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

Затверджено
На засіданні кафедри інформаційних систем факультету прикладної математики та інформатики
Львівського національного університету імені Івана Франка
(протокол № _1_ від _29 серпня_ 2023_ р.)

Завідувач кафедри Шинкаренко Г.А.

Силабус з навчальної дисципліни «Технології захисту інформації», що викладається в межах ОПП Інформатика першого (бакалаврського) рівня вищої освіти для здобувачів з спеціальності 122 Комп'ютерні науки

Львів 2023 р.

Назва дисципліни	Технології захисту інформації
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 інформаційних систем
Галузь знань, шифр та назва спеціальності	Галузь знань: 12 Інформаційні технології Спеціальність: 122 Комп'ютерні науки
Викладачі дисципліни	Бернакевич Ірина Євстахіївна, доцент кафедри інформаційних систем Козій Ірина Ярославівна, доцент кафедри інформаційних систем
Контактна інформація викладачів	Email: iryna.bernakevych@lnu.edu.ua; volodymyr.vovk@lnu.edu.ua Web: https://ami.lnu.edu.ua/employee/bernakevych; https://ami.lnu.edu.ua/employee/vovk-volodymyr Головний корпус ЛНУ ім. І. Франка, каб. 261. Львів, вул. Університетська,1
Консультації з питань навчання по дисципліні відбуваються	Консультації проводять раз на тиждень згідно з оприлюдненим розкладом консультацій викладача. Можливі онлайн консультації через Microsoft Teams.
Сторінка курсу	https://ami.lnu.edu.ua/course/zakhyst-informatsii-kn
Інформація про дисципліну	Курс «Технології захисту інформації» є нормативною дисципліною з спеціальності 122 Комп'ютерні науки для освітньо-професійної програми «Інформатика», яка викладається в сьомому семестрі в обсязі 3-ох кредитів (за Європейською Кредитно-Трансферною Системою ECTS).
Коротка анотація дисципліни	Курс розроблено таким чином, щоб надати учасникам знання принципів захисту інформації, як необхідного інструменту для побудови захищених систем. Тому у курсі представлено програмно-технічні методи захисту інформації як основу захищеної системи. Основну частину курсу займає розгляд практичних і теоретичних аспектів захисту конфіденційності інформації, а також її цілісності та автентичності.
Мета та цілі дисципліни	Метою вивчення нормативної дисципліни «Технології захисту інформації» є освоєння студентами теоретичними і практичними основами захисту інформації від порушення її конфіденційності, цілісності та автентичності.
Література для вивчення дисципліни	1. *Остапов С.Е., Євсеєв С.П., Король О.Г.* Технології захисту інформації: навчальний посібник. – Х.: Новий світ-2000, 2022. – 678 с. 2. *Антонюк А.О.* Моделювання систем захисту інформації: монографія. – Ірпінь: Національний університет ДПС України, 2015. – 273 с. 3. Гулак Г.М. Методологія захисту інформації. Аспекти кібербезпеки: підручник.– К.: Видавництво НА СБ України, 2022. – 256 с. 4. *Корченко О.Г.* Прикладна криптологія: системи шифрування: підручник / О.Г.Корченко, В.П.Сіденко, Ю.О.Дрейс.– К.: ДУТ, 2014.– 448 с. 5. *Бурячок В.Л.* Інформаційна та кібербезпека: соціотехнічний аспект: підручник / В.Л.Бурячок, В.Б.Толубко, В.О.Хорошко, С.В.Толюпа. – К.: ДУТ, 2015. – 288 с.

	6. *Хлобистова О.А., Савченко Ю.Г., Гладка М.В.* Технології захисту інформації [Електронний ресурс]: навчальний посібник. – К.: НУХТ, 2014. – 84 с. 7. *Бернакевич І.Є.* Захист інформації [Електронний ресурс]. Режим доступу: http://e-learning.lnu.edu.ua/course/view.php?id=3009
Обсяг курсу	Загальний обсяг: 90 годин. Аудиторних занять: 48 год., з них 32 год. лекцій та 16 години лабораторних робіт. Самостійної роботи: 42 год.
Очікувані результати навчання	Після завершення цього курсу студент буде: *знати*: • мету та основні завдання захисту інформації, категорії інформаційної безпеки, класифікацію загроз інформаційної безпеки; • типи політик безпеки розмежування доступу, методи захисту інформації, абстрактні моделі захисту інформації; • шкідливе програмне забезпечення та методи протидії; • методи криптографічного захисту інформації на основі симетричних криптосистем; • блокові алгоритми та режими їх роботи; • алгоритми сучасного блокового шифрування; • генератори псевдовипадкових чисел та алгоритми потокового шифрування; • алгоритми асиметричного шифрування; • методи забезпечення цілісності даних та аунтефікації повідомлень; • криптографічні хеш-функції стиснення, на основі блокового шифру; • схеми цифрового підпису; • протоколи ідентифікації та аутентифікації; • протоколи розподілу ключів. *вміти*: • аналізувати та вибирати методи захисту інформації підприємства, будувати політику безпеки; • реалізовувати захист інформації за допомогою симетричного блокового та потокового шифрування; • застосовувати алгоритми асиметричного шифрування для забезпечення конфіденційності, цілісності та автентичності інформації; • створювати електронний цифровий підпис.
Компетентності	*Інтегральна:* Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі комп'ютерних наук або у процесі навчання, що передбачають застосування теорій та методів інформаційних технологій і характеризується комплексністю та невизначеністю умов. *Загальні (ЗК):* ЗК1. Здатність до абстрактного мислення, аналізу та синтезу. ЗК2. Здатність застосовувати знання у практичних ситуаціях. ЗК3. Знання та розуміння предметної області та розуміння професійної діяльності. ЗК6. Здатність вчитися й оволодівати сучасними знаннями ЗК7. Здатність до пошуку, оброблення та аналізу інформації з різних джерел. ЗК8. Здатність генерувати нові ідеї (креативність). *Спеціальні (фахові, предметні) компетентності (СК):* СК3. Здатність до логічного мислення, побудови логічних висновків, використання формальних мов і моделей алгоритмічних обчислень, проектування, розроблення й аналізу алгоритмів, оцінювання їх ефективності та складності,

	розв’язності та нерозв’язності алгоритмічних проблем для адекватного моделювання предметних областей і створення програмних та інформаційних систем. СК8. Здатність проектувати та розробляти програмне забезпечення із застосуванням різних парадигм програмування: узагальненого, об’єктно-орієнтованого, функціонального, логічного, з відповідними моделями, методами й алгоритмами обчислень, структурами даних і механізмами управління. СК14. Здатність застосовувати методи та засоби забезпечення інформаційної безпеки, розробляти й експлуатувати спеціальне програмне забезпечення захисту інформаційних ресурсів об’єктів критичної інформаційної інфраструктури. СК17. Здатність розв’язувати прикладні задачі на основі інтегрованого знання про основні методи інформатики та інформаційні технології, використовувати комп’ютер і технології зв’язку, представляти дані у зрозумілій для всіх формі, яка проявляється у прагненні, здатності і готовності до ефективного застосування сучасних засобів інформаційних та комп’ютерних технологій для розв’язання завдань у професійній діяльності, усвідомлюючи при цьому значущість предмету і результату діяльності.
Програмні результати навчання	ПР1. Застосовувати знання основних форм і законів абстрактно-логічного мислення, основ методології наукового пізнання, форм і методів вилучення, аналізу, обробки та синтезу інформації в предметній області комп'ютерних наук. ПР5. Проектувати, розробляти та аналізувати алгоритми розв’язання обчислювальних та логічних задач, оцінювати ефективність та складність алгоритмів на основі застосування формальних моделей алгоритмів та обчислюваних функцій. ПР9. Розробляти програмні моделі предметних середовищ, вибирати парадигму програмування з позицій зручності та якості застосування для реалізації методів та алгоритмів розв’язання задач в галузі комп’ютерних наук. ПР13. Володіти мовами системного програмування та методами розробки програм, що взаємодіють з компонентами комп’ютерних систем. ПР16. Розуміти концепцію інформаційної безпеки, принципи безпечного проектування програмного забезпечення, забезпечувати безпеку комп’ютерних мереж в умовах неповноти та невизначеності вихідних даних. ПР19. Практично застосувати існуючі та проектувати і розробляти нові алгоритми стиснення даних, побудови завадостійких кодів для мінімізації витрат та підвищення надійності збереження та передавання даних в комп’ютерних інформаційних мережах.
Ключові слова	Політика безпеки, абстрактні моделі захисту інформації, шкідливе програмне забезпечення, симетричні криптосистеми, асиметричні криптосистеми, блокові шифри, потокові шифри, цифровий підпис, протоколи ідентифікації та аунтефікації, розподіл ключів.
Формат курсу	Очний.
Теми	1. **Основні види та джерела атак на інформацію.** Інформація та її властивості. Категорії інформаційної безпеки. Загальні принципи комп’ютерної безпеки. Загрози інформаційної безпеки та їх класифікація. Модель порушника. Політика безпеки та її структура. *лекцій – 2 год., лабораторних – 2 год., самостійна робота – 2 год.* 2. **Методології захисту інформації.** Класифікація методів захисту інформації. Правові, морально-етичні, адміністративні, програмнотехнічні методи захисту. Абстрактні моделі захисту інформації. *лекцій – 2 год., самостійна робота – 3 год.*

	3. **Шкідливе програмне забезпечення та захист від нього.** Методи виявлення вірусів. Структура віруса. Класифікація вірусів та шкідливого програмного забезпечення. Антивіруси та їх класифікація. *лекцій – 2 год., лабораторних – 2 год., самостійна робота – 2 год.* 4. **Елементарна криптографія.** Принцип Керхгофса. Шифри підстановки. Шифри перестановки. *лекцій – 2 год., самостійна робота – 3 год.* 5. **Блокові шифри.** Режими блокових шифрів. Принципи побудови блокових шифрів. Мережа Фейстеля. Базові режими блокових шифрів, їх переваги та недоліки. *лекцій – 2 год., лабораторних – 2 год., самостійна робота – 2 год.* 6. **Сучасні алгоритми блокового шифрування I.** Алгоритм DES, раун-дові перетворення, процедура розгортання ключа. Модифікації алгоритму DES. Вітчизняний алгоритм ДСТУ ГОСТ 28147:2009, режими його використання. *лекцій – 2 год., самостійна робота – 3 год.* 7. **Сучасні алгоритми блокового шифрування II.** Алгоритм шифрування IDEA, структура раунду, раундові перетворення, генерування раундових ключів. Стандарт AES. Криптоаналіз. *лекцій – 2 год., лабораторних – 2 год., самостійна робота – 2 год.* 8. **Потокові шифри.** Генератори псевдовипадкових чисел. Генератор BBS. Регістри зсуву зі зворотним зв'язком. Класифікація потокових шифрів. Потоковий шифр A5. Деталі реалізації та криптоаналіз. Алгоритм RC4. Криптостійкість алгоритму RC4. *лекцій – 2 год., самостійна робота – 3 год.* 9. **Елементи теорії чисел.** Бінарний метод піднесення до степеня. Первісні корені. Квадратичні лишки. Символ Лежандра. Символ Якобі. Псевдопрості числа. Тестування простоти. Ймовірнісні алгоритми тестування простоти. *лекцій – 2 год., лабораторних – 2 год., самостійна робота – 2 год.* 10. **Криптосистеми з відкритим ключем.** Односторонні функції. Криптосистема Меркле–Хеллмана. Алгоритм Шаміра. Криптосистема Рабіна. Криптографічна система Ель-Гамаля. Стандарт шифрування RSA та його стійкість. *лекцій – 2 год., самостійна робота – 3 год.* 11. **Цілісність даних та аунтефікація повідомлень.** Криптрографічні критерії хеш-функцій. Код виявлення модифікацій повідомлення MDC і код автентичності повідомлення MAC. Хеш-код аутентифікації повідомлення HMAC. CMAC. *лекцій – 2 год., лабораторних – 2 год., самостійна робота – 3 год.* 12. **Криптографічні хеш-функції.** Ітеративна криптографічна хеш-функція. Схема Меркеля-Дагмарда. Хеш-функції на основі алгоритмів блокового шифрування. Алгоритм стійкого хешування SHA. Функція гешування за ГОСТом Р 34.11–94. Стійкість геш-функцій. *лекцій – 2 год., самостійна робота – 3 год.* 13. **Цифровий підпис.** Схеми цифрового підпису (RSA, Ель-Гамаля, Шнора). Стандарт цифрового підпису DSS. Класифікація атак на

	схеми цифрового підпису. Особливі схеми цифрового підпису. Електронні гроші. *лекцій – 2 год., лабораторних – 2 год., самостійна робота – 3 год.* 14. **Протоколи ідентифікації та аутентифікації.** Аунтефікація на основі паролю, на основі запиту-відповіді. Підтвердження з нульовим розголошенням. Протокол Фіата-Шаміра. Протокол Фейге-ФіатаШаміра. Протокол Кіскатера-Гійу. Біометрична аутентифікація. *лекцій – 2 год., самостійна робота – 3 год.* 15. **Упраління ключами.** Центр розподілу ключів. Протокол НідхемаШрьодера. Протокол Отвея-Ріcса. Цербер. Домовленість з симетричними ключами. Розподіл відкритого ключа. Інфраструктура відкритих ключів. Режими роботи. Моделі PKI. *лекцій – 2 год., лабораторних – 1 год., самостійна робота – 3 год.* 16. **Розділення секрету.** Основні поняття розділення секрету. Порогові схеми розділення секрету. Схема Блеклі. Схема Шаміра. Схема на основі Китайської теореми про лишки. Досконаліть та ідеальність розділення секрету. (n,n)-порогова схема. *лекцій – 2 год., лабораторних – 1 год., самостійна робота – 2 год.*
Підсумковий контроль, форма	Екзамен у кінці семестру
Пререквізити	Для вивчення курсу студенти потребують базових знань з алгебри, дискретної математики, програмування, математичної криптології.
Навчальні методи та техніки, які будуть використовуватися під час викладання курсу	Презентації, лекції, виконання та оцінювання індивідуальних завдань, самостійна робота з вивченням оприлюднених електронних матеріалів. Проведення тестування студентів на платформі e-learning.lnu.edu.ua. Ознайомлення з Internet курсами по Технологіях захисту інформації Open University courses: https://www.open.edu/openlearn/science-maths-technology/computing-and-ict/systemscomputer/network-security/content-section-0?active-tab=content-tab або COURSERA courses: https://www.coursera.org/learn/metody-i-sredstva-zashity-informacii?
Необхідне обладнання	Для проведення лекцій: комп'ютер, проектор, доступ до мережі Інтернет. Для проведення лабораторних та виконання завдань: комп'ютер, ОС Windows/Linux, доступ до Інтернету, середовище програмування мовою C++, C#, Python (Visual Studio 2022 тощо).
Критерії оцінювання (окремо для кожного виду навчальної діяльності)	Оцінювання проводиться за 100-бальною шкалою. Бали нараховуються за наступним співвідношенням: • індивідуальні завдання : 40% семестрової оцінки; максимальна кількість балів 40 (8 завдань по 5 балів кожне) • колоквіум: 10 % семестрової оцінки; максимальна кількість балів 10 • екзамен: 50% семестрової оцінки; максимальна кількість балів 50

	Підсумкова максимальна кількість балів 100. **Письмові роботи:** Очікується, що студенти виконають одну письмову роботу (тест з теоретичних завдань). **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 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 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 лабораторного 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 екзамену.	1. Категорії інформаційної безпеки. 2. Правові, адміністративні, програмно-технічні методи захисту. 3. Абстрактні моделі захисту інформації. 4. Шкідливе програмне забезпечення. 5. Режими блокових шифрів. 6. Блокові алгоритми шифрування. Алгоритм DES та його модифікації. 7. Вітчизняний алгоритм ДСТУ ГОСТ 28147:2009. 8. Алгоритм шифрування IDEA. 9. Стандарт шифрування AES. 10. Генератори псевдовипадкових чисел. 11. Потоковий шифр A5. Алгоритм RC4. 12. Криптосистеми з відкритим ключем Меркле–Хеллмана, Шаміра, Рабіна, Ель-Гамаля, RSA. 13. Криптографічні хеш-функції. 14. Схеми цифрового підпису. 15. Протоколи ідентифікації та аутентифікації. 16. Упраління ключами. Протоколи.
Опитування	Анкету-оцінку з метою оцінювання якості курсу буде надано по завершенню курсу.