МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ І.І.МЕЧНИКОВА
Кафедра комп'ютерних систем та технологій

"**ЗАТВЕРДЖУЮ**"
Проректор з науково-педагогічної роботи
_____ Т. Лохмакова
"09" 09 2025 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«Безпека хмарних технологій»

Рівень вищої освіти	**Перший (бакалаврський)**
Галузь знань	**12 – Інформаційні технології**
Спеціальність	**122 - Комп'ютерні науки**
Освітньо-професійна програма	**Комп'ютерні науки**

ОНУ
Одеса
2025

Робоча програма навчальної дисципліни «Безпека хмарних технологій». – Одеса: ОНУ, 2025. – 18с.

Розробник: Мартинович Лариса Ярославівна, старший викладач кафедри комп'ютерних систем та технологій,

Робоча програма затверджена на засіданні кафедри комп'ютерних систем та технологій ФМФІТ

Протокол №__1__від «_28_» 08 2025 р.

Завідувач кафедри _____ (Юрій ГУНЧЕНКО)
(підпис)

Погоджено із гарантом ОПП «Комп'ютерна інженерія»

_____ (Алла КАМЄНЄВА)
(підпис)

Схвалено навчально-методичною комісією (НМК) факультету математики, фізики та інформаційних технологій

Протокол №__1__ від «_29_» 08 2025 р.

Голова НМК _____ (Лариса МАРТИНОВИЧ)
(підпис)

Переглянуто та затверджено на засіданні кафедри комп'ютерних систем та технологій

Протокол №___від «___» _____20___ р.

Завідувач кафедри _____ (_____)
(підпис)

Переглянуто та затверджено на засіданні кафедри комп'ютерних систем та технологій

Протокол №___від «___» _____20___ р.

Завідувач кафедри _____ (_____)
(підпис)

1. Опис навчальної дисципліни

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, Спеціальність, спеціалізація, рівень вищої освіти</td><td>Характеристика навчальної дисципліни</td></tr>
<tr><td>Очна (денна) форма навчання</td></tr>
<tr><td rowspan="15">Загальна кількість
кредитів – 5
годин – 150
змістових модулів - 2</td><td rowspan="15">Галузь знань
12 – Інформаційні технології

Спеціальність:
122 – Комп’ютерні науки

Рівень вищої освіти:
<u>Перший</u>
<u>(бакалаврський)</u></td><td>Вибіркова дисципліна</td></tr>
<tr><td>Рік підготовки:</td></tr>
<tr><td>4-й</td></tr>
<tr><td>Семестр</td></tr>
<tr><td>8-й</td></tr>
<tr><td>Лекції</td></tr>
<tr><td>24 год.</td></tr>
<tr><td>Практичні, семінарські</td></tr>
<tr><td>0 год.</td></tr>
<tr><td>Лабораторні</td></tr>
<tr><td>36 год.</td></tr>
<tr><td>Самостійна робота</td></tr>
<tr><td>90 год.</td></tr>
<tr><td>Форма підсумкового контролю:
іспит</td></tr>
</table>

2. Мета та завдання навчальної дисципліни

Метою викладання дисципліни є – є вивчення принципів, технологій та інструментів, пов'язаних з використанням хмарних сервісів для забезпечення високої доступності, масштабованості та ефективності обчислювальних систем.

Завдання:

- формування у здобувачів комплексу знань з основних концепцій та моделей хмарних обчислень;
- вивчення принципів функціонування хмарних сервісів, їх функціональних можливостей;
- вивчення архітектури та інфраструктури хмарних обчислень, що реалізує безпеку в хмарі;
- вивчення інструментів та технологій для розгортання та керування хмарними ресурсами.

Процес вивчення дисципліни спрямований на формування елементів наступних **компетентностей.**

Інтегральна компетентність:

Здатність розв’язувати складні задачі і проблеми в галузі комп’ютерної інженерії або у процесі навчання, що передбачає проведення досліджень та/або здійснення інновацій та характеризується невизначеністю умов і вимог.

Загальні компетентності:

ЗК2. Здатність до абстрактного мислення, аналізу і синтезу.

ЗК6. Здатність виявляти, ставити та вирішувати проблеми.

ЗК7. Здатність приймати обґрунтовані рішення.

Спеціальні (фахові) компетентності:

СК1. Здатність до визначення технічних характеристик, конструктивних особливостей, застосування і експлуатації програмних, програмно-технічних засобів, комп'ютерних систем та мереж різного призначення.

СК3. Здатність проектувати комп'ютерні системи та мережі з урахуванням цілей, обмежень, технічних, економічних та правових аспектів.

СК11. Здатність обирати ефективні методи розв'язування складних задач комп'ютерної інженерії, критично оцінювати отримані результати та аргументувати прийняті рішення.

В результаті вивчення навчальної дисципліни здобувач вищої освіти повинен **знати**:

- основні хмарні сервіси
- побудову хмарної інфраструктури, її складові частини
- основні загрози безпеці в хмарних обчисленнях та методи їх запобігання та виявлення

вміти:

- критично аналізувати предметну область;
- вчитися і оволодівати новими сучасними знаннями;
- автоматизувати управління інфраструктурою хмарних середовищ
- вміти керувати ідентифікацією та доступом в хмарі
- володіти засобами забезпечення мережевого доступу до ресурсів хмари
- володіти доступними методами шифрування даних у спокої та під час передачі
- знати, як збирати дані про активність та події у мережі

Що забезпечують наступні **програмні результати навчання:**

РН3. Будувати та досліджувати моделі комп’ютерних систем і мереж, оцінювати їх адекватність, визначати межі застосовності.

РН6. Аналізувати проблематику, ідентифікувати та формулювати конкретні проблеми, що потребують вирішення, обирати ефективні методи їх вирішення.

РН11. Приймати ефективні рішення з питань розроблення, впровадження та експлуатації комп’ютерних систем і мереж, аналізувати альтернативи, оцінювати ризики та імовірні наслідки рішень.

ЗМІСТОВИЙ МОДУЛЬ 1. Стандарти, архітектура та принципи побудови розподілених систем на базі моделей сервісів і технологій хмарних платформ

Тема 1. Основні поняття та класифікація систем хмарних обчислень. Означення та ключові характеристики хмарних обчислень. Еволюція хмарних технологій: від Grid- та Utility-обчислень до сучасних гіперскейлерів. Класифікація хмарних систем за моделями та типами обчислень. Стандартизація у сфері хмарних технологій: роль NIST SP 800-145 та робота ISO/IEC JTC 1/SC 38.

Тема 2. Базові архітектури та компоненти хмарних платформ. Архітектура хмарних ЦОД: розподіленість, віртуалізація (роль гіпервізора та контейнеризації). Ключові складові хмарної інфраструктури. Принципи мультиорендності (Multi-tenancy). Концепція Програмно-визначених мереж (Software-Defined Networking, SDN) та Програмно-визначеної інфраструктури (Software-Defined Infrastructure, SDI) у контексті безпеки.

Тема 3. Сервісні моделі хмарних платформ (IaaS, PaaS, SaaS) та їх безпекові аспекти. IaaS (Infrastructure as a Service): управління, безпека на рівні хоста та мережі, віртуалізаційні ризики. PaaS (Platform as a Service): безпека рівня застосунків, середовище виконання, управління ідентифікацією та доступом (IAM) на рівні платформи. SaaS (Software as a Service): безпека даних, конфігурація доступу, ризики, пов'язані з довірою до постачальника. Функції як сервіс (FaaS/Serverless Computing): унікальні проблеми безпеки "холодного старту", управління секретами та ін'єкційні атаки.

Тема 4. Моделі розгортання хмарних платформ та ризики. Приватна (Private) хмара: архітектура, управління та відповідність корпоративним стандартам безпеки. Публічна (Public) хмара: висока доступність, масштабованість, але залежність від постачальника та необхідність посиленого контролю конфігурацій. Гібридна (Hybrid) хмара: забезпечення безперервності безпеки при переході між приватним та публічним середовищами (Cloud Bursting). Мультихмарне (Multi-cloud) середовище: управління єдиною політикою безпеки, взаємодія різних провайдерів (Interoperability) та уніфікація інструментів.

ЗМІСТОВИЙ МОДУЛЬ 2. Хмарні платформи: принципи функціонування та побудови. Переваги різних провайдерів та їх комбінація. Способи та моделі захисту в хмарі, різні типи відповідальності.

Тема 5. Загальний огляд сучасних платформ. Хмарна платформа Google Cloud Platform (GCP). Модель Спільної Відповідальності (Shared Responsibility Model): детальний аналіз меж відповідальності між клієнтом та провайдером. GCP Security: філософія "Zero Trust" (BeyondCorp) від Google.

Ключові безпекові компоненти GCP: Cloud Identity and Access Management (IAM), Cloud Armor (WAF/DDoS), VPC Service Controls, Security Command Center (SCC). Огляд інструментів для безпеки даних у GCP: KMS, Secret Manager, Cloud Data Loss Prevention (DLP).

Тема 6. Платформа хмарних обчислень Amazon Web Services (AWS). Архітектура безпеки AWS: багатошаровий захист. AWS Security Tools: детальний розгляд IAM (Policies, Roles, Users), Security Hub, GuardDuty (Threat Detection), Inspector (Vulnerability Management). Безпека мережі в AWS: VPC (Virtual Private Cloud), Security Groups, Network ACLs, Transit Gateway. Захист об'єктних сховищ S3: політики доступу (Bucket Policies), шифрування та логування доступу.

Тема 7. Можливості хмарних послуг Microsoft Azure. Azure Security Strategy: концепція Defence in Depth та інтеграція з корпоративними рішеннями Microsoft. Ключові безпекові сервіси Azure: Azure Active Directory (Azure AD), Azure Security Center (Defender for Cloud), Azure Key Vault (Secrets Management). Azure Sentinel (SIEM/SOAR): автоматизація реакції на інциденти та управління інформацією про безпеку. Забезпечення відповідності (Compliance) та регуляторні вимоги в Azure (наприклад, GDPR, HIPAA) через Azure Policy.

Тема 8. Безпека доступу та хмарні ресурси. Управління ідентифікацією та доступом (IAM): реалізація принципу найменших привілеїв (Least Privilege), рольовий контроль доступу (RBAC), умовний доступ. Багатофакторна автентифікація (MFA) та автентифікація на основі адаптивного ризику. Управління секретами (Secrets Management): використання Key Management Services (KMS) та спеціалізованих сховищ секретів. Безпека API: захист хмарних API-інтерфейсів, API Gateway, управління токенами та лімітуванням запитів.

4. Структура навчальної дисципліни «Безпека хмарних технологій»

Назва тем	Кількість годин				
	Очна (денна) форма				
	Усього	у тому числі			
		Лек.	Пр.	Лаб.	СР
1	**2**	**3**	**4**	**5**	**6**
Змістовий модуль 1. Стандарти, архітектура та принципи побудови розподілених систем на базі моделей сервісів і технологій хмарних платформ					
Тема 1. Основні поняття та класифікація систем хмарних обчислень.	14	2			12
Тема 2. Базові архітектури та компоненти хмарних платформ. .	18	2		4	12
Тема 3. Сервісні моделі хмарних платформ.	18	4		4	10
Тема 4. Моделі розгортання хмарних платформ	20	4		6	10
Разом за змістовим модулем 1	**70**	**12**		**14**	**44**
Змістовий модуль 2. Хмарні платформи: принципи функціонування та побудови. переваги різних провайдерів та їх комбінація. Способи та моделі захисту в хмарі, різні типи відповідальності.					
Тема 5. Загальний огляд сучасних платформ. Хмарна платформа Google Cloud Platform. Основні компоненти та їх призначення.	16	2		4	10
Тема 6. Платформа хмарних обчислень Amazon Web Services (AWS).	20	2		6	12
Тема 7. Можливості хмарних послуг Microsoft Azure.	22	4		6	12
Тема 8. Безпека доступу та хмарні ресурси.	22	4		6	12
Разом за змістовим модулем 2	**80**	**12**		**22**	**46**
Усього годин	**150**	**24**		**36**	**90**

5. Теми семінарських занять

Семінарські заняття не передбачені навчальним планом.

6. Теми практичних занять

Практичні заняття не передбачені навчальним планом.

7. Теми лабораторних робіт

№	Назва теми	Кількість годин
1.	Провести порівняльний аналіз розподілу відповідальності за безпеку даних, операційної системи, мережі та застосунків між клієнтом і провайдером у моделях IaaS, PaaS та Serverless (FaaS).	6
2.	Дослідити впровадження моделі Zero Trust у хмарних середовищах.	6
3.	Життєвий цикл IAM-облікових записів та використання тимчасових облікових даних.	6
4.	Дослідити принципи роботи Key Management Service (KMS) та порівняти підходи BYOK (Bring Your Own Key) та HYOK (Hold Your Own Key) з точки зору контролю та комплаєнсу.	8
5.	Розробити алгоритм реагування на типовий хмарний інцидент (наприклад, скомпрометований обліковий запис адміністратора).	10
	Разом	**36**

8. Самостійна робота

№	Назва теми/питання для підготовки, завдання	Кількість годин
1.	Поглиблений аналіз моделі спільної відповідальності та ризиків сервісних моделей	10
2.	Архітектура Zero Trust та криптографічне розмежування	10
3.	Комплексне управління ідентичністю та доступом (IAM)	10
4.	Захист даних: KMS, BYOK, HYOK та Confidential Computing	10
5.	DevSecOps та автоматизація безпеки у CI/CD	10
6.	Безпека контейнерних та Serverless-середовищ	8
7.	Cloud Security Posture Management (CSPM) та запобігання Misconfiguration	8
8.	Cloud Access Security Brokers (CASB) та запобігання втраті даних (DLP)	8
9.	Регуляторний комплаєнс, Data Sovereignty та хмарні стандарти	8

10.	Реагування на інциденти та хмарна форензика	8
	Разом	**90**

В якості самостійної роботи здобувач може пройти професійні курси тренінги, професійне стажування, он-лайн курси, громадянську освіту, отримати сертифікат на освітніх платформах, що може бути зараховано як періодичний, поточний та фрагмент підсумкового контролю.

Здобувач може самостійно обрати ресурси, які будуть відповідати навчальній дисципліні. Для зарахування в якості періодичного, поточного, фрагмента підсумкового контролю, виконання частини практичних (лабораторних) завдань здобувач має подати документи, що підтверджують неформальну освіту, програми, зробити опис компетентностей та результатів навчання (р.2), сформованих під час неформальної освіти.

Викладач залишає за собою право перевірити сформованість перелічених компетентностей та результатів навчання.

9. Методи навчання

- **Словесні**: лекції (проблемні, лекції-візуалізації, лекції з аналізом конкретних ситуацій та ін.), розповідь, пояснення, бесіда, дискусія, диспут, обговорення проблемних ситуацій, ситуаційне навчання тощо.
- **Наочні**: ілюстрація (у тому числі мультимедійні презентації), демонстрація, метод безпосереднього спостереження, презентація результатів власних досліджень.
- **Практичні**: вправи; тренувальні вправи; розв'язання розрахункових задач; практичні роботи; лабораторні роботи; метод проєктів (проєктування); ділові ігри; рольові ігри; виконання індивідуальних завдань.

Методи організації та здійснення навчально-пізнавальної діяльності:

а) за джерелом інформації – словесні (пояснення, розповідь, бесіда), наочні (спостереження, демонстрація), практичні (моделювання).

б) за логікою передачі і сприймання навчальної інформації (індуктивні, дедуктивні, аналітичні, синтетичні);

в) за ступенем самостійності мислення (репродуктивні, пошукові, дослідницькі);

г) за ступенем керування навчальною діяльністю (під керівництвом викладача, самостійна робота студентів).

2. Методи стимулювання інтересу до навчання і мотивації навчально-пізнавальної діяльності: навчальні дискусії, створення ситуації пізнавальної новизни, інтерактивні вправи та завдання.

Під час проведення лекцій використовуються наступні методи навчання: пояснювально-ілюстративний метод, інформаційно-рецептивний; репродуктивний метод (репродукція - відтворення); метод проблемного викладу; частково-пошуковий метод.

Під час практичних занять використовуються наступні методи навчання частково-пошуковий, або евристичний метод; дослідницький, при захисті лабораторних робіт та індивідуальних завдань використовується дискусійний метод.

10. Форми контролю і методи оцінювання

Контроль здійснюється з дотриманням вимог об'єктивності, індивідуального підходу, систематичності і системності та всебічності.

поточний контроль – опитування; оцінювання індивідуальної роботи, доповідей, PowerPoint презентацій; письмових завдань різних типів (вправ, анотацій, оформлення бібліографії та посилань);

періодичний контроль – ;

підсумковий контроль – залік.

Критерії оцінювання результатів навчання здобувачів другого (магістерського) рівня вищої освіти

Оцінка за національною шкалою для заліку та іспиту	**100 бальна шкала / Оцінка ECTS**	**Теоретична підготовка**	**Практична підготовка**
Зараховано / відмінно	**90-100/ A**	Здобувач у повному обсязі володіє навчальним матеріалом, вільно, розгорнуто, обґрунтовано та аргументовано його викладає під час усних виступів та письмових відповідей. Здобувач демонструє чітке знання відповідних категорій, їх змісту, розуміння їх взаємозв'язку, правильно формулює тлумачення відповідних понять, демонструє знання змісту передбачених програмою робить самостійні висновки. Здобувач вміє самостійно знаходити додаткову інформацію та використовувати її для реалізації поставлених завдань, вільно використовує нові інформаційні технології для поповнення знань.	Здобувач може аргументовано обрати раціональний спосіб виконання практичних завдань, виконує практичні завдання не передбачені навчальною програмою, вільно використовує набуті теоретичні знання при аналізі практичного матеріалу, проявляє творчий підхід до виконання індивідуальних та колективних завдань при самостійній роботі.
Зараховано / добре	**85 – 89 / B**	Здобувач достатньо повно володіє навчальним матеріалом, обґрунтовано його викладає під час усних виступів та письмових відповідей, використовуючи при цьому обов'язкову літературу, застосовує знання для розв'язання стандартних ситуацій, самостійно аналізує, узагальнює і систематизує навчальну інформацію, але допускає неточності, які не є суттєвими для характеристики предмету питання та не впливають істотно на загальну	Здобувач має стійкі навички виконання практичних завдань, правильно вирішує більшість практичних завдань.

		характеристику того чи іншого явища (поняття).	
Зараховано / добре	**75 – 84 / C**	Здобувач виявляє загалом високий рівень знань щодо всієї програми навчальної дисципліни, на достатньому рівні володіє навчальним матеріалом, застосовує знання для розв'язання стандартних ситуацій, але не вміє самостійно аналізувати деякі питання, не повністю переконливо аргументувати свої відповіді, допускає незначні неточності.	Здобувач за зразком самостійно виконує практичні завдання, передбачені програмою навчальної дисципліни.
Зараховано / задовільно	**70 – 74 / D**	Здобувач володіє навчальним матеріалом на репродуктивному рівні або відтворює певну частину навчального матеріалу з елементами логічних зв'язків. Здобувач знає основні поняття навчального матеріалу, але має ускладнення під час виділення суттєвих ознак вивченого та під час виявлення причинно-наслідкових зв'язків та формулювання висновків.	Здобувач має елементарні навички виконання практичних завдань, правильно вирішує лише половину практичних завдань.
Зараховано / задовільно	**60 – 69 / E**	Здобувач не повною мірою розуміє предмет навчальної дисципліни, наявні недоліки у розкритті змісту понять. Здобувач надає нечіткі характеристики відповідних явищ, викладає свої думки з істотним порушенням логіки подання матеріалу.	Здобувач може використовувати знання лише в стандартних практичних ситуаціях, має нестійкі навички виконання практичних завдань, робить багато суттєвих помилок.
Не зараховано з можливістю повторного складання/	**35 – 59 / FX**	Здобувач неправильно розкриває сутність базових питань навчальної дисципліни, допускає суттєві змістові помилки, володіє навчальним матеріалом поверхнево й фрагментарно, безсистемне виокремлює випадкові ознаки вивченого, не вміє сформулювати свою думку та викласти її в логічній послідовності, робити узагальнення та висновки.	Здобувач здатний виконати лише окремі практичні завдання за допомогою викладача. У здобувача відсутні сформовані уміння та навички.
Не зараховано з обов'язковим повторним вивченням дисципліни/	**0 – 34 / F**	Здобувач не знає основних положень навчальної дисципліни, не володіє навчальним матеріалом.	Здобувач виконує лише елементи практичних завдань, потребує постійної допомоги викладача.

10. Форми контролю та методи оцінювання

Поточний контроль здійснюється за результатами виконання 2 контрольних робіт, захисту завдань лабораторних робіт. Оцінюється також активність студента в процесі занять: усне опитування на лекції, написання звітів до лабораторних робіт, їх захист, розв'язання практичних задач. Підсумковий контроль - залік.

При оцінюванні в балах рівня засвоєння матеріалу використовуються загальні критерії оцінювання навчальних досягнень здобувачів вищої освіти:

Критерії оцінювання підсумкового контролю

Підсумковий семестровий контроль (залік) проводиться в накопичувальній формі. Кількість балів, що здобувач отримав на заліку, є сумою балів, що були отримані за кожне завдання поточного та періодичного контролю. Кінцева оцінка виставляється за шкалою, що наведена нижче (п.12).

11. Питання для підготовки для поточного та підсумкового контролю.

Частина І: Основи та архітектура (Питання 1-10)

1. Поясніть сутність Моделі спільної відповідальності (Shared Responsibility Model). Наведіть приклад конкретного ризику, за який відповідає клієнт у моделі PaaS, і ризику, за який відповідає провайдер.
2. Опишіть архітектурну роль та основні функції CASB (Cloud Access Security Broker). Як CASB допомагає у реалізації політики DLP (Data Loss Prevention) між локальною мережею та хмарними сервісами SaaS?
3. Проаналізуйте принцип Zero Trust у контексті хмарних мікросервісних архітектур. Як концепція "периметра, що визначається ідентичністю" замінює традиційний мережевий периметр?
4. Яка критична відмінність між Атрибутивним контролем доступу (ABAC) та Рольовим контролем доступу (RBAC)? Наведіть сценарій у хмарі (наприклад, AWS, Azure), де використання ABAC є більш вигідним.
5. Що таке Confidential Computing і яке ключове обмеження традиційного шифрування (дані в стані спокою та в процесі передачі) воно покликане вирішити за допомогою апаратних анклавів (TEE)?
6. Обґрунтуйте, чому помилкова конфігурація (Cloud Misconfiguration) вважається найбільшою загрозою для хмарної безпеки. Який інструментальний підхід (наприклад, CSPM) використовується для її запобігання та моніторингу?
7. Поясніть концепцію Data Sovereignty (Суверенітет даних) та Data Residence (Резиденція даних). Який вплив це має на стратегію розміщення конфіденційних даних (наприклад, персональних даних, що регулюються GDPR)?
8. Опишіть механізм Federated Identity (Федеративна ідентифікація) (наприклад, з використанням SAML або OIDC) і його значення для реалізації Single Sign-On (SSO) у гібридному хмарному середовищі.
9. У чому полягає відмінність між мережевими механізмами контролю Security Groups та Network Access Control Lists (NACLs) у хмарі? Наведіть ключові відмінності щодо stateful/stateless роботи.
10. Як Infrastructure as Code (IaC), зокрема використання таких інструментів як Terraform або CloudFormation, сприяє реалізації підходу Shift Left у безпеці?

Частина ІІ: Безпека робочих навантажень та даних (Питання 11-20)

11. Детально поясніть різницю між BYOK (Bring Your Own Key) та HYOK (Hold Your Own Key) у контексті сервісів управління ключами (KMS). Який підхід забезпечує вищий рівень контролю для клієнта?

12. Які унікальні проблеми безпеки виникають у середовищах Serverless (FaaS) порівняно з традиційними VM? Зосередьтеся на питанні IAM-дозволів функції та Cold Start ризиків.

13. Що таке Container Image Scanning (Сканування образів контейнерів) і на якому етапі CI/CD пайплайну його необхідно інтегрувати для ефективного запобігання Supply Chain Attacks (Атакам ланцюга постачання)?

14. Опишіть призначення та принцип дії DAST (Dynamic Application Security Testing). Чому DAST є важливішим для хмарної безпеки, ніж SAST при виявленні вразливостей, пов'язаних з логікою виконання?

15. Яку функцію виконує Web Application Firewall (WAF) у хмарній архітектурі? Наведіть приклади трьох видів атак із переліку OWASP Top 10, від яких WAF забезпечує захист.

16. Поясніть ризик Over-Privileging (Надлишкові привілеї) та його наслідки. Як інструменти CIEM (Cloud Infrastructure Entitlement Management) допомагають у вирішенні цієї проблеми?

17. У чому полягає ризик 'бічного руху' (Lateral Movement) у хмарній мережі? Як Мікросегментація (Microsegmentation) допомагає мінімізувати потенційну шкоду від такої атаки?

18. Обґрунтуйте необхідність використання Secret Management (Сховища секретів) у хмарі (наприклад, AWS Secrets Manager, Azure Key Vault). Які ризики виникають при зберіганні секретів у коді чи змінних середовища?

19. Яка роль Hardware Security Modules (HSMs) у хмарних KMS? Як вони підвищують безпеку ключів шифрування порівняно з програмними рішеннями?

20. Які заходи безпеки потрібно вжити для захисту API-інтерфейсів у хмарі (наприклад, API Gateway), щоб запобігти несанкціонованому доступу та надмірному використанню (rate limiting)?

Частина III: Комплаєнс, аудит та управління ризиками (Питання 21-30)

21. Які основні етапи включає процес Cloud Risk Assessment (Оцінка хмарних ризиків)? На чому слід зосередитися при аналізі загроз, пов'язаних із зовнішніми інтеграціями?

22. Поясніть, як механізми журналювання та аудиту (CloudTrail, Azure Monitor) використовуються у процесі розслідування інцидентів (Incident Response). Яка інформація є найважливішою для проведення хмарної форензики?

23. Опишіть принцип Імутабельності інфраструктури (Immutable Infrastructure) і те, як він впливає на безпеку та управління патчами.

24. Як застосування політик безпеки у вигляді коду (Security-as-Code) допомагає забезпечити відповідність (Compliance) та запобігти відхиленню від базової конфігурації (Configuration Drift)?

25. Розкрийте поняття Вендорний локін (Vendor Lock-in) у контексті безпеки хмари. Які стратегії можуть бути використані для його мінімізації?

26. Які ризики пов'язані з використанням загальнодоступних репозиторіїв (наприклад, Docker Hub, PyPI) для отримання базових образів/бібліотек? Яким чином ці ризики можна пом'якшити?

27. Що таке Cloud Security Alliance (CSA) Star та CIS Benchmarks? Поясніть їхнє значення для клієнтів при виборі та налаштуванні хмарних сервісів.

28. Поясніть важливість ротації секретів (Secret Rotation) та тимчасових облікових даних (Temporary Credentials) у хмарі. Як це знижує ризик, пов'язаний із компрометацією довгострокових ключів доступу?

29. У чому полягає відмінність між ізоляцією на рівні гіпервізора та ізоляцією на рівні контейнера (наприклад, у Kubernetes)? Які наслідки для безпеки несе порушення ізоляції в обох випадках?

30. Який міжнародний стандарт безпеки (наприклад, ISO/IEC 27017) найбільш релевантний для аудиту та оцінки безпеки хмарних сервісів і чому?

12. Розподіл балів, які отримують здобувачі

Поточний та періодичний контроль відбувається у ***Google Classroom*** та через усне спілкування на занятті. У ході поточного контролю здобувач вищої освіти може отримати від 7 до 13 балів за кожну тему змістового модуля.

Загальна оцінка з навчальної дисципліни – це сума балів за поточний та періодичний контроль.

Поточний та періодичний контроль								**Іспит**	**Сума балів**
Змістовий модуль 1				**Змістовий модуль 2**					
Т1	Т2	Т3	Т4	Т5	Т6	Т7	Т8	20	100
6	6	6	8	8	8	8	10		
Контрольна робота 1 - 10				Контрольна робота 2 - 10					

Т1…Т8 – теми, КР – контрольна робота.

Контрольна робота здійснюється у формі письмових тестових завдань після вивчення матеріалу кожного змістового модуля. Тестові письмові завдання для модульних контрольних робіт складаються з 5 тестових завдань і відповідають змісту навчального матеріалу модуля. За кожну правильну відповідь на одне тестове завдання студент отримує 3 бали.

Зарахування результатів неформальної освіти

Наявність у здобувача дійсних на час проходження навчання за курсом “Безпека хмарних технологій” сертифікатів від однієї з платформ:

1. Google Cloud Platform;
2. Amazon Web Services (AWS);
3. Microsoft Azure;

може бути зарахована за повний курс дисципліни.

Наявність бейджів навичок або сертифікатів про успішне проходження навчання за програмами на платформі GCP від Google Cloud Skills Boost: зараховується, як виконання лабораторних робіт, з додаванням відповідної кількості балів до підсумкової оцінки.

Для зарахування навчання у інших представників неформальної освіти здобувач має подати документи, що підтверджують таку освіту, програми, зробити опис компетентностей та результатів навчання, сформованих під час неформальної освіти.

Шкала оцінювання: національна та ECTS

Сума балів за всі види навчальної діяльності		**Оцінка за національною шкалою**	
	Оцінка ЄКТС	для екзамену, курсового проекту (роботу), практики	для заліку
90 – 100	A	відмінно	зараховано
85-89	B	добре	
75-84	C		
70-74	D	задовільно	
60-69	E		
35-59	FX	незадовільно	не зараховано
1-34	F		

13. Навчально-методичне забезпечення

Навчально-методичне забезпечення: робоча програма навчальної дисципліни; силабус, конспекти лекцій; презентації; методичні вказівки до виконання лабораторних робіт, первинний інструктаж з техніки безпеки, порядок виконання лабораторних робіт на платформі.

14. Рекомендована література

Основна

1. John Culkin, Mike Zazon. AWS Cookbook: Recipes for Success on AWS. — 1st Edition — O'Reilly Media, 2022 — 356 p.

2. Reza Salehi. Azure Cookbook: Recipes to Create and Maintain Cloud Solutions in Azure. — 1st Edition — O'Reilly Media, 2023 — 332 p.

3. Rui Costa, Drew Hodun. Google Cloud Cookbook: Practical Solutions for Building and Deploying Cloud Services. — 1st Edition — O'Reilly Media, 2021 — 282 p.

4. Sean P. Kane, Karl Matthias. Docker: Up & Running: Shipping Reliable Containers in Production. — 3rd Edition — O'Reilly Media, 2023 — 422 p.

5. Alan Hohn. The Book of Kubernetes: A Complete Guide to Container Orchestration. — No Starch Press, 2022 — 384 p.

6. Chris Richardson. Microservices Patterns: With examples in Java. — 1st Edition — Manning, 2018 — 520 p.

7. Thomas Erl, Zaigham Mahmood, and Ricardo Puttini. Cloud Computing Concepts, Technology & Architecture. Prentice Hall, 2013 . - 528 p.

8. Ray J Rafaels. Cloud Computing: From Beginning to End. CreateSpace Independent Publishing Platform, 2015 – 152p.

Додаткова

9. AWS Documentation. https://docs.aws.amazon.com/

10. Azure documentation. https://learn.microsoft.com/en-us/azure/

11. Google Cloud documentation. https://cloud.google.com/docs/

12. Yevgeniy Brikman. Terraform: Up and Running: Writing Infrastructure as Code. — 3rd Edition — O'Reilly Media, 2022 — 457 p.

15. Електронні інформаційні ресурси

1. https://mon.gov.ua/ – офіційний сайт Міністерства освіти і науки України;
2. http://nbuv.gov.ua/ - Сайт Національної бібліотеки України імені В. І. Вернадського;
3. http://www.dnpb.gov.ua/ - Сайт Державної науково-педагогічної бібліотеки України імені В.О. Сухомлинського;
4. http://onu.edu.ua/- Сайт бібліотеки ОНУ імені 1.1. Мечникова;
5. http://odnb.odessa.ua/ - Сайт Одеської національної наукової бібліотеки;
6. http://korolenko.kharkov.com/ - Сайт Харківської державної наукової бібліотеки імені В.Г. Короленка.
7. https://cloudonair.withgoogle.com/events/cloud-for-students/resources - Матеріали вебінарів для студентів на платформі GCP
8. https://www.cloudskillsboost.google/ - навчання, заходи та тестування на платформі GCP від Google Cloud Skills Boost
9. https://aws.amazon.com/training/?intClick=gsrc_navbar – навчання та сертифікація AWS
10. https://learn.microsoft.com/uk-ua/training/browse/?products=azure - навчання та сертифікація Microsoft Azure