

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
“Технологія Blockchain для кібербезпеки”,
що викладається в межах ОПШ
Технології штучного інтелекту в кібербезпеці
другого (магістерського) рівня вищої освіти
для здобувачів з спеціальності
125 – Кібербезпека та захист інформації

Назва дисципліни	Технологія Blockchain для кібербезпеки
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	Пелешко Дмитро Дмитрович, професор кафедри кібербезпеки Ребець Андрій Ігорович, асистент
Контактна інформація викладачів	Dmytro.peleshko@lnu.edu.ua https://ami.lnu.edu.ua/employee/peleshko-d-d andrii.rebets@lnu.edu.ua https://ami.lnu.edu.ua/employee/rebets-a
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 “Технологія Blockchain для кібербезпеки” 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, теоретичних засад та практичних навиків застосування технології Blockchain для кібербезпеки.
Мета та цілі дисципліни	Метою курсу є формування у студентів знань про технологію Blockchain в задачах кібербезпеки. Принципи функціонування блокчейну. Основні принципи транзакцій у блокчейні. Забезпечення безпеки технології блокчейн. Використання криптографії в блокчейні. Проблема масштабування в технології Blockchain. Архітектура приватних блокчейнів. Архітектура публічних блокчейнів. Можливості використання технології Blockchain для кібербезпеки. Використання блокчейну для цифрової ідентифікації.
Література для вивчення дисципліни	<ol style="list-style-type: none"> 1. Поліщук В. Г. Блокчейн як засіб забезпечення безпеки в цифровому світі / В. Г. Поліщук // Харків, ХНУРЕ, Матеріали 27-го Міжнародного молодіжного форуму «Радіоелектроніка і молодь у XXI столітті». Том 4. – 2023. – С. 54-55 2. Namane S., Ben Dhaou I. Blockchain-Based Access Control Techniques for IoT Applications // Security and Privacy in Blockchain/IoT. 15 June 2022 [Електронний ресурс]. URL: https://doi.org/10.3390/electronics11142225 3. A Blockchain-Inspired Attribute-Based Zero-Trust Access Control Model for IoT / S. M. Awan, M. A. Azad, J. Arshad [et al.] // Pervasive Computing in IoT. 16 February 2023 [Електронний ресурс]. URL: https://doi.org/10.3390/info14020129 4. Ensuring Information Security of Web Resources Based on Blockchain Technologies / A. Barakova; O. Ussatova, Y. Begimbayeva, I. Sogukpinar // International Journal of Advanced Computer Science and Applications

	<p>(IJACSA). 2023 [Електронний ресурс]. URL: https://doi.org/10.14569/IJACSA.2023.0140689</p> <p>5. Mahmood Samreen, Chadhar Mehmood, Firmin Selena. Cybersecurity Challenges in Blockchain Technology: A Scoping Review // School of Engineering, Information Technology and Physical Sciences. 05 Apr 2022 [Електронний ресурс]. URL: https://doi.org/10.1155/2022/7384000</p>
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	<p>У результаті вивчення навчальної дисципліни студент має набути таких компетентностей:</p> <p>знати:</p> <ul style="list-style-type: none"> – основні поняття та принципи технології Blockchain; – властивості транзакцій та смарт-контрактів блокчейну; – поняття і властивості консенсусу в блокчейні; – принципи забезпечення безпеки блокчейну; – застосування криптографії в блокчейні; – сфери застосування блокчейну; – варіанти використання властивостей блокчейну для вирішення задач кібербезпеки. <p>вміти:</p> <ul style="list-style-type: none"> – застосовувати принципи та властивості блокчейну; – розробляти та модифікувати ланки ланцюгів блокчейну; – розробляти прості алгоритми і смарт-контракти технології Blockchain; – використовувати криптографічні перетворення під час побудови мережі Blockchain; – застосовувати блокчейн вирішення для задач кібербезпеки.
Ключові слова	Blockchain, децентралізація, криптографія, приватність.
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 незарахування 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.

Політика 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 запізнь 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 балів)	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. Принципи функціонування блокчейну. (Структура блокчейну. Поняття і технології консенсусу. Proof of Work (PoW). Proof of Stake (PoS). Proof of Stake. Властивості блокчейну.	лекція, самостійна робота	[1-5]	2 9	2 тижні
		лаб.	[1-5]	2	
3	Тема 2. Основні принципи транзакцій у блокчейні. (Види і особливості транзакцій блокчейну. Схема транзакцій блокчейну. Поняття безпеки транзакцій.	лекція, самостійна робота		1 5	1 тиждень
		лаб.	[1-5]	1	

4-5	Тема 3. Забезпечення безпеки технології блокчейн. (Концепції консенсусу та незмінності в технології Blockchain. Принципи перевірки цілісності блоків блокчейну. Застосування криптології в блокчейні.)	лекція, самостійна робота	[1-5]	2 8	2 тижні
		лаб.	[1-5]	2	
6-7	Тема 4. Можливості використання технології блокчейн. (Сфери застосування технології Blockchain. Аналіз властивостей блокчейну в контексті його практичного застосування. Обмеження технології Blockchain.)	лекція, самостійна робота	[1-5]	2 8	2 тижні
		лаб.	[1-5]	2	
8	Тема 5. Проблема масштабування в технології блокчейн. (Вплив криптографічних перетворень блокчейну на масштабованість мережі. Вплив децентралізації блокчейну на масштабованість мережі.)	лекція, самостійна робота	[1-5]	1 5	1 тиждень
		лаб.	[1-5]	1	
9-10	Тема 6. Архітектура приватних блокчейнів. (Поняття і концепція приватного блокчейну. Властивості і переваги приватних блокчейнів. Недоліки приватних блокчейнів. Забезпечення цілісності даних і безпеки приватного блокчейну.)	лекція, самостійна робота	[1-5]	2 9	2 тижні
		лаб.	[1-5]	2	
11-12	Тема 7. Архітектура публічних блокчейнів. (Поняття і концепція публічного блокчейну. Властивості і переваги публічних блокчейнів. Недоліки публічних блокчейнів. Забезпечення цілісності даних і безпеки публічного блокчейну.)	лекція, самостійна робота	[1-5]	2 9	2 тижні
		лаб.	[1-5]	2	
13-14	Тема 8. Застосування технології Blockchain у кібербезпеці. (Унікальні властивості технології блокчейн для кібербезпеки. Порівняння підходів до вирішення задач кібербезпеки. Переваги і недоліки блокчейну з позиції прикладних задач кібербезпеки. Приклади застосування технології Blockchain для кібербезпеки)	лекція, самостійна робота	[1-5]	2 10	2 тижні
		лаб.	[1-5]	2	

15-16	Тема 9. Цифрова ідентифікація з використанням технології Blockchain. (Постановка проблеми збереження і обробки персональних даних. Переваги технології Blockchain для вирішення задачі цифрової ідентифікації. Архітектура система цифрової ідентифікації з використанням технології блокчейн. Приклад практичної реалізації системи цифрової ідентифікації з використанням технології блокчейн.)	лекція, самостійна робота	[1-5]	2 10	2 тижні
		лаб.	[1-5]	2	