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

СИЛАБУС
Безпека в хмарних технологіях

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

«_26_» ___08_____ 2024 р.

Розробник (-и): Базилевич В.М., к.е.н., доцент,
Содиль М.О., викладач _____
(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_____2024р. №_7___

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

---

1. Загальна інформація про дисципліну.

Тип дисципліни	*Вибіркова*
Мова викладання	українська
Рік навчання та семестр	2024-2025 навчальний рік, 2 семестр, ОПП Кібербезпека за спеціальністю 125 Кібербезпека та захист інформації галузь знань 12 Інформаційні технології
Викладач (-і)	Базилевич В.М., к.е.н., доцент, Содиль М.О., викладач кафедри кібербезпеки та математичного моделювання.
Профайл викладача (-ів)	https://mmi.stu.cn.ua/personal-kafedry/
Контакти викладача	Т.м. +38(093) 791-03-73, E-mail: nick.sodyl@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:

Після завершення курсу студенти повинні:

- **Знати**:
  - Основні принципи безпеки хмарних технологій.
  - Типові загрози та вразливості хмар та сервісів.
  - Методи захисту даних, механізми аутентифікації та авторизації в хмарах.
  - Техніки шифрування та захисту конфіденційності даних.
  - Основи правових аспектів безпеки хмарних технологій, зокрема міжнародні стандарти та вимоги щодо захисту персональних даних.
- **Вміти**:

- створювати та підтримувати простий хмарний сервіс;
- вставновлювати ролі для послуги;
- оцінювати ризики, закладені у вразливих ситуаціях;
- застосовувати основні методи захисту хмарних сервісів.

КЗ 1. Здатність застосовувати знання у практичних ситуаціях.

КЗ 2. Здатність проводити дослідження на відповідному рівні.

КЗ 4. Здатність оцінювати та забезпечувати якість виконуваних робіт.

КФ 6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

КФ 9. Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому

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

ПРН 11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

5. Пререквізити. Передумови для вивчення дисципліни: для ефективного засвоєння матеріалів курсу «Управління мережевою безпекою», "Стандартизація, сертифікація засобів і комплексів захисту інформації".

6. Обсяг курсу:

Вид заняття	Загальна кількість годин денна/заочна
Лекції	16/6
Лабораторні заняття	16/6
Самостійна робота	58/108
Всього кредитів	4

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

7. Тематика курсу.

Змістовий модуль 1. Загальні поняття хмарних технологій

Тема 1. Вступ до хмарних технологій

Термінологія та історія хмарних технологій. Суть та характеристики хмарних технологій. Моделі хмарного розміщення та їх класифікація: PaaS, SaaS, DaaS, WaaS, CaaS, EaaS. Переваги та недоліки. Архітектура і пропозиції від провідних компаній надання хмарних послуг.

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

Тема 2. Сценарії використання хмарних технологій

Користувальницький сегмент. Освіта. Ігрові онлайн-сервіси. Персональна продуктивність. Бізнес-сегмент. Ритейл. Управління персоналом. Blockchain. Аналіз та огляд найбільших компаній які надають послуги хмарних технологій.

Змістовий модуль 2. Захист та загрози в хмарних середовищах

Тема 1. Загрози в хмарних середовищах

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

Тема 2. **Шифрування даних у хмарах**

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. Практичне використання SSL/TLS для захисту. 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. Створення аккаунта на AWS. Навчання по роботі з сервісами AWS, S3 Bucket, Основи EC2, Інстанси

Тема 3. Управління доступом та ідентифікація (IAM)

Основні компоненти IAM. Методи автентифікації. Управління доступом. Реалізація та інструменти IAM. Виклики та загрози в IAM. Кращі практики IAM. Налаштування механізмів аутентифікації та авторизації. Практичне налаштування аутентифікації. Налаштування складних паролів, двофакторної аутентифікації. Визначення та усунення потенційних вразливостей в механізмах авторизації.

8. Система оцінювання та вимоги

Загальна система оцінювання курсу	Оцінювання курсу базується на **накопичувальній системі** та включає: **поточний контроль** (оцінювання лабораторних занять) – 60 балів, **та підсумковий контроль** – 40 балів. Оцінювання кожного виду діяльності здійснюється окремо відповідно до **досягнення навчальних цілей**.
Вимоги до РГР, КР, КП тощо	**Критерії оцінювання:** 1) відповідність завдання вимогам курсу – **2 балів;** 2) обґрунтування вибору стандартів та методів захисту – **2 балів;** 3) якість аналізу ризиків та оцінка відповідності – **2 балів;** 4) оформлення роботи, відповідність методичним рекомендаціям – **2 балів;** 5) своєчасність здачі роботи – **2 бали.**
Практичні заняття	Оцінка кожного практичного заняття здійснюється за наступними критеріями: 1) виконання практичного завдання – **3 бали;** 2) аналіз отриманих результатів – **1 бал**; 3) належне оформлення звіту – **1 бал.**
Умови допуску до підсумкового контролю	1. Виконання та захист **не менше 50% практичних робіт** (щонайменше 4 із 8). 2. Проходження проміжного модульного контролю.

Розподіл балів, які отримують здобувачі вищої освіти

Модуль за тематичним планом дисципліни та форма контролю		**Кількість балів**
Змістовий модуль 1. **Загальні поняття хмарних технологій**		**24**
1	Тема 1. Вступ до хмарних технологій	**12**
2	Тема 2. Сценарії використання хмарних технологій	**12**
	Змістовий модуль 2. **Захист та загрози в хмарних середовищах**	**48**
1	Тема 1. Загрози в хмарних середовищах	**12**
2	Тема 2. Шифрування даних у хмарах	**12**
3	Тема 3. Управління доступом та ідентифікація (IAM)	**12**
Усього поточний і проміжний модульний контроль		**60**
Семестровий контроль (Диференційований залік)		**40**
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 (за необхідності).

При вивченні цього курсу для дистанційного навчання, тестування та обговорення питань курсу використовуються платформи *Moodle* та *Microsoft Teams*, для виконання лабораторних робіт застосовується комутаційне й серверне обладнання, а також ПК та програмне забезпечення навчальних аудиторій 105, 106, 110, 111 кафедри кібербезпеки та математичного моделювання.

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 (25), він не допускається до складання диференційованого заліку 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

Своєчасність здачі лабораторної роботи оцінюється в 0,5 балу за кожну лабораторну роботу. Своєчасність здачі РГР оцінюється в 1 бал. Відповідно, 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