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

Затверджено
На засіданні
кафедри теорії оптимальних процесів
факультету прикладної математики та інформатики
Львівського національного університету імені Івана Франка
(протокол № ____ від _____ 2020__ р.)

Завідувач кафедри Шахно С.М.

_____

Силабус з навчальної дисципліни "Основи криптології", що викладається в межах ОПП Системний аналіз першого (бакалаврського) рівня вищої освіти для здобувачів з спеціальності 124 – системний аналіз

Львів 2020 р.

Назва дисципліни	Основи криптології
Адреса викладання дисципліни	Головний корпус ЛНУ ім. І. Франка м. Львів, вул. Університетська 1
Факультет та кафедра, за якою закріплена дисципліна	Факультет прикладної математики та інформатики Кафедра теорії оптимальних процесів
Галузь знань, шифр та назва спеціальності	12 – інформаційні технології 124 – системний аналіз
Викладачі дисципліни	Голуб Богдан Михайлович, доцент кафедри теорії оптимальних процесів Шунькін Юрій Валерійович, асистент кафедри теорії оптимальних процесів
Контактна інформація викладачів	bohdan.holub@lnu.edu.ua; https://ami.lnu.edu.ua/employee/holub; yuriy.shunkin@lnu.edu.ua; https://ami.lnu.edu.ua/employee/shunkin-yu-v; Головний корпус ЛНУ ім. І. Франка, каб. 269. м. Львів, вул. Університетська, 1
Консультації з питань навчання по дисципліні відбуваються	Консультації в день проведення лекцій/практичних занять (за попередньою домовленістю).
Сторінка курсу	https://teams.microsoft.com/_#/school/conversations/%D0%97%D0%B0%D0%B3%D0%B0%D0%BB%D1%8C%D0%BD%D0%B5?threadId=19:979a0bf5d8cb4a49a848aae28ab6ebc6@thread.tacv2&ctx=channel
Інформація про дисципліну	Курс розроблено таким чином, щоб надати учасникам знання основних методів захисту інформації від несанкціоновоного доступу, застосування симетричних та асиметричних алгоритмів криптографії, алгоритмів генерування ключів, цифрового підпису, розподілу таємниці.
Коротка анотація дисципліни	Дисципліна “Основи криптології” є нормативною дисципліною зі спеціальності 124 – системний аналіз для освітньої програми Системний аналіз, яка викладається у 5-му семестрі в обсязі 2-ох кредитів (за Європейською Кредитно-Трансферною Системою ECTS).
Мета та цілі дисципліни	Метою вивчення нормативної дисципліни “Основи криптології” є освоєння студентами теоретичних і практичних основ криптології, криптографії та принципів розробки програмного забезпечення для їх реалізації на робочих станціях і кластерах.
Література для вивчення дисципліни	1. О.В.Вербіцький. Вступ до криптології. – Львів: ВНТЛ, 1998. - 246с. 2. І.Я. Берегуляк.Класичні методи криптування. – Львів: Львівський ун-т, 1997. – 180с. 3. В.Ємець, А.Мельник, Р.Попович. Сучасна криптографія. Основні поняття. – Львів: БаК, 2003. – 144с. 4. Корченко В.П., Сіденко Ю.О., Дрейс О. Г. Прикладна криптологія: системи шифрування. - К. : ДУТ, 2014. – 448 с. 5. Mollin, R. A. Introduction to Cryptography. — CRC Press, 2007. — P. 80. — 413 p. — ISBN 1584886188. 6. Глушаков С.В., Сурядный А.С., Тесленко Н.С. Антихакер. – М.:АСТ,

	2008. – 501с. 7. Б.М.Голуб. Системи захисту інформації. Текст лекцій. – Львів, 2018. Електронна версія.
Обсяг курсу	Загальний обсяг: 96 годин. Аудиторних занять: 64 год., з них 32 год. лекцій та 32 години лабораторних робіт. Самостійної роботи: 32 год.
Очікувані результати навчання	Після завершення цього курсу студент буде : Знати: - класичні криптологічні методи: шифр простої заміни, частотний аналіз, гомофонний шифр заміни, поліграмні шифри, поліалфавітні шифри, шифри перестановок - шифри з використанням булевої алгебри. - криптосистему DES. - математичні основи криптографії: конгруенції, кільце лишків, символ Якобі, розподіл і пошук простих чисел, псевдопрості числа. - асиметричні криптосистеми: RSA, Ель-Гамаля, Рабіна, ймовірнісні алгоритми, алгоритми на основі еліптичних кривих - генератори псевдовипадкових бітів, важкооборотні функції, геш-функції. - архітектуру та методи цифрового підпису, поняття сертифікатів, криптокласи бібліотеки .NET Framework - адміністрування ключами: обмін ключами, розподіл таємниці. - основи стеганографії Вміти: - програмно реалізовувати симетричні та асиметричні криптосистеми - використовувати навички криптоаналізу - утворювати системи цифрового підпису - реалізовувати протоколи обміну ключами та розподілу таємниці
Ключові слова	Криптологія, криптографія, криптоаналіз, симетричні криптосистеми, асиметричні криптосистеми, цифровий підпис.
Формат курсу	Очний, дистанційний Проведення лекцій, лабораторних робіт і консультацій.

Теми	1. Елементарна криптологія 2. Шифри з використанням булевої алгебри 3. Математичні основи криптографії 4. Афінні шифри 5. Арифметичні задачі та алгоритми 6. Факторизація. Розпізнавання квадратичності і добування квадратних коренів 7. Криптосистеми з відкритим ключем 8. Генератори псевдовипадкових бітів 9. Важкооборотні функції 10. Цифровий підпис 11. Адміністрування ключами
Підсумковий контроль, форма	Комбінований залік і екзамен у кінці семестру
Пререквізити	Для вивчення курсу студенти потребують базових знань з - Чисельних методів; - Програмування; - Функціонального аналізу достатніх для сприйняття категоріального апарату методів скінченних і граничних елементів.
Навчальні методи та техніки, які будуть використовуватися під час викладання курсу	Презентації, лекції Індивідуальні завдання Групові проекти, менторство
Необхідне обладнання	Комп'ютер із програмним забезпеченням Visual Studio 2017/2019, Internet доступ до обчислювального кластера.
Критерії оцінювання (окремо для кожного виду навчальної діяльності)	Оцінювання проводиться за 100-бальною шкалою. Бали нараховуються за наступним співвідношенням: • індивідуальні завдання : 50% семестрової оцінки; максимальна кількість балів 50 • екзамен: 50% семестрової оцінки; максимальна кількість балів 50 Підсумкова максимальна кількість балів 100. **Лабораторні роботи:** Очікується, що студенти виконають 10 лабораторних робіт. **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 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. 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 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.
Питання до заліку чи екзамену.	Шифр простої заміни Частотний аналіз Гомофонний шифр заміни Поліграмні шифри Поліалфавітні шифри Шифри перестановок Шифр одноразового блокноту. Композиція (добуток) шифрів Криптосистема DES Модифікації блокових шифрів Дешифрування ітераціями Алгоритм Евкліда Конгруенції. Кільце лишків. Кільце матриць Бінарний метод піднесення до степеня. Випадковий вибір. Первісні корені. Квадратичні лишки. Символ Якобі. Розподіл простих чисел. Ймовірносний тест Соловея-Штрассена. Псевдопрості числа. Ймовірносний тест Міллера-Рабіна Розпізнавання квадратичності і добування квадратних коренів Криптосистема RSA. Криптосистема Рабіна. Криптосистема Ель-Гамаля. Ймовірносне криптування. Криптосистеми на основі еліптичних кривих Генератори псевдовипадкових бітів Важкооборотні функції Цифровий підпис Адміністрування ключами
Опитування	Анкету-оцінку з метою оцінювання якості курсу буде надано по завершенню курсу.