Міністерство освіти і науки України
Національний університет «Чернігівська політехніка»
Навчально-науковий інститут електронних та інформаційних технологій
Кафедра кібербезпеки та математичного моделювання

РОБОЧА ПРОГРАМА
Безпека в хмарних технологіях

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ __Ткач Ю.М.__
(підпис) (прізвище та ініціали)

«_26_» ___08_____ 2025 р.

Розробник (-и): Базилевич В.М., директор ННІ ЕІТ, к.е.н., доцент, _____
(прізвище та ініціали, посада, науковий ступінь і вчене звання) (підпис)

Силабус навчальної дисципліни обговорено на засіданні кафедри кібербезпеки та математичного моделювання

Протокол від «_26____»__08_____2025р. №_6___

Узгоджено з гарантом освітньої програми: _____ _____Ю.М.Ткач_____
(підпис) (прізвище та ініціали)

---

1. Загальна інформація про дисципліну.

Тип дисципліни	*Вибіркова*
Мова викладання	Українська/англійська
Рік навчання та семестр	2025-2026 навчальний рік, І семестр, ОП Кібербезпека за спеціальністю F5 Кібербезпека та захист інформації галузь знань F Інформаційні технології
Викладач (-і)	Базилевич Володимир Маркович, директор ННІ ЕІТ, кандидат економічних наук наук, доцент
Профайл викладача (-ів)	https://cs.stu.cn.ua/bazylevych-volodymyr-markovych/
Контакти викладача	bazvlamar@stu.cn.ua

2. Анотація курсу.

Дисципліна «Безпека в хмарних технологіях» є важливою складовою підготовки фахівців у галузі кібербезпеки, яка фокусується на вивченні сучасних технологій та інструментів для забезпечення безпеки. Цей курс знайомить вас із кібербезпекою для хмари. Ми вивчимо та застосуємо класичні методи безпеки для сучасних проблем безпеки в хмарі. Ми проаналізуємо останні вразливості хмарної безпеки, використовуючи стандартні систематичні методи. Розглянемо сучасні та майбутні тренди.

3. Мета та цілі курсу.

Метою дисципліни є надання студентам знань і практичних навичок для забезпечення безпеки в хмарних технологіях. Вони мають навчитися виявляти та усувати вразливості, впроваджувати ефективні механізми захисту даних і користувачів.

Цілі курсу:

1. Ознайомити студентів з основними принципами та концепціями безпеки в хмарних технологіях.
2. Навчити студентів ідентифікувати типові загрози безпеки в хмарних середовищах.
3. Надати студентам практичні навички використання інструментів на хмарних серверах.
4. Вміння впроваджувати стратегії захисту для запобігання атакам.
5. Поглибити розуміння принципів шифрування та захисту даних.
6. Ознайомити студентів з правовими аспектами кібербезпеки в контексті хмарних технологій, зокрема, GDPR, закони про захист персональних даних.

4. Результати навчання:

ПРН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.

ПРН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.

КЗ 1. Здатність застосовувати знання у практичних ситуаціях.

КЗ 3. Здатність до абстрактного мислення, аналізу та синтезу.

КЗ 4. Здатність оцінювати та забезпечувати якість виконуваних робіт.

КФ 2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки

КФ 3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури.

5. Пререквізити.

Базові знання за темами: Основи комп’ютерних мереж та їх безпеки. Технології програмування. Бази даних. Базові поняття інфраструктури ПЗ, контейнеризації та віртуалізації.

6. Обсяг курсу:

Вид заняття	Загальна кількість годин денна/заочна
Лекції	16/6
Лабораторні заняття	16/6
Самостійна робота	88/108
Всього кредитів	4

Лекційні, лабораторні роботи, самостійна робота – з використанням системи дистанційного навчання Moodle, Teams, рекомендованих джерел, відеоматеріалів тощо.

7. Тематика курсу.

Лекції (16/6 годин):

Вступ до хмарних технологій (2 години)

Термінологія та історія хмарних технологій. Суть та характеристики хмарних технологій. Моделі хмарного розміщення та їх класифікація. Переваги та недоліки..

Сценарії використання хмарних технологій (2 години)

Користувальницький сегмент. Освіта. Ігрові онлайн-сервіси. Персональна продуктивність. Бізнес-сегмент. Рітейл. Управління персоналом. Blockchain.

Загрози в хмарних середовищах (4 години)

Загрози для безпеки в хмарі. Конфігурація хмари. Політики віддаленої роботи на особистих пристроях. Соціальна інженерія та інші види кіберзагроз.

Шифрування даних у хмарах (4 години)

Основні поняття шифрування. Шифрування даних у хмарах. Моделі управління ключами. Переваги шифрування даних у хмарах. Виклики та ризики. Кращі практики шифрування в хмарах. Приклади хмарних сервісів з шифруванням. Майбутні тренди.

Управління доступом та ідентифікація (IAM) (4 години)

Основні компоненти IAM. Методи автентифікації. Управління доступом. Реалізація та інструменти IAM. Виклики та загрози в IAM. Кращі практики IAM.

Лабораторні роботи (16 годин):

Моделі надання хмарних послуг (2 години)

Моделі надання IT-послуг: PaaS, SaaS, DaaS, WaaS, CaaS, EaaS

Архітектура і пропозиції від провідних компаній надання хмарних послуг (2 години)

приватна хмара (Private Cloud);
загальна хмара (Community Cloud);
публічна хмара (Public Cloud);
гібридна хмара (Hybri Cloud).

Досвід використання хмарних технологій за кордоном (2 години)

Аналіз та огляд найбільших компаній які надають послуги хмарних технологій.

Практичне використання SSL/TLS для захисту (2 години)

Налаштування SSL/TLS для захисту передавання даних між сервером та клієнтом.
Аналіз ризиків від використання незахищених з’єднань і впровадження HTTPS.

Створення VM на Amazon Web Services (2 години)

Створення аккаунта на AWS
Створення ВМ в AWS
Налаштування ВМ в AWS.

Навчання по роботі з сервісами AWS (2 години)

S3 Bucket
Основи EC2
Інстанси

Налаштування механізмів аутентифікації та авторизації (2 години)

Практичне налаштування аутентифікації.
Налаштування складних паролів, двофакторної аутентифікації.
Визначення та усунення потенційних вразливостей в механізмах авторизації.

Правові вимоги до безпеки web-ресурсів: GDPR та PCI DSS (2 години)

Аналіз вимог до безпеки хмарних сервісів з точки зору GDPR та PCI DSS.
Практичні рекомендації для забезпечення відповідності вимогам GDPR та PCI DSS.

Самостійна робота (88 годин):

Самостійна робота студентів є важливою складовою навчального процесу і сприяє глибшому засвоєнню тем, пов'язаних з безпекою в хмарних технологіях.

Самостійна робота – з використанням системи дистанційного навчання університету, рекомендованих інформаційних джерел, презентацій, нормативно-правових актів тощо.

Опрацювання теоретичних матеріалів (20 год)

Вивчення додаткової літератури та стандартів з безпеки хмарних технологій (ISO/IEC 27017, NIST SP 800-144).

Аналіз моделей хмарного розгортання: Private, Public, Hybrid, Community.

Порівняння архітектурних підходів у провайдерів (AWS, Azure, Google Cloud).

Підготовка конспекту-огляду (2–3 сторінки) за результатами аналізу.

Підготовка до лекцій і лабораторних занять (18 год)

Опрацювання тематики кожної лекції перед заняттям (читання статей, перегляд відео-уроків).

Ознайомлення з інструментами, які будуть використані на лабораторних (AWS Free Tier, OpenSSL, Wireshark, Burp Suite).

Виконання контрольних питань після лекцій (по 5–7 питань на тему).

Реферативні та аналітичні завдання (16 год)

Написання короткого реферату (5–7 сторінок) на одну із тем:

Використання хмарних сервісів в освіті та бізнесі.

Проблеми соціальної інженерії у хмарних середовищах.

Шифрування даних у хмарі: виклики та перспективи.

Системи IAM у провайдерів AWS/Azure/Google Cloud.

Презентація результатів у групі (короткий виступ 3–5 хв).

Міні-проекти та практичні завдання (18 год)

Налаштувати тестове середовище в одній з хмарних платформ (AWS, Azure, GCP Free Tier).

Виконати кейси:

створення S3 Bucket з базовими політиками доступу;

налаштування HTTPS для веб-ресурсу;

демонстрація прикладу атаки «людина посередині» (MITM) та способів захисту.

Підготувати скріншоти, конфігураційні файли й пояснення (звіт 3–4 сторінки).

Підготовка до тестування та модульного контролю (8 год)

Складання глосарію основних термінів (не менше 50 понять).

Підготовка відповідей на контрольні запитання до кожної теми.

Робота з тренажерами (наприклад, AWS Skill Builder або Coursera Free Cloud Security Labs).

Виконання індивідуальної роботи (8 год)

Вибір теми (наприклад: *OAuth у хмарних сервісах*, *Політики доступу в AWS*, *Шифрування у Microsoft Azure*).

- Розробка плану, підбір матеріалів.
- Виконання практичної частини (налаштування політик/тестування механізму).
- Оформлення звіту (10–15 сторінок).

8. Система оцінювання та вимоги

Загальна система оцінювання курсу	Оцінювання курсу базується на **накопичувальній системі** та включає: **поточний контроль** (оцінювання лабораторних занять) – 50 балів, **проміжний модульний контроль** – 25 балів **та підсумковий контроль** – 25 балів. Оцінювання кожного виду діяльності здійснюється окремо відповідно до **досягнення навчальних цілей**.
Вимоги до РГР, КР, КП тощо	Відсутні
Практичні заняття	Оцінка кожного лабораторного заняття здійснюється за наступними критеріями: 1) виконання практичного завдання – **6 бали;** 2) аналіз отриманих результатів – **2 бал**; 3) належне оформлення звіту – **2 бал.**
Умови допуску до підсумкового контролю	1. Отримання не менше 35 балів протягом семестру (лабораторні + проміжний контроль). 2. Відвідування щонайменше 50% занять.

Розподіл балів, які отримують здобувачі вищої освіти

Модуль за тематичним планом дисципліни та форма контролю		**Кількість балів**
Змістовий модуль 1.		**75**
1	Тема 1. Вступ до хмарних технологій	**15**
2	Тема 2. Сценарії використання хмарних технологій	**15**
3	Тема 3. Загрози в хмарних середовищах	**15**
4	Тема 4. Шифрування даних у хмарах	**15**
5	Тема 5. Управління доступом та ідентифікація (IAM)	**15**
Усього поточний і проміжний модульний контроль		**75**
Семестровий контроль (Екзамен)		**25**
Разом		**0…100**

Шкала оцінювання результатів навчання

Оцінка в балах	**Оцінка ECTS**	**Оцінка за національною шкалою (диференційований залік)**	
		для екзамену (диференційованого заліку), курсового проєкту (роботи), практики, атестації	для заліку
90 – 100	**A** (*відмінно*)	відмінно	зараховано
82-89	**B** (*дуже добре*)	добре	
75-81	**C** (*добре*)		
66-74	**D** (*задовільно*)	задовільно	
60-65	**E** (*достатньо*)		

0-59	**FX** (*незадовільно*)	незадовільно з можливістю повторного складання	незараховано з можливістю повторного складання

9. Обладнання та програмне забезпечення.

При вивченні курсу використовується наступне **обладнання та програмне забезпечення**:

І. Апартне забезпечення:

Персональні комп'ютери або ноутбуки з підтримкою віртуалізації та можливістю роботи з образами дисків та цифровими доказами.

Операційні системи: Windows 10/11 Pro, Linux (Ubuntu, Kali Linux – для аналізу вразливостей), macOS.

ІІ. Програмне забезпечення:

1. Для дослідження операційних систем та лог-файлів:

Registry Explorer – аналіз реєстру Windows.

Event Log Explorer – дослідження журналів подій Windows.

Plaso, Timesketch – створення хронологій подій на основі логів системи.

2. Для термінального підключення

MobaXterm – SSH клієнт

3. Для аналізу трафіку:

Wireshark – аналіз мережевого трафіку.

4. Платформи для дистанційного навчання:

Moodle, Microsoft Teams – розміщення навчальних матеріалів, тестування та проведення лекцій.

Google Drive, OneDrive – спільна робота з документами та звітами.

Використання наведеного обладнання та програмного забезпечення дозволяє студентам отримати практичний досвід у сфері цифрової криміналістики та підготуватися до роботи в реальних криміналістичних розслідуваннях.

10. Політики курсу.

У випадку, якщо здобувач протягом семестру не виконав у повному обсязі всіх видів навчальної роботи, має невідпрацьовані лабораторні роботи або не набрав мінімально необхідну кількість балів (35), він не допускається до складання екзамену під час семестрового контролю, але має право ліквідувати академічну заборгованість у порядку, передбаченому «Положенням про поточне та підсумкове оцінювання знань здобувачів НУ "Чернігівська політехніка"». Повторне складання заліку з метою підвищення позитивної оцінки не дозволяється. У випадку повторного складання заліку всі набрані протягом семестру бали анулюються, а повторний диференційований залік складається у вигляді тестування.

До загальної політики курсу відноситься дотримання принципів відвідування занять у відповідності до затвердженого розкладу, а також вільного відвідування лекційних занять для осіб, які отримали на це дозвіл відповідно до «Порядку надання дозволу на вільне відвідування занять здобувачам вищої освіти НУ «Чернігівська політехніка»». Запорукою успішного вивчення дисципліни є активність та залучення під час проведення лабораторних/практичних та лекційних занять – відповіді на запитання викладача (як один з елементів поточного контролю), задавання питань для уточнення незрозумілих моментів, вирішення практичних завдань. Консультації відбуваються в аудиторіях університету у відповідності до затвердженого розкладу або ж особистих чи групових консультацій (через вбудований форум) на сторінці курсу в системі дистанційного навчання НУ «Чернігівська політехніка».

Політика дедлайнів

Максимальна оцінка за невчасно здані роботи зменшується на зазначену кількість балів. Виключенням може бути наявність поважних причин несвоєчасної здачі зазначених

робіт (хвороба, участь в зазначений час в інших видах навчальної, наукової чи організаційної роботи, офіційна робота за фахом тощо).

Політика користування ноутбуками / смартфонами

Прохання до здобувачів тримати смартфони переведеними у беззвучний режим протягом лекційних та практичних занять, так як дзвінки, переписки та спілкування у соціальних мережах відволікають від проведення занять як викладача, так й інших здобувачів. Ноутбуки, планшети та смартфони не можуть використовуватися в аудиторіях під час занять та під час проведення підсумкового контролю (за виключенням проходження тестового контролю в системі Moodle).

Політика заохочень та стягнень

За результатами навчальної, наукової або організаційної діяльності здобувачів вищої освіти за курсом їм можуть нараховуватися додаткові бали – до 10 балів, у залежності від вагомості досягнень. Види позанавчальної діяльності, за якими здобувачі вищої освіти заохочуються додатковою кількістю балів: участь у міжнародних проектах, наукові дослідження, тези, участь у науково-практичних конференціях, винаходи, патенти, авторські свідоцтва за напрямами курсу.

Політика академічної доброчесності

Академічна доброчесність повинна бути забезпечена під час проходження даного курсу, зокрема при виконанні лабораторних, контрольних та розрахунково-графічних робіт (КР/КП) (принципи описані у Кодексі академічної доброчесності НУ «Чернігівська політехніка»). Списування під час проміжного та підсумкового контролів, виконання практичних завдань на замовлення, підказки вважаються проявами академічної недоброчесності. Від усіх слухачів курсу очікується дотримання академічної доброчесності у зазначених вище моментах. До здобувачів вищої освіти, у яких було виявлено порушення академічної доброчесності, застосовуються різноманітні дисциплінарні заходи (включаючи повторне проходження певних етапів).

Правила перезарахування кредитів

Кредити, отримані в інших закладах вищої освіти, а також результати навчання у неформальній та/або інформальній освіті, можуть бути перезараховані викладачем у відповідності до положення «Порядок визначення академічної різниці та перезарахування навчальних дисциплін у НУ «Чернігівська політехніка»». Визнання результатів навчання у неформальній освіті розповсюджується на окремі змістові модулі (теми) навчальної дисципліни.

11. Рекомендована література.

Базові підручники:

1. Злочини проти інформаційної безпеки держави: поняття, виявлення, досудове розслідування: монографія / І.В. Гора, В.А. Колесник, В.В. Малюк, В.О. Ходанович, А.М. Черняк, Л.І. Щербина. Київ: 7БЦ, 2023. 512 с.

2. Shao Y. Z. Guide to Security Assurance for Cloud Computing / Y. Z. Shao, H. Richard, T. Marcello., 2023. – (Springer). – (ISBN 3319259865).

3. Chris D. Practical Cloud Security: A Guide for Secure Design and Deployment / Dotson Chris., 2022. – 196 с. – (O'Reilly Media). – (ISBN-13: 978-1492037514).

4.Ivan R. Bulletproof SSL and TLS: The Complete Guide to Deploying Secure Servers and Web Applications / Ristic Ivan., 2023. – 425 с. – (Feisty Duck Ltd). – (ISBN 1907117040)..

5. Introduction to Forensic and Criminal Psychology. 7th Edition. Dennis Howitt Loughborough University. New York: Pearson Education Limited, 2022. 768 p.

Джерела:

1. ISO/IEC 27037 Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence. URL: https://www.amnafzar.net/files/1/ISO%2027000/ISO%20IEC%2027037-2012.pdf

2. https://www.coursera.org/learn/cloud-security-basics/
3. https://aws.amazon.com/security/
4. Образ віртуальної машини Kali Linux. URL: https://www.kali.org/get-kali/#kali-platforms
5. https://cloud.google.com/security
6. Autopsy – платформа цифрової криміналістики та графічний інтерфейс для The Sleuth Kit та інших інструментів цифрової криміналістики. URL: https://github.com/sleuthkit/autopsy
7. WireShark – найпопулярніший у світі аналізатор мережевих протоколів. URL: https://www.wireshark.org/
8. BelkaGPT — перший автономний AI-помічник для розслідувань DFIR. URL: https://belkasoft.com/belkagpt?utm_campaign=Police%201&utm_source=Media&utm_medium=Article&utm_term=eforensicsmag&utm_content=belkagpt