МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Львівський національний університет імені Івана Франка
Факультет прикладної математики та інформатики
Кафедра кібербезпеки

Затверджено
На засіданні кафедри кібербезпеки
факультету прикладної математики та
інформатики
Львівського національного університету
імені Івана Франка
(Протокол №9/24 від 29 серпня 2024 р.)

Завідувач кафедри .

Петро ВЕНГЕРСЬКИЙ

Силабус з навчальної дисципліни
“Хмарна безпека та віртуалізація”,
що викладається в межах ОПП
Технології штучного інтелекту в кібербезпеці
другого (магістерського) рівня вищої освіти
для здобувачів з спеціальності
125 – Кібербезпека та захист інформації

Львів 2024 р.

Назва дисципліни	Хмарна безпека та віртуалізація
Адреса викладання дисципліни	Львівський національний університет імені Івана Франка, вул. Університетська 1, м. Львів, Україна, 79000
Факультет та кафедра, за якою закріплена дисципліна	Факультет прикладної математики та інформатики Кафедра кібербезпеки
Галузь знань, шифр та назва спеціальності	12 – інформаційні технології 125 – кібербезпека та захист інформації
Викладачі дисципліни	Брич Тарас Богданович, кандидат тех. наук доцент кафедри кібербезпеки (лекції та лабораторні заняття)
Контактна інформація викладачів	taras.brych@lnu.edu.ua https://ami.lnu.edu.ua/employee/brych-t-b
Консультації з питань навчання по дисципліні відбуваються	Консультації проводять раз на тиждень згідно з оприлюдненим розкладом консультацій викладача. Можливі онлайн консультації через Zoom чи Microsoft Teams. Для погодження часу онлайн консультацій слід писати на електронну пошту викладача.
Сторінка курсу	https://ami.lnu.edu.ua/admission/specializations
Інформація про дисципліну	Дисципліна “Хмарна безпека та віртуалізація” є вибірковою дисципліною зі спеціальності 125 – кібербезпека та захист інформації для освітньої програми Технології штучного інтелекту в кібербезпеці, яка викладається в 2-му семестрі другого (магістерського) рівня освіти в обсязі 3,5 кредитів (за Європейською Кредитно-Трансферною Системою ECTS).
Коротка анотація дисципліни	Курс спрямований на формування у студентів професійних компетентностей в області хмарних технологій, розвиток системи знань про безпеку хмарних сервісів, хмарних обчислень та безпеку інтернету речей, розуміння основних принципів розподілу відповідальності з постачальниками хмарних послуг.
Мета та цілі дисципліни	Метою курсу є формування у студентів знань про інформаційну безпеку при використанні хмар. Модель розподіленої відповідальності. Налаштування безпеки доступу до ресурсів хмари. Основи служб аутентифікації та керування доступом. Захист інфраструктури. Налаштування публічних та приватних підмереж та internet-протоколів. Групи безпеки, списки управління доступом в хмарі. Засоби ідентифікації та технології передачі даних в IoT. Топологія хмарних обчислень в IoT. Забезпечення кібербезпекбезпеки в IoT.
Література для вивчення дисципліни	1. https://docs.aws.amazon.com/ 2. https://aws.amazon.com/whitepapers/ 3. https://media.amazonwebservices.com/AWS_TCO_Web_Applications.pdf 4. https://aws.amazon.com/what-is-aws/ 5. https://docs.aws.amazon.com/pdfs/whitepapers/latest/overview-aws-cloud-adoption-framework/overview-aws-cloud-adoption-framework.pdf 6. https://docs.microsoft.com/ru-ru/azure/iot-accelerators/iot-accelerators-architecture-overview 7. https://www.datacenterknowledge.com/archives/2015/03/30/big-data-bubble-set-burst 8. https://intellect.ml/big-data-6821 9. http://www.mckinsey.com/insights/business_technology/big_data_the_next_frontier_for_innovation 10. http://www.ogcs.com.ua/index.php/articles/121-big-data-v-promyshlennosti-innovatsii-k-kotorym-pridetsya-privykat

Обсяг курсу	Загальний обсяг: 105 годин. Аудиторних занять: 32 год., з них 16 год. лекцій та 16 год. лабораторних робіт. Самостійної роботи: 73 год.
Очікувані результати навчання	У результаті вивчення навчальної дисципліни студент має набути таких компетентностей: **знати:** – моделі розподілення відповідальності при використанні Amazon Web Services; – методи шифрування даних у спокої та під час передачі; – як збирати дані про активність та події у мережі; – засоби ідентифікації та вимірювань (сенсори) в IoT; – технології передачі даних IoT; – топологія хмарних обчислень в IoT; – основи роботи Azure IoT, та індустріальний Інтернет речей; **вміти:** – керувати ідентифікацією та доступом в AWS; – володіти засобами забезпечення мережевого доступу до ресурсів AWS; – розподілити трафік за допомогою балансувальників навантаження; – визначати які AWS-сервіси можна використовувати для моніторингу; – визначати, які AWS-сервіси можна використовувати для реагування на інциденти; – забезпечити кібербезпеку IoT
Ключові слова	Віртуалізація, хмарні послуги, інтернет речей.
Формат курсу	очний Проведення лекцій, лабораторних робіт і консультацій.
Теми	Теми подані у Схемі курсу нижче
Підсумковий контроль, форма	залік у кінці семестру
Пререквізити	Для вивчення курсу студенти потребують базові знання з дисциплін "Основи кібербезпеки", "Безпека комп'ютерних мереж", "Менеджмент інформаційної безпеки".
Навчальні методи та техніки, які будуть використовуватися під час викладання курсу	Презентації, лекції Модульний контроль Лабораторні роботи
Необхідне обладнання	Комп’ютери, комп’ютерні системи та мережі. Віртуальні машини. Інтернет ресурси.

Критерії оцінювання (окремо для кожного виду навчальної діяльності)

Оцінювання проводиться за 100-бальною шкалою. Бали нараховуються за наступним співвідношенням:

• лабораторні роботи: 40% семестрової оцінки;
• самостійна робота: 10% семестрової оцінки;
• модульний контроль: 50% семестрової оцінки

Підсумкова максимальна кількість балів 100.

Академічна доброчесність: Очікується, що роботи студентів будуть їх оригінальними дослідженнями чи міркуваннями. Відсутність посилань на використані джерела, фабрикування джерел, списування, втручання в роботу інших студентів становлять, але не обмежують, приклади можливої академічної недоброчесності. Виявлення ознак академічної недоброчесності в письмовій роботі студента є підставою для її незарахуванння викладачем, незалежно від масштабів плагіату чи обману.

Відвідання занять є важливою складовою навчання. Очікується, що всі студенти відвідають усі лекції та лабораторні заняття курсу. Студенти повинні інформувати викладача про неможливість відвідати заняття. У будь-якому випадку студенти зобов'язані дотримуватися термінів визначених для виконання всіх видів письмових робіт та індивідуальних завдань, передбачених курсом.

Література. Уся література, яку студенти не зможуть знайти самостійно, буде надана викладачем виключно в освітніх цілях без права її передачі третім особам. Студенти заохочуються до використання також й іншої літератури та джерел, яких немає серед рекомендованих.

П**олітика виставлення балів.** Враховуються бали набрані при виконанні індивідуальних завдань, самостійній роботі та бали підсумкового модульного контролю. При цьому обов'язково враховуються присутність на заняттях та активність студента під час лабораторного заняття; недопустимість пропусків та запізнень на заняття; користування мобільним телефоном, планшетом чи іншими мобільними пристроями під час заняття в цілях не пов'язаних з навчанням; списування та плагіат; несвоєчасне виконання поставленого завдання і т. ін.

Жодні форми порушення академічної доброчесності не толеруються.

Критерії оцінювання знань студентів	**Бали рейтингу**	**Макс. к-сть балів**
1. Бали поточної успішності за виконання 5-ти індивідуальних завдань		
Критерії оцінювання (5*8 бали)	**40 балів**	
Студент в повному обсязі володіє навчальним матеріалом, вільно самостійно та аргументовано його викладає під час захисту індивідуальних завдань, глибоко та всебічно розкриває зміст теоретичних питань. Реалізоване програмне забезпечення пройшло перевірку на плагіат та повністю виконує умову завдання.	**8**	
Студент достатньо повно володіє навчальним матеріалом, обґрунтовано його викладає під час захисту індивідуальних завдань, в основному розкриває зміст теоретичних питань. Але при викладанні деяких питань не вистачає достатньої глибини та аргументації. Реалізоване програмне забезпечення містить окремі несуттєві неточності та незначні помилки.	**7-5**	
Студент не в повному обсязі володіє навчальним матеріалом. Фрагментарно, поверхнево (без аргументації та обґрунтування) викладає його під час захисту індивідуального завдання, недостатньо розкриває зміст теоретичних питань, допускаючи при цьому суттєві неточності, програмна реалізація завдання частково виконана.	**4-1**	

	Студент не виконав лабораторне завдання та не володіє матеріалом.	**0**
	2. Самостійна робота студентів (СРС)	
	Критерії оцінювання (5*2 балів)	**10 балів**
	Самостійна робота (додаткове опрацювання матеріалу за темами дисципліни поза межами наданого лектором, з додаткових джерел) Самостійна робота студентів, оцінюється під час захисту відповідних лабораторних робіт. Студент додатково опрацював матеріал, підготував доповідь та аргументовано його викладає.	**2**
	Студент не опрацював самостійно додаткових джерел і не володіє матеріалом	**0**
	3. Модульний контроль	**50**
	Підсумкова контрольна робота містить **5 теоретичних питань по 10 балів**	
	Критерії оцінювання відповіді на теоретичні питання (5*10 балів):	***50***
	Відповідь написано в повному обсязі, аргументовано, глибоко та всебічно розкрито зміст теоретичного питання.	**10**
	Відповідь в основному розкриває зміст теоретичного питання, не вистачає достатньої глибини та аргументації, допущено окремі несуттєві неточності та незначні помилки.	**8-9**
	Відповідь в цілому розкриває основний зміст питання але без глибокого всебічного аналізу, обґрунтування та аргументації, допущено окремі суттєві неточності та помилки.	**5-7**
	Відповідь не повна, фрагментарна без аргументації та обґрунтування.	**2-4**
	Відповідь не надана	**0**
	Загальна кількість балів по завершенні вивчення дисципліни	**100**
Опитування	Анкету-оцінку з метою оцінювання якості курсу буде надано по завершенню курсу.	

Схема курсу

Тиж.	Тема, план, короткі тези	Форма діяльності (заняття)	Література	Завдання, год.	Термін виконання
1-2	**Тема 1. Хмарні технології, економіка, огляд концепцій.** (Поняття послуг, конфігурації, ціноутворення у хмарних ресурсах на прикладі AWS – концепції хмарних рішень. Моделі розгортання хмарних обчислень. Категорії веб-сервісів послуги хмарних провайдерів. Служби AWS та огляд категорій послуг. Основні послуги, які надаються AWS)	лекція, самостійна робота	[1-5]	2 8	2 тижні
		лаб.	[1-5]	4	
3-4	**Тема 2. Хмарна архітектура, глобальна інфраструктура**. (Компоненти глобальної інфраструктури AWS. Архітектурні принципи AWS Cloud. Зони доступності. Центри обробки даних AWS. Точки присутності. Функції інфраструктури AWS.)	лекція, самостійна робота		2 8	2 тижні
		лаб.	[1-5]	4	

5-6	**Тема 3. Безпека хмарних послуг – основні концепції. Модель розподіленої відповідальності.** (Модель спільної відповідальності AWS. AWS Identity and Access Management (IAM). Основні компоненти. IAM MFA. AWS CLI. AWS Management Console. Захист облікових записів.)	лекція, самостійна робота	[1-5]	2 8	2 тижні
		лаб.	[1-5]	4	
7-8	**Тема 4. Безпека доступу та хмарні ресурси. Налаштування безпеки доступу до ресурсів хмари. Автентифікація та авторизація.** (Безпека доступу до хмарних ресурсів. Захист інфраструктури та даних користувача. Журналювання та моніторинг у хмарі. Реагування на інцидент та управління ним. Служби AWS, які можна використовувати для моніторингу та реагування на інциденти.)	лекція, самостійна робота	[1-5]	2 8	2 тижні
		лаб.	[1-5]	2	
9-10	**Тема 5. Логування та моніторинг. Реагування на інциденти.** (Використання VPC. Налаштування публічних та приватних підмереж та інтернет-протоколів. елементи безпеки vpc – Security groups, Network ACLs, Subnets, Route tables. Використання балансувальників навантаження AWS. Amazon Inspector та AWS Systems Manager.)	лекція, самостійна робота	[1-5]	2 8	2 тижні
		лаб.	[1-5]	2	
11	**Тема 6. Хмарні технології та IoT. Засоби ідентифікації та вимірювань (датчики) в IoT.** (Загальні принцип побудови та архітектура IoT. Класифікація систем IoT. Класифікація засобів автоматичної ідентифікації. Класифікація датчиків. Технологія Micro-Electro-Mechanical Systems.)	лекція, самостійна робота	[6-10]	1 8	1 тиждень
12-13	**Тема 7. Інтелектуальні кінцеві точки та живлення в IoT. Технології передачі даних IoT** (Інтелектуальні кінцеві точки IoT. Відеосистема. Виконавчі пристрої. Джерела енергії та управління живленням. Стандарт IEEE 802.15.4, Bluetooth (IEEE 802.15.1), ZigBee і IEEE 802.15.4, Wi-Fi та IEEE 802.11. Технології LPWAN. Технологія PLC.)	лекція, самостійна робота	[6-10]	2 8	2 тижні
14	**Тема 8. Топологія хмарних обчислень в IoT. Основи роботи Azure IoT.** (Модель хмарних сервісів. Види хмар та хмарна архітектура. Хмарна архітектура OpenStack. Обмеження хмарних архітектур для IoT. Туманні обчислення. Архітектура OpenFog RA. Amazon Greengrass і лямбда-функції. Туманні топології.)	лекція, самостійна робота	[6-10]	1 8	1 тиждень

15-16	**Тема 9. Індустріальний Інтернет речей Azure. Питання забезпечення Кібербезпеки в IoT** (Принципи роботи Azure IoT. Підключення пристроїв до Azure: Центр IoT та Центри подій. Індустріальний IoT Azure. Управління пристроями Azure IoT Open Platform Communications (OPC). Управління сертифікатами UA Azure IoT Open Platform Communications (OPC). Акселератор рішень IoT.)	лекція, самостійна робота	[6-10]	2 9	2 тижні