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 № 16/23 від 7 вересня 2023р.)

Завідувач кафедри П.С.Венгерський

Силабус з навчальної дисципліни
“ Застосування криптології у віртуальній економіці”,
що викладається в межах ОПП Інформатика
першого (бакалаврського) рівня вищої освіти для здобувачів з спеціальності 122 – Комп’ютерні науки

Львів-2023

Назва дисципліни	Застосування криптології у віртуальній економіці
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 122 – Комп'ютерні науки
Викладачі дисципліни	Пелешко Дмитро Дмитрович, Професор кафедри кібербезпеки
Контактна інформація викладачів	Dmytro.peleshko@lnu.edu.ua Головний корпус ЛНУ ім. І. Франка, каб. 380. м. Львів, вул. Університетська, 1
Консультації зпитань 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/course/zastosuvannia-kryptolohii-u-virtualniy-ekonomitsi-kn-dvvs
Інформація про дисципліну	Дисципліна "Застосування криптології у віртуальній економіці" є вибірковою дисципліною з спеціальності 122 – Комп'ютерні науки для освітньої програми Інформатика, яка викладається у 8-му семестрі в обсязі 4-х кредитів (за Європейською Кредитно-Трансферною Системою ECTS).
Коротка анотація дисципліни	Дисципліна "Застосування криптології у віртуальній економіці" охоплює вивчення основних принципів та методів криптографії, її застосування в віртуальній економіці та розглядає проблеми безпеки, пов'язані з її використанням. Серед основних завдань дисципліни - ознайомлення з різними типами криптографічних алгоритмів, дослідження методів шифрування даних, що використовуються в віртуальній економіці, аналіз переваг та недоліків використання криптографії в економіці та суспільстві загалом, вивчення інструментів криптографії, які використовуються в біткоїні та інших криптовалютах, а також розуміння впливу використання криптографії на розвиток віртуальної економіки та її інфраструктури.
Мета та цілі дисципліни	Метою дисципліни "Застосування криптології у віртуальній економіці" є надання студентам знань та навичок у сфері захисту інформації та криптографії в контексті віртуальної економіки. Студенти повинні навчитись використовувати криптографічні

	методи для захисту електронної комунікації, збереження конфіденційності даних, підтвердження автентичності та забезпечення цілісності транзакцій. Крім того, студентам будуть надані знання про розробку та застосування криптовалют та інших криптованих активів у віртуальній економіці. Навчальний курс допоможе студентам зрозуміти принципи та практичні аспекти криптографії та захистуінформації, що є важливими для розвитку віртуальної економіки та забезпечення її стабільності та безпеки.
Література для вивчення дисципліни	**Основна** 1. Євсеєв С.П., Мілов О.В., Остапов С.Е. Северінов О.В. Кібербезпека: основи кодування та криптографії: навч. Посібник. – Харків: ХПІ, 2023. – 658 с. 2. Козіна Г. Л. Криптографія від історії до сучасних стандартів: навч. посібник. – Запоріжжя : НУ «Зап. пол.», 2020. – 192 с 3. Стасюк М. Елементи математичних основ криптографії : навчальний посібник – Львів : ЛДУ БЖД, 2021. – 216 с. 4. Щур Н.О., Покотило О.А. Основи криптології: навч. посібник. – Житомир: Державний університет «Житомирська політехніка», 2021. – 120с. 5. Dan Boneh, Victor Shoup. A Graduate Course in Applied Cryptography, 2020. – 943 p. 6. David Wong. Real-World Cryptography, Version 12, 2021 – 369 p **Допоміжна** 7. Інформаційні технології; Методи захисту; Цифрові підписи з доповненням / А. Анісімов (пер.і наук.-техн.ред.). - Офіц. вид. - К. : Держспоживстандарт України, 2006. - (Національний стандарт України). 8. Основи захисту інформації : навч. посібн. / О. А. Смірнов, Л. Г. Віхрова,С. І. Осадчий та ін. – Кіровоград, 2010. – 322 с. 9. Основи інформаційної безпеки / С. В. Кавун, О. А. Смірнов, В. Ф. Столбов – Кіровоград : Вид. КНТУ, 2012. – 414 с. 10. Вербіцький О.В. Вступ до криптології. Львів, 1998 – 247с. 11. Захарченко М.В., Йона Л.Г., Щербина Ю.В., Онацький О.В. Розвинення криптології та її місце у сучасному суспільстві, Одеса, 2003. – 80 с. 12. Корченко О. Г. Прикладна криптологія: системи шифрування: підручник / О. Г. Корченко, В. П. Сіденко, Ю. О. Дрейс. – К. : ДУТ, 2014. – 448 с. 13. Остапов С. Е., Валь Л.О. Основи криптографії: Навчальний посібник. – Чернивці: Книги – XXI, 2008. – 188 с. 14. Фільштінський В. А.,Бережний А. В. – Суми: Сумський державний університет, 2011. – 138 с. 15. Douglas R. Stinson. Introduction to modern cryptography. Second Edition. 2015. – 576 p. 16. Douglas R. Stinson, Maura B. Paterson. Cryptography. Theory and Practice. Fourth Edition, 2019. – 580 p.

	17. Bruce Schneier. Applied cryptography, second edition, protocols, algorithms, and source code in C, 2015. – 792 p. 18. Gilbert Baumslag, Benjamin Fine, Martin Kreuzer, Gerhard Rosenberger. A Course in Mathematical Cryptography, 2015. – 376 p. 19. Alko R. Meijer. Algebra for Cryptologists, 2016. – 301 p. 20. Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman. An Introduction to Mathematical Cryptography, 2014. – 538 p. 21. Nigel P. Smart. Cryptography Made Simple, 2016. – 481 p. 22. Christof Paar · Jan Pelzl. Understanding Cryptography. A Textbook for Students and Practitioners, 2010. – 372 p. 23. Richard Crandall, Carl Pomerance. Prime Numbers. A Computational Perspektive. Second Editson. Springer, 2005. 24. Ю.В. Капітонова, С.Л. Кривий, О.А. Летичевський, М.К. Печурін. Основи дискретної математики. К.: Наукова думка, 2002. **Інформаційні ресурси в Інтернет** Міжнародна асоціація криптології (IACR): https://www.iacr.org/ Інтернаціональна організація з кібербезпеки (ICSPA): https://www.icspa.org/ Міжнародний стандартизаційний орган з кібербезпеки (ISO/IEC JTC1SC27): https://www.iso.org/committee/45306/x/catalogue/ Європейський офіс з інтелектуальної власності (EUIPO): https://euipo.europa.eu/ohimportal/uk/home
Обсяг курсу	Загальний обсяг: 120 годин. Аудиторних занять: 56 год., з них 28 год. лекцій та 28 год. лабораторних робіт. Самостійної роботи: 64 год. К-ть кредитів: 4
Очікувані результати навчання	Завданнями вивчення дисципліни "Застосування криптології у віртуальній економіці" є: - розуміння основних принципів криптографії та її застосування віртуальній економіці; - ознайомлення з типами криптографічних алгоритмів та їхньою роботою; - дослідження методів шифрування даних, що використовуються у віртуальній економіці; - вивчення інструментів криптографії, які використовуються в біткоїні та інших криптовалютах; - аналіз переваг та недоліків використання криптографії в економіці та суспільстві загалом; - вивчення проблем безпеки, пов'язаних з використанням криптографії, таметодів їх уникнення; - розуміння впливу використання криптографії на розвиток віртуальної економіки та її інфраструктури; - ознайомлення з перспективами застосування криптографії у віртуальній економіці та її майбутніми тенденціями; - вивчення принципів та методів криптографії, які використовуються в блокчейні та децентралізованих системах; - розуміння ризиків та викликів, пов'язаних з використанням

	криптографії віртуальної економіки, та розроблення методів їх зменшення.
Ключові слова	Криптологія, криптографія, шифрування даних, захист інформації, безпека, криптовалюти.
Формат курсу	Очний.
Теми	Теми подані у схемі курсу нижче
Підсумковий контроль, форма	Залік у кінці 8 семестру Підсумковий контроль складається з результатів усіх модульних контролів, що передбачені за весь термін викладання дисципліни.
Навчальні методи та техніки, які будуть використовуватися під час викладання курсу	Реалізація компетентностного підходу передбачає широке використання в навчальному процесі здобувачів вищої освіти традиційних освітніх технологій в поєднанні з активними та інтерактивними формами проведеннязанять. Питома вага занять, що проводяться в інтерактивних формах, складає не менше 50% аудиторних занять. В рамках вивчення даної дисципліни використовуються: - мультимедійні освітні технології: інтерактивні лекції (презентації) з використанням програми MS Power Point в поєднанні з анімацією і звуковим супроводом; перегляд відеороликів за окремими пунктами тем занять, використання електронних посібників; - діалогові технології: організація групових дискусій, використання «мозкового штурму», техніки «touchstone»; - використання інформаційних технологій: використання спеціалізованих пакетів для розрахунку, проектування і дослідження систем управління та мережі Інтернет. Лекції проводяться з використанням технічних засобів навчання і супроводжуються демонстрацією презентацій за допомогою відеопроектора. Також проводиться дискусійне обговорення проблемних питань. Лабораторні заняття проводяться в аудиторіях, що мають комп'ютерну техніку та необхідне методичне забезпечення. У разі виникнення необхідності забезпечення навчального процесу у дистанційному режимі супровід та контроль знань реалізовується за допомогою хмарних сервісів або додатків он-лайн конференцій. Онлайн лекції, консультації та усні відповіді на питання проводяться за допомогою Microsoft Teams або Zoom, поточне та підсумкове тестування – Online Test Pad.
Необхідне обладнання	Комп'ютери, комп'ютерні системи та мережі. Інтернет ресурси.
Політика та процедура академічної поведінки та етики	Курс передбачає самостійне виконання здобувачами навчальних завдань, завдань поточного та підсумкового контролю результатів навчання. Виконання роботи замість інших здобувачів, а також намагання здати чужу роботу є порушенням академічної доброчесності.

	Обов'язковим є посилання на джерела інформації у разі використання ідей, розробок, тверджень, відомостей; надання достовірної інформації про результати власної навчальної (наукової, творчої) діяльності, використані методики досліджень і джерела інформації. **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 практичні зайняття 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 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 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 (окремо для кожного виду навчальної діяльності)	Студенти виконують 10 лабораторних робіт по 2 год. – 8 балів і 2 роботи по 4 год. – 10 балів. Оцінка за лабораторну роботу (у % від кількості балів, виділених на завдання із заокругленням до цілого числа): - 0% – завдання не виконано; - 40% – завдання виконано частково, висновки не аргументовані і не конкретні, звіт підготовлено недбало; - 60% – завдання виконано повністю, висновки містять окремі недоліки, судження студента не достатньо аргументовані, звіт підготовлено з незначним відхиленням від вимог; - 80% – завдання виконано повністю і вчасно, проте містить окремі несуттєві недоліки не системного характеру; - 100% – завдання виконано правильно, вчасно і без зауважень

Питання для самоперевірки	1.Що таке криптографія та які є її основні принципи? 2.У чому полягає забезпечення конфіденційності, цілісності, доступності, інформаційних ресурсів? 3.Дайте визначення поняттям: криптологія, криптографія та криптоаналіз. 4.Що таке криптографічний алгоритм та шифр? 5.Що таке криптографічний ключ? 6.Розкрийте поняття зашифрування та дешифрування даних. 7.Опишіть алгоритм шифрування Цезаря. 8.До якого виду шифрів заміни (підстановки) відносять шифр Цезаря? 9.Опишіть алгоритм шифру частоколу. 10.Опишіть алгоритм шифру Плейфера. 11.Опишіть алгоритм шифрування криптосистемою Хілла. 12.Що являє собою ключ в криптосистемі Хілла? 13.Що є ключем у шифрі Віженера? 14.Опишіть алгоритм шифрування Віженера. 15.У чому суть методу частотного криптоаналізу? 16.Відмінність між шифрами моноалфавітної та поліалфавітної підстановки (заміни). 17.Дайте визначення відкритого та закритого тексту. 18.Назвіть складові криптографічної системи. 19. Симетричні та асиметричні криптографіцні системи. 20.У чому полягає криптостійкість криптографічної системи? 21.Що таке атака на криптографічну систему? 22.Коротка класифікація шифрів. 23.Що таке індекс збігу? 24.Які інструменти криптографії використовуються в біткоїні та інших криптовалютах? 25.Які переваги та недоліки використання криптографії в економіці та суспільстві загалом? 26.Які проблеми безпеки пов'язані з використанням криптографії та як їх можна уникнути? 27.Як використання криптографії впливає на розвиток віртуальної економіки та її інфраструктури? 28.Які є перспективи застосування криптографії у віртуальній економіці та її майбутніх тенденціях?
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	Тема 1. Основи криптографії: історія та розвиток.	лекція, самостійна	[1-5]	2 5	1 тиждень

		робота			
	Тема 1. Основи криптографії: історія та розвиток.	лаб	[1-5]	2	
2	Тема 2. Модулярні обчислення.	лекція, самостійна робота	[1,2,4,5]	2 5	1 тиждень
	Тема 2. Модулярні обчислення	лаб.	[1,2,4,5]	2	
3	Тема 3 Елементи теорії чисел. Алгоритм Евкліда. Теорема Ейлера. Теореми Ферма. Обчислення у скінченних полях	лекція, самостійна робота	[1,2,4,5]	2 5	1 тиждень
	Тема 3 Елементи теорії чисел. Алгоритм Евкліда. Теорема Ейлера. Теореми Ферма. Обчислення у скінченних полях	лаб	[1,2,4,5]	2	
4	Тема 4. Поняття та принципи шифрування, симетричне та асиметричне шифрування.	лекція, самостійна робота	[5-6]	2 6	1 тиждень
	Тема 4. Поняття та принципи шифрування, симетричне та асиметричне шифрування.	лаб.	[5-6]	2	
5	Тема 5 Геш-функції.	лекція, самостійна робота	[5-6]	2 5	1 тиждень
	Тема 5 Геш-функції.	лаб.	[5-6]	2	
6	Тема 6. Електронний цифровий підпис: поняття, принципи та види підписів, застосування у віртуальній економіці, алгоритми та протоколи підписування.	лекція, самостійна робота	[5-6]	2 5	1 тиждень
	Тема 6. Електронний цифровий підпис: поняття, принципи та види підписів, застосування у віртуальній економіці, алгоритми та протоколи підписування.	лаб.	[5-6]	2	
7	Тема7.Криптографічний протокол SSL / TLS: основи, структура та принцип роботи, забезпечення безпеки транзакцій та зв'язку на мережі Інтернет.	лекція, самостійна робота	[5-6]	2 5	1 тиждень
	Тема7.Криптографічний протокол SSL / TLS: основи, структура та принцип роботи, забезпечення безпеки транзакцій та зв'язку на мережі Інтернет.	лаб.	[5-6]	2	

8-9	Тема 8. Криптовалюти та технології блокчейн: принцип роботи, види криптовалют, розвиток технології блокчейн, застосування у віртуальній економіці.	лекція, самостійна робота	[1,2,4-6]	4 6	2 тижні
	Тема 8. Криптовалюти та технології блокчейн: принцип роботи, види криптовалют, розвиток технології блокчейн, застосування у віртуальній економіці.	лаб.	[1,2,4-6]	4	
10	Тема 9. Захист від кібератак: загрози та типи кібератак, методи захисту від кібератак, розробка та застосування криптографічних методів захисту.	лекція, самостійна робота	[1,2,4-6]	2 6	1 тиждень
	Тема 9. Захист від кібератак: загрози та типи кібератак, методи захисту від кібератак, розробка та застосування криптографічних методів захисту.	лаб.	[1,2,4-6]	2	
11	Тема 10. Цифрові ідентифікації та аутентифікація: поняття, принципи, методи та технології, застосування у віртуальній економіці.	лекція, самостійна робота	[1,2,4-6]	2 6	1 тиждень
	Тема 10. Цифрові ідентифікації та аутентифікація: поняття, принципи, методи та технології, застосування у віртуальній економіці.	лаб.	[1,2,4-6]	2	1 тиждень
12-13	Тема 11. Прикладні аспекти криптографії у віртуальній економіці: захист фінансових транзакцій, електронна комерція, збереження конфіденційності даних тощо.	лекція, самостійна робота	[1,2,4]	4 6	2 тижні
	Тема 11. Прикладні аспекти криптографії у віртуальній економіці: захист фінансових транзакцій, електронна комерція, збереження конфіденційності даних тощо.	лаб.	[1,2,4]	4	
14	Тема 12. Юридичні та регуляторні питання криптографії у віртуальній економіці: правові аспекти використання криптографії в електронній комерції, віртуальних грошах та платіжних системах, міжнародне регулювання криптографії та її застосування.	лекція, самостійна робота	[1,2,4,5]	2 4	1 тиждень

	Тема 12. Юридичні та регуляторні питання криптографії у віртуальній економіці: правові аспекти використання криптографії в електронній комерції, віртуальних грошах та платіжних системах, міжнародне регулювання криптографії та її застосування.	лаб.	[1,2,4,5]	2	