервності бізнесу;
- Виявляти та протидіяти сучасним загрозам у хмарних середовищах, використовуючи передові методи захисту та аналітики загроз;
- Управляти безпекою в мультихмарних та гібридних середовищах, забезпечуючи єдині стандарти безпеки та централізоване управління.

Завдання лекційних занять.

Завданням лекційних занять є формування теоретичної бази знань з управління та захисту хмарних інфраструктур, включаючи вивчення сучасних підходів до забезпечення безпеки хмарних систем, ознайомлення з передовими технологіями захисту та розуміння принципів комплексного управління безпекою в динамічних хмарних середовищах.

Завдання проведення лабораторних робіт.

Завданням лабораторних робіт полягає у закріпленні теоретичних знань через практичне застосування сучасних інструментів та технологій хмарної безпеки, розвитку навичок роботи з провідними хмарними платформами та формуванні комплексного розуміння процесів управління безпекою хмарних інфраструктур в умовах постійно змінюваного ландшафту загроз.

3. Програма навчальної дисципліни

Змістовний модуль 1. Основи управління та безпеки хмарних інфраструктур.

Тема 1. Вступ до хмарних обчислень та їх безпеки.

Пояснювати різницю між сервісними та моделями розгортання хмарних середовищ. Аналізувати та застосовувати модель спільної відповідальності (Shared Responsibility Model) для різних хмарних сервісів. Визначати основні переваги та ризики використання хмарних технологій для бізнесу. Класифікувати ключові загрози безпеці у хмарних інфраструктурах.

Тема 2. Архітектура та компоненти хмарної інфраструктури.

Принципи роботи технологій віртуалізації та контейнеризації. Розрізняти типи хмарних сховищ (об'єктні, блокові, файлові) та їх застосування. Пояснювати архітектуру програмно-визначених мереж (SDN) та їх роль у хмарі. Проєктувати базову архітектуру хмарного застосунку, обираючи відповідні компоненти.

Тема 3. Управління ідентифікацією та доступом (Identity and Access Management - IAM).

Налаштовування політики IAM на основі принципу найменших привілеїв (Principle of Least Privilege). Впроваджувати багатофакторну автентифікацію (MFA) для користувачів та сервісних акаунтів. Керувати життєвим циклом ідентичностей у хмарному середовищі. Інтегрувати хмарні сервіси з корпоративними системами ідентифікації.

Тема 4. Мережева безпека у хмарі.

Проєктувати та створювати безпечну мережеву топологію в хмарі за допомогою VPC та підмереж. Налаштовувати правила фільтрації трафіку за допомогою груп безпеки та мережевих ACL. Розгортати та конфігурувати віртуальні брандмауери та VPN-з'єднання. Аналізувати мережевий трафік для виявлення аномалій та загроз.

Тема 5. Захист даних: шифрування та управління ключами.

Застосовувати шифрування для різних типів хмарних сховищ та баз даних. Налаштовувати SSL/TLS для захисту даних під час передачі. Керувати ключами шифрування (створення, ротація, знищення) за допомогою Key Management Service. Обирати відповідний метод захисту (шифрування, токенізація) залежно від чутливості даних.

Тема 6. Безпека обчислювальних ресурсів.

Застосовувати техніки "зміцнення" (hardening) для образів віртуальних машин та контейнерів. Налаштовувати автоматизоване сканування на вразливості та управління виправленнями. Ізолювати контейнерні застосунки для мінімізації поверхні атаки. Впроваджувати системи захисту кінцевих точок (Endpoint Protection) для хмарних ресурсів..

Тема 7. Моніторинг, логування та виявлення загроз.

Налаштовувати централізований збір та аналіз логів (CloudTrail, Azure Monitor). Створювати панелі моніторингу (dashboards) для візуалізації стану безпеки інфраструктури. Налаштовувати правила оповіщення (alerts) для підозрілої активності. Інтегрувати хмарні логи з SIEM-системами для комплексного аналізу загроз.

Змістовий модуль 2. Просунуті технології та практики хмарної безпеки.

Тема 8. Безпека додатків та DevSecOps.

Інтегрувати інструменти сканування безпеки в конвеєр CI/CD. Аналізувати та усувати вразливості в коді додатків та їх залежностях. Впроваджувати заходи безпеки для API-шлюзів (автентифікація, авторизація, rate limiting). Оцінювати ризики безпеки для serverless-функцій (напр., AWS Lambda, Azure Functions).

Тема 9. Реагування на інциденти та розслідування у хмарі.

Розробляти план реагування на інциденти, адаптований до хмарної специфіки. Використовувати хмарні інструменти для збору та аналізу цифрових доказів (знімки дисків, логи). Виконувати процедури ізоляції скомпрометованих ресурсів для запобігання поширенню атаки. Проводити аналіз першопричин (root cause analysis) інциденту.

Тема 10. Комплаєнс та управління політиками в хмарі.

Аналізувати вимоги основних стандартів безпеки та застосовувати їх до хмарної

інфраструктури. Використовувати хмарні сервіси для проведення аудиту та моніторингу відповідності. Налаштовувати автоматизовані правила для запобігання порушенням політик безпеки. Готувати звітність щодо стану відповідності інфраструктури вимогам.

Тема 11. Автоматизація безпеки (Security Automation).

Писати безпечні шаблони IaC для автоматичного створення хмарних ресурсів. Впроваджувати перевірки безпеки в процес розгортання інфраструктури. Налаштовувати автоматизовані скрипти (напр., Lambda-функції) для реагування на події безпеки. Використовувати інструменти для автоматичного виправлення виявлених проблем конфігурації.

Тема 12. Управління станом безпеки хмари (Cloud Security Posture Management - CSPM).

Використовувати CSPM-інструменти для сканування хмарних середовищ на наявність ризиків. Інтерпретувати звіти CSPM та пріоритезувати виправлення на основі рівня ризику. Налаштовувати базові політики в CSPM-рішеннях. Пояснювати роль CSPM у підтримці безперервного комплаєнсу.

Тема 13. Відновлення після збоїв та безперервність бізнесу (DR/BCP).

Розробляти та тестувати план відновлення після збоїв (Disaster Recovery Plan). Налаштовувати автоматизоване резервне копіювання для різних типів даних. Проєктувати архітектуру, яка розподілена між кількома зонами доступності або регіонами. Розраховувати показники RTO (Recovery Time Objective) та RPO (Recovery Point Objective) для бізнес-процесів.

Тема 14. Просунуті загрози та методи захисту.

Налаштовувати хмарні сервіси для захисту від DDoS-атак. Аналізувати тактики, техніки та процедури (TTPs), що використовуються APT-групами. Застосовувати сервіси аналітики загроз для проактивного виявлення шкідливої активності. Впроваджувати архітектурні патерни для зменшення ризиків від складних атак.

Тема 15. Безпека мультихмарних та гібридних середовищ.

Визначати основні проблеми безпеки в мультихмарних та гібридних архітектурах. Розробляти єдину стратегію управління ідентифікацією та доступом для різних середовищ. Використовувати інструменти для отримання централізованого огляду стану безпеки всієї інфраструктури. Планувати безпечне з'єднання між локальними дата-центрами та публічними хмарами.

4. Структура залікового кредиту дисципліни

4.1 Структура залікового кредиту дисципліни для ДФН

ДФН	Кількість годин					
	Лекції	Лабор. роботи	СРС	ІРС	Тренінг	Контрольні заходи
Змістовий модуль 1. Основи управління та безпеки хмарних інфраструктур.						
Тема 1. Вступ до хмарних обчислень та їх безпеки	2		5	2	4	Поточне опитування
Тема 2. Архітектура та компоненти хмарної інфраструктури	2		5			
Тема 3. Управління ідентифікацією та доступом (Identity and Access Management - IAM)	2		5			
Тема 4. Мережева безпека у хмарі	2	2	5			
Тема 5. Захист даних: шифрування та управління ключами	2	2	5			
Тема 6. Безпека обчислювальних ресурсів	2	2	5			
Тема 7. Моніторинг, логування та виявлення загроз	2	2	5			
Змістовий модуль 2. Просунуті технології та практики хмарної безпеки.						
Тема 8. Безпека додатків та DevSecOps	2	2	5	3	2	Поточне опитуванн

Тема 9. Реагування на інциденти та розслідування у хмарі	2	2	7			я
Тема 10. Комплаєнс та управління політиками в хмарі	2	2	7			
Тема 11. Автоматизація безпеки (Security Automation)	2		7			
Тема 12. Управління станом безпеки хмари (Cloud Security Posture Management - CSPM)	2		8			
Тема 13. Відновлення після збоїв та безперервність бізнесу (DR/BCP)	2		8			
Тема 14. Просунуті загрози та методи захисту	3		8			
Тема 15. Безпека мультихмарних та гібридних середовищ	3		8			
Разом	**32**	**14**	**93**	**5**	**6**	

4.2 Структура залікового кредиту дисципліни для ЗФН

ЗФН	Кількість годин					
	Лекції	Лабора то. роб.	Самостійна робота	Контрольні заходи		
Змістовий модуль 1. Основи управління та безпеки хмарних інфраструктур.						
Тема 1. Вступ до хмарних обчислень та їх безпеки	2		5	Поточне опитування		
Тема 2. Архітектура та компоненти хмарної інфраструктури			10			
Тема 3. Управління ідентифікацією та доступом (Identity and Access Management - IAM)			5			
Тема 4. Мережева безпека у хмарі			8			
Тема 5. Захист даних: шифрування та управління ключами			10			
Тема 6. Безпека обчислювальних ресурсів			10			
Тема 7. Моніторинг, логування та виявлення загроз			10			
Змістовий модуль 2. Просунуті технології та практики хмарної безпеки.						
Тема 8. Безпека додатків та DevSecOps	2	2	10	Поточне опитування		
Тема 9. Реагування на інциденти та розслідування у хмарі						
Тема 10. Комплаєнс та управління політиками в хмарі			10			
Тема 11. Автоматизація безпеки (Security Automation)			10			
Тема 12. Управління станом безпеки хмари (Cloud Security Posture Management - CSPM)			10			
Тема 13. Відновлення після збоїв та безперервність бізнесу (DR/BCP)			10			
Тема 14. Просунуті загрози та методи захисту	2		10			
Тема 15. Безпека мультихмарних та гібридних середовищ			10			
Разом	**8**	**4**	**138**			

5. Тематика лабораторних робіт.

Лабораторна робота № 1.

Тема: Проєктування та конфігурація віртуального приватного хмари (VPC) із сегментацією та мережевими ACL.

Мета: Набути практичних навичок створення сегментованої мережевої архітектури у хмарі для контролю трафіку між сегментами та Інтернетом.

Питання для обговорення: Вибір та налаштування VPC, підмереж (публічних/приватних). Конфігурація маршрутних таблиць і підключення до Інтернет-шлюзу. Групи безпеки vs мережеві ACL: відмінності та сценарії використання. Політики дозволу/заборони трафіку між сегментами. Захист від зовнішніх загроз (DDoS, несанкціонований доступ)

Лабораторна робота № 2.

Тема: Реалізація шифрування даних на стороні сервера з використанням KMS.

Мета: Отримати навички налаштування й використання сервісу управління ключами та шифрування даних у хмарі.

Питання для обговорення: Архітектура KMS: симетричні та асиметричні ключі. Створення, ротація та видалення ключів. Шифрування та розшифрування файлів в об'єктному сховищі. BYOK, HYOK, BYOE—порівняння моделей управління ключами. Логи доступу до ключів та аудит операцій.

Лабораторна робота № 3.

Тема: Жорстка конфігурація віртуальної машини та перевірка вразливостей.

Мета: Навчитись проводити базове заточення ОС і проводити сканування вразливостей хмарних обчислювальних ресурсів.

Питання для обговорення: Основні кроки hardening віртуальної машини (оновлення, мінімальні пакети). Налаштування host-based firewall і SELinux/AppArmor. Встановлення та конфігурація агента сканування вразливостей. Аналіз результатів сканера та пріоритезація виправлень. Розробка плану регулярного hardening та моніторингу конфігурації.

Лабораторна робота № 4.

Тема: Налаштування централізованого логування та виявлення аномалій.

Мета: Отримати навички інтеграції лог-агентів та налаштування правил в SIEM для виявлення підозрілої активності.

Питання для обговорення: Вибір архітектури централізованого логування (агенти, шлюзи, SIEM). Формати та протоколи передачі логів (Syslog, JSON, TLS). Створення парсингу та нормалізації подій. Конфігурація кореляційних правил та алертів. Методи виявлення аномалій: порогові значення, машинне навчання, поведінкова аналітика.

Лабораторна робота № 5.

Тема: Інтеграція статичного аналізу коду та SAST у CI/CD-конвеєр.

Мета: Набути навичок автоматизації перевірки безпеки на етапі розробки та забезпечення якісного коду.

Питання для обговорення: Вибір інструменту для SAST (SonarQube, Fortify, CodeQL). Налаштування етапу статичного аналізу у GitLab/GitHub Actions. Інтерпретація результатів аналізу: типи вразливостей, пріоритизація. Автоматична блокування збірки при критичних знайдених вразливостях. Управління виключеннями та тюнінг правил аналізатора.

Лабораторна робота № 6.

Тема: Імітація та розслідування інциденту безпеки в хмарному середовищі.

Мета: Отримати навички відтворення інцидентів, збору цифрових доказів та аналізу ланцюжка атаки.

Питання для обговорення: Інструменти для генерації підозрілих подій (скрипти, підроблені запити). Збір артефактів: логи, знімки дисків, мережеві трейси. Використання cloud-forensics методів для аналізу образів VM. Визначення точки входу, векторів атаки та обсягу компрометації. Підготовка інцидент-репорту та рекомендацій з усунення наслідків.

Лабораторна робота № 7.

Тема: Створення та перевірка політик доступу за допомогою Infrastructure as Code

Мета: Навчитись описувати, розгортати та аудитувати політики доступу у хмарі засобами Terraform або CloudFormation.

Питання для обговорення: Опис IAM-політик у HCL/JSON: ролі, групи, привілеї. Використання модулів та шаблонів для уніфікації політик. Інтеграція з CIS Benchmarks та перевірка відповідності.

Використання linter'ів та IaC-сканерів для виявлення неправильних конфігурацій. Автоматизація деплойменту та реверс-бека та відкат змін у разі невідповідності.

6. Тренінг з дисципліни.

Порядок проведення тренінгу:

Вступна частина проводиться з метою ознайомлення здобувачів зі структурою і ключовими концепціями тренінгу з управління та захисту хмарних інфраструктур.

Організаційна частина полягає у формуванні робочих груп по 3–4 особи та виборі теми дослідження або проєкту в межах проблематики хмарної безпеки.

Практична частина реалізується шляхом колективної розробки прототипу рішення або проведення кейс-стаді (наприклад, налаштування CSPM, побудова моделі реагування на інциденти, автоматизація DevSecOps-процесів) із використанням інструментів хмарного провайдера.

Підведення підсумків. Обговорення результатів виконаних завдань, рефлексія щодо обраних підходів, презентація напрацювань та обмін досвідом між групами.

Рекомендована тематика тренінгу: Впровадження автоматизованої системи реагування на інциденти в мультихмарному середовищі

Здобувачі обирають одну із запропонованих тем або формулюють власну тему у межах проблематики управління та захисту хмарних інфраструктур.

Орієнтовна перелік завдань:

1. Аналіз архітектури обраного хмарного середовища та виявлення вразливих зон.
2. Розробка моделі Identity and Access Management із застосуванням принципу найменших привілеїв.
3. Налаштування сценаріїв автоматичної ротації ключів шифрування та моніторингу доступу до KMS.
4. Проєктування мережевої сегментації й інтеграція NGFW/VPC для захисту критичних сервісів.
5. Створення конвеєру DevSecOps із включенням статичного аналізу коду та перевірки інфраструктури IaC.
6. Реалізація централізованого логування в SIEM та розробка кореляційних правил для виявлення аномалій.
7. Розробка та тестування автоматизованих playbook'ів реагування на інциденти за допомогою SOAR.
8. Проведення аудиту відповідності стандартам (CIS, ISO 27001, GDPR) і виправлення невідповідностей.
9. Розгортання прототипу CSPM-сканера для виявлення неправильних конфігурацій і демонстрація їх самовідновлення.
10. Створення плану DR/BCP із автоматизованим запуском резервних середовищ і перевіркою працездатності.

7. Самостійна робота.

Самостійна робота з курсу «Управління та захист хмарних інфраструктур» включає вивчення наведених тем та оцінюється у вигляді тесту:

1. Вступ до хмарних обчислень: моделі IaaS, PaaS, SaaS; модель спільної відповідальності.
2. Архітектура хмарної інфраструктури: компоненти, сервіси, принципи розгортання.
3. Identity and Access Management (IAM): аутентифікація, авторизація, федерація, MFA, принцип найменших привілеїв.
4. Мережева безпека у хмарі: VPC, підмережі, групи безпеки, мережеві ACL, NGFW, захист від DDoS.
5. Захист даних: методи симетричного та асиметричного шифрування, управління ключами (KMS, BYOK, HYOK).
6. Безпека обчислювальних ресурсів: hardening віртуальних машин і контейнерів, захист без-серверних функцій.
7. Моніторинг, логування та виявлення загроз: SIEM, SOAR, нормалізація логів, кореляційні правила, аномалістика.
8. Безпека додатків та DevSecOps: інтеграція SAST/DAST у CI/CD, управління секретами, IaC-сканування.

9. Реагування на інциденти та розслідування у хмарі: методи cloud-forensics, збір артефактів, playbook-и SOAR.
10. Комплаєнс та управління політиками: GDPR, HIPAA, CIS Benchmarks, IAM-політики через IaC.
11. Автоматизація безпеки: Security Automation, використання скриптів та інструментів для автоматичного відновлення конфігурацій.
12. Cloud Security Posture Management (CSPM): принципи роботи, виявлення і виправлення неправильних конфігурацій.
13. Відновлення після збоїв та безперервність бізнесу: DRaaS, резервне копіювання, RTO/RPO, тестування планів DR/BCP.
14. Просунуті загрози та методи захисту: zero-trust, UEBA, EDR, штучний інтелект у захисті.
15. Безпека мультихмарних та гібридних середовищ: централізоване управління, уніфікована видимість, інтеграція політик.

8. Методи навчання.

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

9. Засоби оцінювання та методи демонстрування результатів навчання.

У процесі вивчення дисципліни «Управління та захист хмарних інфраструктур» використовуються наступні засоби оцінювання та методи демонстрування результатів навчання:

- поточне тестування та опитування;
- підсумкове тестування за кожним змістовним модулем;
- оцінювання виконання лабораторних робіт;
- оцінювання тренінгів;
- оцінювання результатів самостійної роботи.

10. Політика оцінювання

- *Політика щодо дедлайнів і перескладання.* Для всіх видів навчальних завдань і контрольних заходів встановлюються чіткі дедлайни. Роботи, здані із порушенням термінів без поважних причин, оцінюються на нижчу оцінку (-10 балів). Перескладання проводиться у встановленому порядку.
- *Політика щодо академічної доброчесності.* Здобувач ОПП зобов'язаний виконувати усі роботи та завдання самостійно. Під час контрольного заходу він може користуватися лише дозволеними допоміжними матеріалами або засобами; йому забороняється в будь-якій формі обмінюватися інформацією з іншими здобувачами, а також використовувати, розповсюджувати або збирати варіанти чужих робіт чи контрольних завдань..
- *Політика щодо відвідування.* За об'єктивних причин (наприклад, карантин, воєнний стан, хвороба, закордонне стажування) навчання може відбуватись у дистанційній формі за погодженням із керівником курсу та з дозволу дирекції факультету.

11. Критерії, форми поточного та підсумкового контролю

Підсумковий бал (за 100-бальною шкалою) з дисципліни „Управління та захист хмарних інфраструктур" визначається як середньозважена величина, залежно від питомої ваги кожної складової залікового кредиту:

Для екзамену

Модуль 1		Модуль 2	Модуль 3	Модуль 4
20%	20%	5%	15%	40%
Поточне оцінювання	Модульний контроль	Тренінги	Самостійна робота	Екзамен
Визначається як середнє арифметичне з	Модульна робота.	Оцінка за виконання та презентацію	Оцінка за виконане завдання самостійної роботи.	Теоретичні питання:

оцінок отриманих на заняттях.		завдання тренінгу.		1 питання - max 40 балів. 2 практичних завдання по 30 балів - max 60 балів

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:

90–100 балів – правильно виконано 90–100% завдань тесту.

75–89 балів – правильно виконано 75–89% завдань тесту.

60–74 бали – правильно виконано 60–74% завдань тесту.

1–59 балів – правильно виконано менше 60% завдань тесту.

Тренінг:

90-100 балів (Відмінно) - здобувач освіти самостійно, без помилок, виконав усі етапи завдання, правильно задокументував усі етапи роботи, та вільно оперує поняттями та принципами дисципліни.

75-89 балів (Добре) - здобувач освіти виконав завдання, але з кількома дрібними помилками, які не вплинули на кінцевий результат, в процесі роботи виникали додаткові запитання.

60-74 балів (Задовільно) - здобувач освіти виконав завдання, але з суттєвими помилками, наприклад, не з першого разу. 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 апаратним та програмним забезпеченням.

Самостійна робота: оцінюється у вигляді тестування за результатами опрацювання теоретичного матеріалу. Теоретичні питання: 25 питань по 4 бали, Максимальна оцінка 100 балів.

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

Перший блок містить одне теоретичне запитань, за кожне з яких можна отримати від 0 до 40 балів. За відповідь на питання здобувач отримує 20–40 балів, якщо у повному обсязі володіє навчальним матеріалом, всебічно, самостійно та аргументовано відповідає на питання білету і 1–20 балів – якщо володіє навчальним матеріалом не в повному обсязі, викладає його фрагментарно, допускаючи при цьому суттєві неточності.

Другий блок містить практичне завдання:

40 – 60 балів - доповідь охоплює всі основні аспекти обраної теми, демонструючи глибоке розуміння предмету дисципліни. Здобувач вільно володіє матеріалом, відповідає впевнено на всі запитання.

21–40 балів - доповідь розкриває основні питання теми, але може бути недостатньо деталізованою; є аналітичні елементи, але вони можуть бути не достатньо глибокими. Здобувач демонструє знання матеріалу, але має незначні труднощі з відповідями на додаткові питання.

11–20 балів - відповідь охоплює лише основні аспекти теми, бути пропущені важливі деталі. Здобувач не завжди впевнено відповідає на запитання.

1–10 балів - відповідь містить значні помилки або не зовсім відповідає завданню.

Шкала оцінювання

За шкалою університету	За національною шкалою	За шкалою ECTS
90–100	відмінно	A (відмінно)
85–89	добре	B (дуже добре)
75–84		C (добре)
65–74	задовільно	D (задовільно)
60–64		E (достатньо)
35–59	незадовільно	FX (незадовільно з можливістю повторного складання)
1–34		F (незадовільно з обов'язковим повторним курсом)

12. Інструменти, обладнання та програмне забезпечення, використання яких передбачає навчальна дисципліна.

№	Найменування	Номер теми
1	Мультимедійний проектор та проєкційний екран	1 -15
2	Персональні комп'ютери	1 -15
3	Комунікаційне програмне забезпечення (Zoom) для проведення занять у режимі он-лайн (за необхідності)	1 -15
4	Комунікаційна навчальна платформа (Moodle) для організації дистанційного навчання (за необхідності)	1 -15
5	Наявність доступу до мережі Інтернет	1 -15
6	Браузери (Chrome, Firefox) та доступ до панелі управління хмарними провайдерами (AWS Console, Azure Portal)	1-15

РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

1. Cloud infrastructure security: 10 key best practices. N-iX, 2024. Режим доступу: https://www.n-ix.com/cloud-infrastructure-security/ (переглянуто 2025).
2. Cloud Infrastructure Security: 7 Best Practices. Syteca, 2025. Режим доступу: https://www.syteca.com/en/blog/cloud-infrastructure-security (переглянуто 2025).
3. 9 Open source cloud security tools for 2025. Sysdig, 2025. Режим доступу: https://www.sysdig.com/blog/9-open-source-cloud-security-tools (переглянуто 2025).
4. What Is Cloud Infrastructure Security? Risks and Best Practices. LegitSecurity, 2025. Режим доступу: https://www.legitsecurity.com/aspm-knowledge-base/cloud-infrastructure-security (переглянуто 2025).
5. Top 10 Cloud Security Tools for 2025. Jit.io, 2024. Режим доступу: https://www.jit.io/resources/cloud-sec-tools/cloud-security-tools-for-2023 (переглянуто 2025).
6. Cloud Threats on the Rise: Alert Trends Show Intensified Attacks. Palo Alto Networks Unit42, 2025. Режим доступу: https://unit42.paloaltonetworks.com/2025-cloud-security-alert-trends/ (переглянуто 2025).
7. Cloud computing trends for 2023 - 2025. Nearshore, 2024. Режим доступу: https://nearshore-it.eu/technologies/cloud-computing-trends-for-2023-2025/ (переглянуто 2025).
8. 20 Cloud Security Best Practices. CrowdStrike, 2024. Режим доступу: https://www.crowdstrike.com/en-us/cybersecurity-101/cloud-security/cloud-security-best-practices/ (переглянуто 2025).
9. Top 7 Cloud Security Frameworks and How to Choose. Exabeam, 2025. Режим доступу: https://www.exabeam.com/explainers/cloud-security/top-7-cloud-security-frameworks-and-how-to-choose/ (переглянуто 2025).
10. What is Cloud Risk Management?. Orca Security, 2024. Режим доступу: https://orca.security/resources/blog/what-is-cloud-risk-management/ (переглянуто 2025).
11. What is Cloud Infrastructure Security?. SentinelOne, 2025. Режим доступу: https://www.sentinelone.com/cybersecurity-101/cloud-security/cloud-infrastructure-security/ (переглянуто 2025).
12. Cloud Security Risks: What to Look Out for and How to Stay Safe. Gigacloud, 2025. Режим доступу: https://gigacloud.ua/en/articles/ryzyky-hmarnoyi-bezpeky-na-shho-zvernuty-uvagu-ta-yak-zahystytysya/ (переглянуто 2025).

13. Cloud Security Best Practices: 22 Steps for 2025. Wiz.io, 2024. Режим доступу: https://www.wiz.io/academy/cloud-security-best-practices (переглянуто 2025).
14. A Guide to Cloud Security Frameworks. Sangfor, 2024. Режим доступу: https://www.sangfor.com/blog/cloud-and-infrastructure/guide-to-cloud-security-frameworks (переглянуто 2025).
15. How to Perform a Cloud Risk Assessment. Cymulate, 2025. Режим доступу: https://cymulate.com/blog/cloud-risk-assessment/ (переглянуто 2025).