**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 № \_\_\_\_ від \_\_\_\_\_\_\_ 2020\_\_ р.)

Завідувач кафедри Шинкаренко Г.А.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Силабус з навчальної дисципліни**

**“Захист інформації”,**

**що викладається в межах ОПП Комп’ютерні науки**

**першого (бакалаврського) рівня вищої освіти для здобувачів з спеціальності 122 – комп’ютерні науки**

**Львів 2020 р.**

|  |  |
| --- | --- |
| **Назва дисципліни** | Захист 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** | 12 – інформаційні технології  122 – комп’ютерні науки |
| **Викладачі дисципліни** | Бернакевич Ірина Євстахіївна, доцент кафедри інформаційних систем  Козій Ірина Ярославівна, доцент кафедри інформаційних систем,  Кондратюк Ярослав Вікторович, доцент кафедри інформаційних систем |
| **Контактна інформація викладачів** | [iryna.bernakevych@lnu.edu.ua](mailto:iryna.bernakevych@lnu.edu.ua); <https://ami.lnu.edu.ua/employee/bernakevych>;  [iryna.koziy@lnu.edu.ua](mailto:iryna.koziy@lnu.edu.ua); <https://ami.lnu.edu.ua/employee/kozij-i-ya>;  [Yaroslav.Kondratiuk@lnu.edu.ua](mailto:Yaroslav.Kondratiuk@lnu.edu.ua); <https://ami.lnu.edu.ua/employee/kondratiuk-ya-v>;  Головний корпус ЛНУ ім. І. Франка, каб. 261.  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://ami.lnu.edu.ua/course1/> |
| **Інформація про дисципліну** | 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. |
| **Коротка анотація дисципліни** | Дисципліна “Захист інформації” є нормативною дисципліною з спеціальності 122 – комп’ютерні науки для освітньої програми Комп’ютерні науки, яка викладається в 7-му семестрі в обсязі 4-ох кредитів (за Європейською Кредитно-Трансферною Системою ECTS). |
| **Мета та цілі дисципліни** | Метою вивчення нормативної дисципліни “Захист інформації” є освоєння студентами теоретичних і практичних основ захисту інформації від порушення її конфіденційності, цілісності та автентичності. |
| **Література для вивчення дисципліни** | 1. *Антонюк А.О.* **Mоделювання систем захисту інформації: монографія**. – Ірпінь: Національний університет ДПС України, 2015. – 273 с. 2. *Корченко О. Г.* **Прикладна криптологія : системи шифрування** *: підручник /* О. Г. Корченко, В. П. Сіденко, Ю. О. Дрейс. – К. : ДУТ, 2014. – 448 с. 3. *Фороузан Б.А.***Криптография и безопосность сетей: Учебное пособие.** – М.: Интернет-Университет Информационных Технологий: БИНОМ. Лаборатория знаний, 2010. – 784 с. 4. Хлобистова О.А., Савченко Ю.Г., Гладка М.В. **Технології захисту інформації** [Електронний ресурс]: навчальний посібник. – К.: НУХТ, 2014. – 84 с. 5. *Остапов С. Е., Євсеєв С. П., Король О. Г.* **Технології захисту інформації : навчальний посібник.** – Х. : Вид. ХНЕУ, 2013. – 476 с. 6. *Панасенко С.* **Алгоритмы шифрования. Специальный справочник.** СПб.:БХВ-Петербург, 2009.- 576 с. 7. *Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф.* **Защита информации в компьютерных системах и сетях** / Под ред. В.Ф. Шаньгина. – М.: Радио и связь, 2001. – 376 с. 8. https://www.coursera.org/learn/metody-i-sredstva-zashity-informacii? |
| **Обсяг курсу** | Загальний обсяг: 120 годин. Аудиторних занять: 64 год., з них 32 год. Лек­цій та 32 години лабораторних робіт. Самостійної роботи: 56 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; * Будувати електронний цифровий підпис. |
| **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, дистанційний  Проведення лекцій, лабораторних робіт і консультацій.  Ознайомлення з Internet курсами по Захисту інформації  [Open University courses](http://www.open.ac.uk/courses/types):  <https://www.open.edu/openlearn/science-maths-technology/computing-and-ict/systems-computer/network-security/content-section-0?active-tab=content-tab>  або COURSERA courses:  https://www.coursera.org/learn/metody-i-sredstva-zashity-informacii? |
| **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. 2. **Методології захисту інформації.** Класифікація методів захисту інформації. Правові, морально-етичні, адміністративні, програмно-технічні методи захисту. Абстрактні моделі захисту інформації. 3. **Шкідливе програмне забезпечення та захист від нього.** Методи виявлення вірусів. Структура віруса. Класифікація вірусів та шкідливого програмного забезпечення. Антивіруси та їх класифікація. 4. **Елементарна криптографія.** Принцип Керхгофса. Типи криптографічних атак. Шифри підстановки. Шифри перестановки. 5. **Блокові шифри. Режими блокових шифрів.** Принципи побудови блокових шифрів. Мережа Фейстеля. Базові режими блокових шифрів, їх переваги та недоліки. 6. **Сучасні алгоритми блокового шифрування I.** Алгоритм DES, раундові перетворення, процедура розгортання ключа. Модифікації алгоритму DES. Вітчизняний алгоритм ДСТУ ГОСТ 28147:2009, режими його використання. 7. **Сучасні алгоритми блокового шифрування II.** Алгоритм шифрування IDEA, структура раунду, раундові перетворення, генерування раундових ключів. Стандарт AES. Криптоаналіз. 8. **Потокові шифри.** Генератори псевдовипадкових чисел. Генератор BBS. Регістри зсуву зі зворотним зв'язком. Класифікація потокових шифрів. Потоковий шифр А5. Деталі реалізації та криптоаналіз. Алгоритм RC4. Криптостійкість алгоритму RC4. 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. 10. **Криптосистеми з відкритим ключем.** Односторонні функції. Криптосистема Меркле–Хеллмана. Алгоритм Шаміра. Криптосистема Рабіна. Криптографічна система Ель-Гамаля. Стандарт шифрування RSA та його стійкість. 11. **Протоколи ідентифікації та аутентифікації.** Криптрографічні критерії хеш-функцій. Код виявлення модифікацій повідомлення MDC i код автентичності повідомлення MAC. Хеш-код аутентифікації повідомлення HMAC. CMAC. 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. 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. 14. **Протоколи ідентифікації та аутентифікації.** Аунтефікація на основі паролю, на основі запиту-відповіді. Підтвердження з нульовим розголошенням. Протокол Фіата-Шаміра. Протокол Фейге-Фіата-Шаміра. Протокол Кіскатера-Гійу. Біометрична аутентифікація. 15. **Упраління ключами.** Центр розподілу ключів. Протокол Ніідома-Шрьодера. Протокол Отвея-Рісса. Цербер. Домовленість з симетричними ключами. Розподіл відкритого ключа. Інфраструктура відкритих ключів. Режими роботи. Моделі PKI. |
| **Підсумковий контроль, форма** | Екзамен у кінці семестру |
| **Пререквізити** | Для вивчення курсу студенти потребують базових знань з   * Алгебри; * Дискретна математика; * Програмування;   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 |
| **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.  **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.  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 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 заліку чи екзамену.** | 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 А5. Алгоритм RC4.  Криптосистеми з відкритим ключем Меркле–Хеллмана, Шаміра, Рабіна, Ель-Гамаля, RSA.  Криптографічні хеш-функції.  Схеми цифрового підпису.  Протоколи ідентифікації та аутентифікації.  Упраління ключами. Протоколи. |
| **Опитування** | Анкету-оцінку з метою оцінювання якості курсу буде надано по завер­шенню курсу. |