

**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 28 серпня 2023 р.)

Завідувач кафедри Шинкаренко Г.А.



---

**Силабус з навчальної дисципліни**  
**«Технології захисту інформації»,**  
**що викладається в межах ОПП Середня освіта (Інформатика)**  
**першого (бакалаврського) рівня вищої освіти**  
**для здобувачів з спеціальності 014.09 середня освіта**  
**(Інформатика)**

Львів 2023 р.

<b>Назва дисципліни</b>	Технології захисту інформації
<b>Адреса викладання дисципліни</b>	Головний корпус ЛНУ ім. І. Франка м. Львів, вул. Університетська 1
<b>Факультет та кафедра, за якою закріплена дисципліна</b>	Факультет прикладної математики та інформатики Кафедра інформаційних систем
<b>Галузь знань, шифр та назва спеціальності</b>	Галузь знань: 12 Інформаційні технології Спеціальність: 122 Комп'ютерні науки Спеціалізація: Інформатика
<b>Викладачі дисципліни</b>	Бернакевич Ірина Євстахіївна, доцент кафедри інформаційних систем
<b>Контактна інформація викладачів</b>	Email: <a href="mailto:iryna.bernakevych@lnu.edu.ua">iryna.bernakevych@lnu.edu.ua</a> ; Web: <a href="https://ami.lnu.edu.ua/employee/bernakevych">https://ami.lnu.edu.ua/employee/bernakevych</a> ; Головний корпус ЛНУ ім. І. Франка, каб. 261. Львів, вул. Університетська, 1
<b>Консультації з питань навчання по дисципліні відбуваються</b>	Консультації проводять раз на тиждень згідно з оприлюдненим розкладом консультацій викладача. Можливі онлайн консультації через Microsoft Teams.
<b>Сторінка курсу</b>	<a href="https://ami.lnu.edu.ua/course/tekhnolohii-zakhystu-informatsii-so">https://ami.lnu.edu.ua/course/tekhnolohii-zakhystu-informatsii-so</a>
<b>Інформація про дисципліну</b>	Курс «Технології захисту інформації» є нормативною дисципліною з спеціальності 014 Середня освіта для освітньо-професійної програми «Середня освіта (Інформатика)», яка викладається в сьомому семестрі в обсязі 3-ох кредитів (за Європейською Кредитно-Трансферною Системою ECTS).
<b>Коротка анотація дисципліни</b>	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.
<b>Мета та цілі дисципліни</b>	Метою вивчення нормативної дисципліни «Технології захисту інформації» є освоєння студентами теоретичними і практичними основами захисту інформації від порушення її конфіденційності, цілісності та автентичності.
<b>Література для вивчення дисципліни</b>	<ol style="list-style-type: none"> <li>1. <i>Остапов С.Е., Євсєєв С.П., Король О.Г.</i> Технології захисту інформації: навчальний посібник. – Х.: Новий світ-2000, 2022. – 678 с.</li> <li>2. <i>Антонюк А.О.</i> Моделювання систем захисту інформації: монографія. – Ірпінь: Національний університет ДПС України, 2015. – 273 с.</li> <li>3. Гулак Г.М. Методологія захисту інформації. Аспекти кібербезпеки: підручник.– К.: Видавництво НА СБ України, 2022. – 256 с.</li> <li>4. <i>Корченко О.Г.</i> Прикладна криптологія: системи шифрування: підручник / О.Г.Корченко, В.П.Сіденко, Ю.О.Дрейс.– К.: ДУТ, 2014.– 448 с.</li> <li>5. <i>Бурячок В.Л.</i> Інформаційна та кібербезпека: соціотехнічний аспект: підручник / В.Л.Бурячок, В.Б.Толубко, В.О.Хорошко, С.В.Толюпа. – К.: ДУТ, 2015. – 288 с.</li> <li>6. <i>Хлобистова О.А., Савченко Ю.Г., Гладка М.В.</i> Технології захисту інформації [Електронний ресурс]: навчальний посібник. – К.: НУХТ, 2014. – 84 с.</li> <li>7. <i>Бернакевич І.Є.</i> Захист інформації [Електронний ресурс]. Режим доступу: <a href="http://e-learning.lnu.edu.ua/course/view.php?id=3009">http://e-learning.lnu.edu.ua/course/view.php?id=3009</a></li> </ol>

<b>Обсяг курсу</b>	Загальний обсяг: 90 годин. Аудиторних занять: 48 год., з них 24 год. лекцій та 24 години лабораторних робіт. Самостійної роботи: 42 год.
<b>Очікувані результати навчання</b>	<p>Після завершення цього курсу студент буде:</p> <p><i>знати:</i></p> <ul style="list-style-type: none"> <li>– мету та основні завдання захисту інформації, категорії інформаційної безпеки, класифікацію загроз інформаційної безпеки;</li> <li>– типи політик безпеки розмежування доступу, методи захисту інформації, абстрактні моделі захисту інформації;</li> <li>– шкідливе програмне забезпечення та методи протидії;</li> <li>– методи криптографічного захисту інформації на основі симетричних криптосистем;</li> <li>– блокові алгоритми та режими їх роботи;</li> <li>– алгоритми сучасного блокового шифрування;</li> <li>– генератори псевдовипадкових чисел та алгоритми потокового шифрування;</li> <li>– алгоритми асиметричного шифрування;</li> <li>– методи забезпечення цілісності даних та аунтефікації повідомлень;</li> <li>– криптографічні хеш-функції стиснення, на основі блокового шифру;</li> <li>– схеми цифрового підпису;</li> </ul> <p><i>вміти:</i></p> <ul style="list-style-type: none"> <li>– аналізувати та вибирати методи захисту інформації підприємства, будувати політику безпеки;</li> <li>– реалізовувати захист інформації за допомогою симетричного блокового та потокового шифрування;</li> <li>– застосовувати алгоритми асиметричного шифрування для забезпечення конфіденційності, цілісності та автентичності інформації;</li> <li>– створювати електронний цифровий підпис.</li> </ul>
<b>Компетентності</b>	<p><i>Загальні (ЗК):</i></p> <p>ЗК1. Здатність до абстрактного мислення, аналізу та синтезу.</p> <p>ЗК2. Здатність вчитися й оволодівати сучасними знаннями. Застосовувати знання у практичних ситуаціях</p> <p>ЗК3. Знання та розуміння предметної області та розуміння професійної діяльності.</p> <p>ЗК6. Здатність до застосування сучасних інформаційних і комунікаційних технологій у освітній діяльності</p> <p>ЗК7. Здатність генерувати нові ідеї (креативність).</p> <p><i>Спеціальні (фахові, предметні) компетентності (СК):</i></p> <p>СК7. 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.</p> <p>СК11. 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.</p> <p>СК13. Здатність застосовувати методології, технології та інструментальні засоби для управління процесами життєвого циклу інформаційних і програмних систем, продуктів і сервісів інформаційних технологій відповідно до вимог замовника.</p>
<b>Програмні результати навчання</b>	<p>ПР8. 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.</p> <p>ПР11. 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.</p>

	<p>ПР14. 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.</p> <p>ПР16. Застосовувати знання методології та CASE-засобів проектування складних систем, методів структурного аналізу систем, об'єктно-орієнтованої методології проектування при розробці і дослідженні функціональних моделей організаційно-економічних і виробничо-технічних систем.</p>
<b>Ключові слова</b>	<p>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.</p>
<b>Формат курсу</b>	<p>Очний: проведення лекцій, лабораторних робіт та консультацій в приміщеннях університету, а в умовах карантину – онлайнний на платформі Microsoft Teams</p> <p>Ознайомлення з Internet курсами по Технологіях захисту інформації</p> <p>Open University courses:  <a href="https://www.open.edu/openlearn/science-maths-technology/computing-and-ict/systems-computer/network-security/content-section-0?active-tab=content-tab">https://www.open.edu/openlearn/science-maths-technology/computing-and-ict/systems-computer/network-security/content-section-0?active-tab=content-tab</a>  або COURSERA courses:  <a href="https://www.coursera.org/learn/metody-i-sredstva-zashity-informacii?">https://www.coursera.org/learn/metody-i-sredstva-zashity-informacii?</a></p>
<b>Теми</b>	<ol style="list-style-type: none"> <li><b>Основні види та джерела атак на інформацію.</b> 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.</li> <li><b>Методології захисту інформації.</b> Класифікація методів захисту інформації. Правові, морально-етичні, адміністративні, програмно-технічні методи захисту. Абстрактні моделі захисту інформації.</li> <li><b>Шкідливе програмне забезпечення та захист від нього.</b> Методи виявлення вірусів. Структура віруса. Класифікація вірусів та шкідливого програмного забезпечення. Антивіруси та їх класифікація.</li> <li><b>Елементарна криптографія.</b> Принцип Керхгофса. Шифри підстановки. Шифри перестановки.</li> <li><b>Блокові шифри.</b> Режими блокових шифрів. Принципи побудови блокових шифрів. Мережа Фейстеля. Базові режими блокових шифрів, їх переваги та недоліки.</li> <li><b>Сучасні алгоритми блокового шифрування I.</b> Алгоритм DES, раунд-дові перетворення, процедура розгортання ключа. Модифікації алгоритму DES. Вітчизняний алгоритм ДСТУ ГОСТ 28147:2009, режими його використання.</li> <li><b>Сучасні алгоритми блокового шифрування II.</b> Алгоритм шифрування IDEA, структура раунду, раундові перетворення, генерування раундових ключів. Стандарт AES. Криптоаналіз.</li> <li><b>Потокові шифри.</b> Генератори псевдовипадкових чисел. Генератор VBS. Регістри зсуву зі зворотним зв'язком. Класифікація поточкових шифрів. Поточковий шифр A5. Деталі реалізації та криптоаналіз. Алгоритм RC4. Криптостійкість алгоритму RC4.</li> <li><b>Елементи теорії чисел.</b> Бінарний метод піднесення до степеня. Первісні корені. Квадратичні лишки. Символ Лежандра. Символ Якобі. Псевдопрості числа. Тестування простоти. Ймовірнісні алгоритми тестування простоти.</li> <li><b>Криптосистеми з відкритим ключем.</b> Односторонні функції. Криптосистема Меркле–Хеллмана. Алгоритм Шаміра. Криптосистема Рабіна. Криптографічна система Ель-Гамала. Стандарт шифрування RSA та його стійкість.</li> </ol>

	<p>11. <b>Криптографічні хеш-функції.</b> 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.</p> <p>12. <b>Цифровий підпис.</b> Схеми цифрового підпису (RSA, Ель-Гамалія, Шнора). Стандарт цифрового підпису DSS. Класифікація атак на схеми цифрового підпису. Особливі схеми цифрового підпису. Електронні гроші.</p>
<b>Підсумковий контроль, форма</b>	Екзамен у кінці семестру
<b>Пререквізити</b>	Для вивчення курсу студенти потребують базових знань з алгебри, дискретної математики, програмування, математичної криптології.
<b>Навчальні методи та техніки, які будуть використовуватися під час викладання курсу</b>	Презентації, лекції, виконання та оцінювання індивідуальних завдань, самостійна робота з вивченням оприлюднених електронних матеріалів. Проведення тестування студентів на платформі e-learning.lnu.edu.ua.
<b>Необхідне обладнання</b>	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).
<b>Критерії оцінювання (окремо для кожного виду навчальної діяльності)</b>	<p>Оцінювання проводиться за 100-бальною шкалою. Бали нараховуються за наступним співвідношенням:</p> <ul style="list-style-type: none"> <li>• індивідуальні завдання : 40% семестрової оцінки; максимальна кількість балів 40</li> <li>• колоквиум: 10 % семестрової оцінки; максимальна кількість балів 10</li> <li>• екзамен: 50% семестрової оцінки; максимальна кількість балів 50</li> </ul> <p>Підсумкова максимальна кількість балів 100.</p> <p><b>Письмові роботи:</b> Очікується, що студенти виконають одну письмову роботу (тест з теоретичних завдань).</p> <p><b>Академічна доброчесність:</b> 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.</p> <p><b>Відвідання занять</b> 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.</p> <p><b>Література.</b> 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.</p> <p><b>Політика виставлення балів.</b> 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 запізнь на</p>

	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.
<b>Питання до заліку чи екзамену.</b>	<ol style="list-style-type: none"> <li>1. Категорії інформаційної безпеки.</li> <li>2. Правові, адміністративні, програмно-технічні методи захисту.</li> <li>3. Абстрактні моделі захисту інформації.</li> <li>4. Шкідливе програмне забезпечення.</li> <li>5. Режими блокових шифрів.</li> <li>6. Блокові алгоритми шифрування. Алгоритм DES та його модифікації.</li> <li>7. Вітчизняний алгоритм ДСТУ ГОСТ 28147:2009.</li> <li>8. Алгоритм шифрування IDEA.</li> <li>9. Стандарт шифрування AES.</li> <li>10. Генератори псевдовипадкових чисел.</li> <li>11. Поточковий шифр A5. Алгоритм RC4.</li> <li>12. Криптосистеми з відкритим ключем Меркле–Хеллмана, Шаміра, Рабіна, Ель-Гамалія, RSA.</li> <li>13. Криптографічні хеш-функції.</li> <li>14. Схеми цифрового підпису.</li> </ol>
<b>Опитування</b>	Анкету-оцінку з метою оцінювання якості курсу буде надано по завершенню курсу.