МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Львівський національний університет імені Івана Франка
Механіко-математичний факультет
Кафедра математичної статистики і диференціальних рівнянь

Затверджено
На засіданні
кафедри математичної статистики і диференціальних рівнянь
механіко-математичного факультету
Львівського національного університету імені Івана Франка
(протокол № 1 від 22.06.2023 р.)

Завідувач кафедри: Олег БУГРІЙ

Силабус з навчальної дисципліни
“ Основи захисту інформації ”,
що викладається в межах ОПП “ Статистичний аналіз даних ”
першого (бакалаврського) рівня вищої освіти для здобувачів з спеціальності 112 - Статистика

Львів 2023 р.

Назва дисципліни	Основи захисту інформації
Адреса викладання дисципліни	Головний корпус ЛНУ ім. І. Франка м. Львів, вул. Університетська 1, 79000
Факультет та кафедра, за якою закріплена дисципліна	Механіко-математичний факультет Кафедра математичної статистики і диференціальних рівнянь
Галузь знань, шифр та назва спеціальності	11 - Математика та статистика 112 - Статистика
Викладачі дисципліни	Домanська О.В., кандидат фізико-математичних наук, доцент кафедри математичної статистики і диференціальних рівнянь
Контактна інформація викладачів	olena.domanska@lnu.edu.ua, https://new.mmf.lnu.edu.ua/employee/domanska-o-v;
Консультації з питань навчання по дисципліні відбуваються	Консультації в день проведення лекцій/практичних занять (за попередньою домовленістю). Головний корпус ЛНУ ім. І. Франка, каб. 267. м. Львів, вул. Університетська, 1
Сторінка курсу	https://new.mmf.lnu.edu.ua/course/ozakhi-112-bak23
Інформація про дисципліну	Дисципліна “Основи захисту інформації” є вибірковою дисципліною зі спеціальності 112 – Статистика для освітньої програми “Статистичний аналіз даних”, яка викладається в 8-му семестрі в обсязі 5-х кредитів (за Європейською Кредитно-Трансферною Системою ECTS).
Коротка анотація дисципліни	Курс розроблено для ознайомлення студентів з основними поняттями і методами захисту інформаційних систем.
Мета та цілі дисципліни	*Мета:* ознайомити студентів з основними підходами та методами захисту інформації у комп’ютерних системах. *Цілі:* формування у студентів базових понять про принципи та методи захисту інформаційних систем.
Література для вивчення дисципліни	1) Jonathan Katz, Yehuda Lindell. *Introduction to Modern Cryptography, 3rd ed.* Chapman & Hall, 2020. 2) Jean-Philippe Aumasson. *Serious Cryptography: A Practical Introduction to Modern Encryption.* No Starch Press, 2017. 3) Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman. *An Introduction to Mathematical Cryptography, 2nd ed.* Springer, 2014. 4) Dan Boneh, Victor Shoup. *A Graduate Course in Applied Cryptography.* Published online, 2023. (toc.cryptobook.us) 5) Al Sweigart. *Cracking Codes with Python.* No Starch Press, 2018. 6) Niels Ferguson, Bruce Schneier, Tadayoshi Kohno. *Cryptography Engineering.* Wiley, 2010.
Обсяг курсу	Загальний обсяг: 150 годин. Аудиторних занять: 78 год., з них 39 год. лекційних та 39 годин лабораторних занять. Самостійної роботи: 72 год.
Очікувані	У результаті вивчення даного курсу студент буде:

результати навчання	**знати**: основні завдання захисту інформації, базові алгоритми шифрування, основні протоколи шифрування, поняття про функціонування комп'ютерних систем і мереж, способи і методи їх захисту **вміти**: застосовувати основні методи шифрування інформації, обирати правильні алгоритми шифрування, аналізувати комп'ютерні системи на предмет їх вразливості до атак
Ключові слова	Шифрування, безпека, інформація, криптографія, комп'ютерна мережа, атака, протокол
Формат курсу	Очний
Теми	Див. **Схема курсу**
Підсумковий контроль, форма	Залік
Пререквізити	Для вивчення даного курсу студенти потрібні базові знання з: - Користування комп'ютером; - Алгебри та теорії чисел; - Програмування на Python.
Навчальні методи та техніки, які будуть використовуватися під час викладання курсу	Інформаційні методи (лекція, бесіда, ілюстрація, демонстрація); дедуктивні методи на основі узагальнень; евристичні методи (проблемна лекція); інтерактивні методи (дискусія)
Необхідне обладнання	Для проведення лекційних занять: комп'ютер (мінімальні характеристики: процесор Intel Core i3, 4ГБ оперативної пам'яті), доступ до мережі Internet, засоби мультимедіа (в т.ч. проектор). Для проведення практичних/лабораторних занять: комп'ютер (мінімальні характеристики: процесор Intel Core i3, 4ГБ оперативної пам'яті), доступ до мережі Internet. Необхідне програмне забезпечення включає в себе ОС Windows 10, програмні додатки (MS Teams, MS Excel).
Критерії оцінювання (окремо для кожного виду навчальної діяльності)	Оцінювання проводиться за 100-бальною шкалою. Бали нараховуються за наступним співвідношенням: • Змістовий модуль 1: 20% семестрової оцінки за виконання практичних аудиторних завдань, 20% семестрової оцінки за виконання і захист домашніх завдань, максимальна кількість балів 40. • Змістовий модуль 2: 18% семестрової оцінки за виконання практичних аудиторних завдань, 18% семестрової оцінки за виконання і захист домашніх завдань, максимальна кількість балів 36. • Контрольне тестування: 24% семестрової оцінки, максимальна кількість балів 24. Підсумкова максимальна кількість балів 100. **Академічна доброчесність**: Очікується, що роботи студентів будуть оригінальними дослідженнями чи міркуваннями. Списування та втручання в роботу інших студентів становлять, але не обмежують, приклади можливої академічної недоброчесності. Виявлення ознак академічної недоброчесності в написанні завдань є підставою для її незарахування викладачем, незалежно від масштабів плагіату чи обману.

	Жодні форми порушення академічної доброчесності не толеруються. **Відвідання занять** є важливою складовою навчання. Очікується, що всі студенти відвідають усі лекції та практичні/лабораторні зайняття курсу. Студенти повинні інформувати викладача про неможливість відвідати заняття. У будь-якому випадку студенти зобов'язані дотримуватися термінів визначених для виконання всіх видів робіт, 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 контролі 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. **Оцінювання практичних робіт** (1-ий змістовий модуль містить 10 практичних робіт, 2-ий змістовий модуль – 9 практичних робіт, загалом 19 практичних робіт, максимальна кількість балів: 76) відбувається шляхом оцінки роботи студента під час проведення практичної роботи в аудиторії (0-2 балів за одну роботу) та захисту написаної студентом вдома практичної роботи (0-2 балів за одну роботу). Бали оцінювання аудиторного виконання практичних робіт нараховуються за наступним співвідношенням: 2 – студент в повному обсязі володіє навчальним матеріалом, має повне розуміння розглянутої теми, надає правильні відповіді на запитання по темі, код програми функціонує відповідно до завдання; 1.5 – студент достатньо розуміє розглянутий матеріал та принципи написаного ним коду програми, присутні неточності та незначні помилки у відповідях на запитання по темі, код програми функціонує відповідно до завдання; 1 – студент не досить добре розуміє розглянутий матеріал та написаний ним код програми, вагається та надає неточні/не конкретні відповіді на запитання по темі, код програми функціонує з помірними недоліками; 0.5 – студент погано розуміє розглянутий матеріал та написаний ним код програми, студент в більшості надає помилкові відповіді на питання по темі, код програми не функціонує належним чином; 0 - студент зовсім не засвоїв розглянутий матеріал, написаний ним код програми не відповідає темі/не функціонує взагалі. Бали оцінювання домашнього завершення виконання практичних робіт та наданого звіту нараховуються за наступним співвідношенням: 2 – звіт цілком і повністю відображає індивідуальне завдання студента, містить правильні висновки, ілюстрований (за потреби) відповідними графіками і таблицями які правильно відображають суть виконаного завдання, студент має повне розуміння розглянутої теми, надає правильні відповіді на запитання по темі, код програми функціонує відповідно до завдання; 1.5 – звіт в достатній мірі відображає індивідуальне завдання студента,

	містить допустимі висновки, ілюстрований (за потреби) відповідними графіками і таблицями які частково відображають суть виконаного завдання, студент достатньо розуміє принципи написаного ним коду програми, присутні неточності та незначні помилки у відповідях на запитання по темі, код програми функціонує відповідно до завдання; 1 – звіт містить загальні формулювання завдання, висновки нечіткі, необхідні ілюстрації чи таблиці відсутні, студент не досить добре розуміє розглянутий матеріал та представлений код програми, надає неточні/не конкретні відповіді на запитання по темі, код програми функціонує з помірними недоліками; 0.5 – звіт не містить формулювання завдання, висновки необґрунтовані чи неповні, необхідні ілюстрації чи таблиці відсутні, студент погано розуміє розглянутий матеріал та представлений код програми, студент в більшості надає помилкові відповіді на питання по темі, код програми не функціонує належним чином; 0 – звіт відсутній/не відповідає темі, студент зовсім не засвоїв розглянутий матеріал, написаний ним код програми не відповідає темі/не функціонує взагалі. **Оцінювання контрольного тестування** (завдання з тематики кожного змістового модуля) відбувається шляхом оцінки письмових відповідей студента на поставлені запитання. Відсотки нарахування балів оцінювання відповіді на кожне запитання нараховуються за наступним співвідношенням: 75-100% – тема відтворюється в повному обсязі, правильно, обґрунтовано, логічно; 50-75% – відтворюється значна частина розглянутої теми, проте присутні неточності та/або невідповідності; 25-50% – виявлено множинні неточності та невідповідності, пояснення відсутні чи частково помилкові; 0-25% – тему майже не розкрито, кількість викладеного матеріалу не відповідає загальним нормам обраного виду роботи. **Критерії оцінювання результатів неформальної освіти:** Нарахування балів відбувається за публікацію студентом тез доповідей на конференціях, наукових статей, за участь студента у діяльності наукових гуртків, семінарів, круглих столів, конкурсів, участь у заходах неформальної освіти, за отримання сертифікатів про проходження навчання на різних освітніх платформах (Coursera, Prometheus тощо), курсах провідних IT компаній за тематикою навчальної дисципліни. Кількість балів визначається відсотком покриття результатів відповідної активності до вимог результатів навчання з навчальної дисципліни.
Питання для контрольного тестування	- Означення шифру, алгоритму шифрування - Поняття досконалого шифру - Теорема Шеннона - Опис традиційних історичних криптосистем - Хеш-функції та їх властивості - Автентифікація та цифрові підписи - Означення і основні задачі та результати з теорії складності - Опис протоколу Діффі-Гелмана - Еліптичні криві. Арифметика на еліптичних кривих

	- Еліптичний протокол Діффі-Гелмана - Опис криптосистеми RSA - Основні квантові алгоритми
Опитування	Анкету-оцінку з метою оцінювання якості курсу буде надано по завершенню курсу.

Схема курсу "Основи захисту інформації"
для студентів спеціальності 112 - Статистика

Тижні	Лекційний курс		Практичні заняття		К-сть год СР	Літе-ратура
	Назва теми	К-сть год	Назва теми	К-сть год		
1	2	3	4	5	6	7
1	Методи та завдання безпеки інформаційних систем. Вступ у криптографію.	3	Вступне заняття. Налаштування необхідного програмного забезпечення. Практичні завдання по теорії криптографії.	3	5	[1]-[6], Сайт курсу
2	Традиційні криптосистеми. Досконале шифрування.	3	Написання коду на Python, що реалізовує класичні шифри та їх варіанти. Реалізація шифру Вернама на Python.	3	6	[1]-[6], Сайт курсу
3	Випадковість. Блокові шифри.	3	Написання генераторів випадкових чисел. Задачі на використання вбудованих джерел ентропії у системах Windows/Unix. Практичні завдання на побудову блокових шифрів.	3	5	[1]-[6], Сайт курсу
4	Потокові шифри. Хеш-функції.	3	Практичні завдання на побудову потокових шифрів. Практичні завдання на побудову різноманітних хеш-функцій із використанням компресії та перестановок. Реалізація хеш-таблиць у Python.	3	6	[1]-[6], Сайт курсу
5	Хешування з ключем. Автентифікація в шифруванні. Цифрові підписи.	3	Задачі на побудову хешів із ключем із звичайних хешів. Створення хешів із ключем із потокових шифрів. Реалізація автентифікації із використанням MAC. Практичні завдання на використання AES-GCM для автентифікації.	3	5	[1]-[6], Сайт курсу
6	Вступ в теорію складності обчислень. Задачі в теорії складності.	3	Практичні задачі на теорію складності. Практичні задачі на факторизацію та дискретний логарифм.	3	6	[1]-[6], Сайт курсу
7	Протокол Діффі-Гелмана.	3	Реалізація на Python обміну шифрованими	3	5	[1]-[6], Сайт курсу

			повідомленнями із використанням протоколу Діффі-Гелмана.			
8	Схема Ель-Гамаля.	3	Імплементація протоколу Ель-Гамаля на Python.	3	6	[1]-[6], Сайт курсу
9	Криптосистема RSA.	3	Реалізація RSA на Python. Написання односторонніх функцій на функцій швидкого піднесення до степеня.	3	5	[1]-[6], Сайт курсу
10	Еліптичні криві.	3	Виконання арифметичних операцій на еліптичних кривих. Вправи на еліптичний протокол Діффі-Гелмана.	3	6	[1]-[6], Сайт курсу
11	Пост-квантова криптографія.	3	Вступ у бібліотеку cirq.	3	5	[1]-[6], Сайт курсу
12	Пост-квантові криптографічні алгоритми.	3	Реалізація пост-квантових алгоритмів із використанням бібліотеки cirq.	3	6	[1]-[6], Сайт курсу
13	Підсумкове заняття	3	Перевірка знань та вмінь студентів.	3	6	[1]-[6], Сайт курсу
	Разом	**39**		**39**	**72**	
	Викладач: **Доманська О.В.**		Викладач: **Доманська О.В.**			