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 № 15/23 від 29 серпня 2023 р.)

Завідувач кафедри .

Венгерський П.С.

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

Львів 2023 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
Викладачі дисципліни	Брич Тарас Богданович, доцент кафедри кібербезпеки
Контактна інформація викладачів	taras.brych@lnu.edu.ua
Консультації з питань навчання по дисципліні відбуваються	Консультації в день проведення лекцій/практичних занять (за попередньоюдомовленістю).
Сторінка курсу	https://ami.lnu.edu.ua/admission/specializations
Інформація про дисципліну	Дисципліна “Хмарна безпека та віртуалізація” є дисципліною за вибором зі спеціальності 125 – кібербезпека для освітньої програми Кібербезпека, яка викладається в 10-му семестрі в обсязі 4-х кредитів (за Європейською Кредитно-Трансферною Системою ECTS).
Коротка анотація дисципліни	Курс спрямований на формування у студентів професійних компетентностей, розвиток системи знань про безпеку хмарних сервісів, хмарних обчислень та безпеку інтернету речей, розуміння основних принципів розподілуя 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://d0.awsstatic.com/whitepapers/aws-overview.pdf 4. https://d1.awsstatic.com/whitepapers/AWS_Cloud_Best_Practices.pdf 5. https://d0.awsstatic.com/whitepapers/aws_pricing_overview.pdf 6. https://media.amazonwebservices.com/AWS_TCO_Web_Applications.pdf 7. https://aws.amazon.com/what-is-aws/ 8. https://d1.awsstatic.com/whitepapers/aws-overview.pdf https://docs.aws.amazon.com/pdfs/whitepapers/latest/overview-aws-cloud-adoption-framework/overview-aws-cloud-adoption-framework.pdf
Обсяг курсу	Загальний обсяг: 120 годин. Аудиторних занять: 64 год., з них 32 год. лекцій та 32 год. лабораторних робіт. Самостійної роботи: 56 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 (датчики) 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 Курс забезпечує набуття таких компетентностей: КЗ 2, КЗ 3, КЗ 4, КФ 2; та програмних результатів навчання: ПРН 3, ПРН 4, ПРН 5, ПРН 8, ПРН 10, ПРН 13, ПРН 15, ПРН 18, ПРН 20, ПРН 25, ПРН 27, ПРН 30, ПРН 34, ПРН 36, ПРН 39, ПРН 43, ПРН 45, ПРН 48, ПРН 52, ПРН 54.
Ключові слова	Віртуалізація, хмарні послуги, інтернет речей.
Формат курсу	змішаний Проведення лекцій, лабораторних робіт і консультацій.
Теми	Тема 1. Хмарні технології, економіка, огляд концепцій. Тема 2. Хмарна архітектура, глобальна інфраструктура. Тема 3. Безпека хмарних послуг – основні концепції. Модель розподіленої відповідальності Тема 4. Безпека доступу та хмарні ресурси. Налаштування безпеки доступу до ресурсів хмари. Автентифікація та авторизація. Тема 5. Логування та моніторинг. Реагування на інциденти. Тема 6. Хмарні технології та IoT. Засоби ідентифікації та вимірювань (датчики) в IoT Тема 7. Інтелектуальні кінцеві точки та живлення в IoT. Технології передачі даних IoT Тема 8. Топологія хмарних обчислень в IoT. Основи роботи Azure IoT Тема 9. Індустріальний Інтернет речей Azure. Питання забезпечення Кібербезпекбезпеки в IoT
Підсумковий контроль, форма	залік у кінці семестру

Навчальні методи та техніки, які будуть використовуватися під час викладання курсу	Презентації, лекції. Модульний контроль
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 занаступним співвідношенням: • тестування, усне опитування: 50% семестровоїоцінки; максимальна кількість балів 50 • залік 50% семестрової оцінки; максимальна кількість балів 50 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 недобро- чесності в письмовій роботі студента є підставою для її незарахуваннння викладачем, незалежно від масштабів плагіату чи обману. **Відвідання занять** є важливою складовою навчання. Очікується, що всі студенти відвідають усі лекції та практичні зайняття курсу. Студенти повинні інформувати викладача про неможливість відвідати заняття. У будь-якому випадку студенти зобов'язані дотримуватися термінів виз- начених 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 поточному тестуванні, самостійній роботі та бали підсумкового тестування. При цьому обов'язково враховуються присутність на заняттях та активність студента під час практичного заняття; недопустимість пропусків та запізнень на заняття; користування мобільним телефоном, планшетом чи іншими мо- більними 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.
Питання до заліку.	Залік – за результатами поточного контролю протягом семестру і усне опитування. Питання відповідають темам курсу.
Опитування	Анкету-оцінку з метою оцінювання якості курсу буде надано по завершенню курсу.