

**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     2025   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 А4.09 Середня освіта (Інформатика)**

Львів 2025 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>	А Освіта/Педагогіка А4.09 Середня освіта (Інформатика)
<b>Викладачі дисципліни</b>	Бернакевич Ірина Євстахіївна, доцент кафедри інформаційних систем
<b>Контактна інформація викладачів</b>	<a href="mailto:iryna.bernakevych@lnu.edu.ua">iryna.bernakevych@lnu.edu.ua</a> ; <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. м. Львів, вул. Університетська, 1
<b>Консультації з питань навчання по дисципліні відбуваються</b>	Консультації в день проведення лекцій/практичних занять (за попередньою домовленістю).
<b>Сторінка курсу</b>	<a href="https://ami.lnu.edu.ua/course/tekhnohohii-zakhystu-informatsii-so">https://ami.lnu.edu.ua/course/tekhnohohii-zakhystu-informatsii-so</a>
<b>Інформація про дисципліну</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>Коротка анотація дисципліни</b>	Дисципліна “Технології захисту інформації” є дисципліною за вибором студента з спеціальності А4.09 середня освіта (інформатика) для освітньої програми Середня освіта (інформатика), яка викладається в 5-му семестрі в обсязі 3,5-ох кредитів (за Європейською Кредитно-Трансферною Системою ECTS).
<b>Мета та цілі дисципліни</b>	Метою вивчення нормативної дисципліни “ Технології захисту інформації ” є освоєння студентами теоретичних і практичних основ захисту інформації від порушення її конфіденційності, цілісності та автентичності.
<b>Література для вивчення дисципліни</b>	<ol style="list-style-type: none"> <li>1. <i>Антонюк А.О. Моделювання систем захисту інформації: монографія.</i> – Ірпінь: Національний університет ДПС України, 2015. – 273 с.</li> <li>2. <i>Корченко О. Г. Прикладна криптологія : системи шифрування : підручник / О. Г. Корченко, В. П. Сіденко, Ю. О. Дрейс.</i> – К. : ДУТ, 2014. – 448 с.</li> <li>3. <i>Forouzan B.A. Cryptography and Network Security: A Tutorial.</i> – 2021. – 784 p.</li> <li>4. <i>Хлобистова О.А., Савченко Ю.Г., Гладка М.В. Технології захисту інформації [Електронний ресурс]: навчальний посібник.</i> – К.: НУХТ, 2014. – 84 с.</li> <li>5. <i>Остапов С. Е., Євсєєв С. П., Король О. Г. Технології захисту інформації : навчальний посібник.</i> – Х. : Вид. ХНЕУ, 2013. – 476 с.</li> <li>6. <a href="https://www.coursera.org/learn/metody-i-sredstva-zashity-informacii?">https://www.coursera.org/learn/metody-i-sredstva-zashity-informacii?</a></li> </ol>

<b>Обсяг курсу</b>	Загальний обсяг: 105 годин. Аудиторних занять: 64 год., з них 32 год. лекцій та 32 години лабораторних робіт. Самостійної роботи: 41 год.
<b>Очікувані результати навчання</b>	<p>Після завершення цього курсу студент буде :</p> <p>Знати:</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> <li>- Протоколи ідентифікації та аунтефікації;</li> <li>- Протоколи розподілу ключів.</li> </ul> <p>Вміти:</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>- Будувати електронний цифровий підпис.</li> </ul>
<b>Ключові слова</b>	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.
<b>Формат курсу</b>	<p>Очний, дистанційний</p> <p>Проведення лекцій, лабораторних робіт і консультацій.</p> <p>Ознайомлення з Internet курсами по 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>

Теми	<p>1. <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.</p> <p>2. <b>Методології захисту інформації.</b> Класифікація методів захисту інформації. Правові, морально-етичні, адміністративні, програмно-технічні методи захисту. Абстрактні моделі захисту інформації.</p> <p>3. <b>Шкідливе програмне забезпечення та захист від нього.</b> Методи виявлення вірусів. Структура віруса. Класифікація вірусів та шкідливого програмного забезпечення. Антивіруси та їх класифікація.</p> <p>4. <b>Елементарна криптографія.</b> Принцип Керхгофса. Типи криптографічних атак. Шифри підстановки. Шифри перестановки.</p> <p>5. <b>Блокові шифри. Режими блокових шифрів.</b> Принципи побудови блокових шифрів. Мережа Фейстеля. Базові режими блокових шифрів, їх переваги та недоліки.</p> <p>6. <b>Сучасні алгоритми блокового шифрування I.</b> Алгоритм DES, раундові перетворення, процедура розгортання ключа. Модифікації алгоритму DES. Вітчизняний алгоритм ДСТУ ГОСТ 28147:2009, режими його використання.</p> <p>7. <b>Сучасні алгоритми блокового шифрування II.</b> Алгоритм шифрування IDEA, структура раунду, раундові перетворення, генерування раундових ключів. Стандарт AES. Криптоаналіз.</p> <p>8. <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.</p> <p>9. <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.</p> <p>10. <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.</p> <p>11. <b>Протоколи ідентифікації та аутентифікації.</b> Криптографічні критерії хеш-функцій. Код виявлення модифікацій повідомлення MDC і код автентичності повідомлення MAC. Хеш-код аутентифікації повідомлення HMAC. CMAC.</p> <p>12. <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>13. <b>Цифровий підпис.</b> Схеми цифрового підпису (RSA, Ель-Гамала, Шнора). Стандарт цифрового підпису DSS. Класифікація атак на схеми цифрового підпису. Особливі схеми цифрового підпису. Електронні гроші.</p> <p>14. <b>Протоколи ідентифікації та аутентифікації.</b> Аутентифікація на основі паролю, на основі запиту-відповіді. Підтвердження з нульовим розголошенням. Протокол Фіата-Шаміра. Протокол Фейге-Фіата-Шаміра. Протокол Кіскатера-Гію. Біометрична аутентифікація.</p> <p>15. <b>Управління ключами.</b> Центр розподілу ключів. Протокол Ніідома-Шрьодера. Протокол Отвея-Рісса. Цербер. Домовленість з симетричними ключами. Розподіл відкритого ключа. Інфраструктура відкритих ключів. Режими роботи. Моделі PKI.</p>
------	--

<b>Підсумковий контроль, форма</b>	Залік у кінці семестру
<b>Пререквізити</b>	Для вивчення курсу студенти потребують базових знань з <ul style="list-style-type: none"> <li>- Алгебри;</li> <li>- Дискретна математика;</li> <li>- Програмування;</li> </ul> достатніх для сприйняття категоріального апарату методів скінченних і граничних елементів.
<b>Навчальні методи та техніки, які будуть використовуватися під час викладання курсу</b>	Презентації, лекції Індивідуальні завдання
<b>Необхідне обладнання</b>	Комп'ютер із програмним забезпеченням Visual Studio 2019/2022, Internet доступ до обчислювального кластера.
<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 : 70% семестрової оцінки; максимальна кількість балів 70</li> <li>• колоквиум: 30% семестрової оцінки; максимальна кількість балів 30</li> </ul> <p>Вчасно виконані завдання оцінюються так (у відсотках від максимальної оцінки):</p> <ul style="list-style-type: none"> <li>• 100% – умови завдання виконано повністю, алгоритми складено правильно, програма містить належні коментарі, роботу програми перевірено на достатньому наборі тестових даних, автор відповідає на всі запитання щодо використаних підходів, чітко інтерпретує отримані результати, немає ознак недоброчесності;</li> <li>• 80% – наведено логічно правильну послідовність розв'язування, алгоритми складено правильно, бракує окремих коментарів чи тестів, автор не досить повно пояснює використані підходи, немає ознак недоброчесності;</li> <li>• 60% – у правильній послідовності розв'язування допущено окремі помилки, які автор уміє виправити після зауваження викладача, бракує коментарів чи тестів, на запитання щодо використаних підходів автор відповідає з помилками, немає ознак недоброчесності;</li> <li>• 40% – у правильній послідовності розв'язування пропущено окремі етапи, завдання виконано частково, автор не розуміє недоліків поданої роботи, не вміє їх виправити, немає ознак недоброчесності;</li> <li>• 20% – завдання виконано частково, немає тестів, програма працює правильно для окремих наборів вхідних даних, автор не може самостійно інтерпретувати отримані результати, виправити помилки, немає ознак недоброчесності;</li> <li>• 0% – завдання не виконано, написана програма не відповідає умові, або ж виявлено ознаки недоброчесності: запозичення, фрагменти коду, дію яких автор пояснити не може, автор не володіє відповідним теоретичним матеріалом тощо;</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 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.</p>
<p><b>Питання до заліку чи екзамену.</b></p>	<p>Категорії інформаційної безпеки.  Правові, адміністративні, програмно-технічні методи захисту.  Абстрактні моделі захисту інформації.  Шкідливе програмне забезпечення.  Режими блокових шифрів.  Блокові алгоритми шифрування. Алгоритм DES та його модифікації.  Вітчизняний алгоритм ДСТУ ГОСТ 28147:2009.  Алгоритм шифрування IDEA.  Стандарт шифрування AES.  Генератори псевдовипадкових чисел.  Потоковий шифр A5. Алгоритм RC4.  Криптосистеми з відкритим ключем Меркле–Хеллмана, Шаміра, Рабіна, Ель-Гамала, RSA.  Криптографічні хеш-функції.  Схеми цифрового підпису.  Протоколи ідентифікації та аутентифікації.  Управління ключами. Протоколи.</p>
<p><b>Опитування</b></p>	<p>Анкету-оцінку з метою оцінювання якості курсу буде надано по завершенню курсу.</p>