МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Львівський національний університет імені Івана Франка
Факультет електроніки та комп'ютерних технологій
Кафедра радіоелектронних і комп'ютерних систем

Затверджено
На засіданні кафедри радіоелектронних і комп'ютерних систем
факультету електроніки та комп'ютерних технологій
Львівського національного університету імені Івана Франка
(протокол № 1/24 від 28.08 2023 р.)

Завідувач кафедри:
_____ Ігор ОЛЕНИЧ

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

Львів 2023 р.

Назва дисципліни	Технології захисту інформації
Адреса викладання дисципліни	м. Львів, вул. Драгоманова, 50
Факультет та кафедра, за якою закріплена дисципліна	Факультет електроніки та комп'ютерних технологій, кафедра радіоелектронних і комп'ютерних систем
Галузь знань, шифр та назва спеціальності	12 Інформаційні технології, 122 Комп'ютерні науки
Викладачі дисципліни	Монастирський Любомир Степанович, докт. фіз.-мат. наук, професор
Контактна інформація викладачів	liubomyr.monastyrskii@lnu.edu.ua, https://electronics.lnu.edu.ua/employee/monastyrskii-l-s
Консультації з питань навчання по дисципліні відбуваються	Консультації в день проведення лекційних занять (за попередньою домовленістю). Також можливі он-лайн консультації через MS Teams. Для погодження часу он-лайн консультацій слід писати на електронну пошту викладача.
Сторінка дисципліни	https://e-learning.lnu.edu.ua/enrol/index.php?id=1487
Інформація про дисципліну	Дисципліна «Технології захисту інформації» є нормативною дисципліною з спеціальності 122 - Комп'ютерні науки для освітньої програми «Комп'ютерні науки», яка викладається в 7-му семестрі в обсязі 4.0 кредитів (за Європейською Кредитно-Трансферною Системою ECTS).
Коротка анотація дисципліни	Навчальну дисципліну розроблено таким чином, щоб надати учасникам необхідні знання про принципи роботи, будову та особливості використання криптології та стеганографії, основних типів сенсорів, перетворювачів та виконавчих механізмів, які використовуються в інформаційних системах і технологіях захисту інформації. Зокрема, розглянуто особливості застосування IoT, методи аналізу їх характеристик і методи створення інтерфейсних схем для зв'язку сенсорів і виконавчих механізмів захищених обєктів.
Мета та цілі дисципліни	Метою вивчення нормативної дисципліни «Технології захисту інформації» є виклад основ криптології, криптоаналізу, стеганографії та фізико-технічних методів захисту інформації.
Література для вивчення дисципліни	Основна література: 1. Л.С. Монастирський. Системи і методи захисту інформації. Навчальний посібник – Львів: Львівський національний університет ім. І. Франка, 2013. – 172 с. 2. Л.С. Монастирський. Методичні вказівки з курсу.— Львів, Вид.центр ЛНУ, 2012, -166с. 3. Жаровський Р.О. Методичні вказівки до виконання лабораторних робіт з дисципліни Захист інформації у комп'ютерних системах. 2019, Житомир. 4. В. Ємець, А. Мельник, Р. Попович. Сучасна криптографія. Основні поняття. Львів-2013, "Бак", -144с. 5. Т. Корнієнко, А. Мельник, В. Мельник. Алгоритм та процеси симетричного блокового шифрування. Львів-2013, "Бак", -168с. 6. Release OpenSSL 3.2.1 **2023**. *7.* Пузиренко, Олександр (2006). Комп'ютерна стеганографія. Теорія і практика Монографія. Архів оригіналу за 20 січня 2022. *(*PDF, 6,03MB*)* 8. Закон України «Про засади інформаційної безпеки України» Режим доступу: https://ips.ligazakon.net/document. 9. І.Гадзинська Захист даних під час війни. Що змінилось в Україні у 2023 -му. **2023**-07-26.

Обсяг курсу	64 години аудиторних занять. З них 32 години лекцій, 32 години лабораторних робіт та 56 годин самостійної роботи
Очікувані результати навчання	Після завершення цього курсу студент буде: - знати: основні поняття (означення) предмету; фундаментальні принципи криптології, криптоаналізу, квантової криптографії та стеганографії; фізичні основи роботи сенсорних систем захисту інформації. - вміти: застосовувати крипто- та стеганоалгоритми для захисту конкретних інформаційних систем; вміти застосовувати сенсори та системи відеоспостережень для захисту об'єктів, користуватись бібліотекою OpenSSL Після вивчення даного курсу здобувачі набудуть таких Загальних (ЗК), Спеціальних/Фахових (СК) компетентностей та Програмних результатів навчання (ПР): СК 14. Здатність застосовувати методи та засоби забезпечення інформаційної безпеки, розробляти й експлуатувати спеціальне програмне забезпечення захисту інформаційних ресурсів об'єктів критичної інформаційної інфраструктури. ПР 16. Розуміти концепцію інформаційної безпеки, принципи безпечного проектування програмного забезпечення, забезпечувати безпеку комп'ютерних мереж в умовах неповноти та невизначеності вихідних даних.
Ключові слова	Захист інформації, шифр, криптосистема, алгоритм, обробка інформації, сенсорні системи, протокол SSL/TLS
Формат курсу	Очний / змішаний
	Проведення лекцій, лабораторних робіт та консультації для кращого розуміння тем
Теми	Див. СХЕМА КУРСУ
Підсумковий контроль, форма	Іспит в кінці семестру
Пререквізити	Для вивчення курсу студенти потребують базових знань з дисциплін «Дискретна математика», «Операційні системи» , «Онови електроніки»
Навчальні методи та техніки, які будуть використовуватися під час викладання курсу	Презентації, лекції, лабораторні роботи, контрольні роботи, обговорення.
Необхідне обладнання	Для проведення лекційних занять: • монітор TFT 23"; • системний блок (процесор Intel i5-6500, 8GB оперативної пам'яті, HDD 256GB) ; • мультимедійне обладнання (проектор, проекційний екран, дошка настінна, звуковий підсилювач та аудіосистема); • комутатор мережевий для доступу до мережі Internet. Для проведення лабораторних занять: • комп'ютерна лабораторія з 12-14 робочими місцями; • монітори TFT 23"; • системні блоки (процесор Intel i5-6500, 8GB оперативної пам'яті, HDD 256GB); • мультимедійне обладнання (проектор, проекційний екран, дошка настінна, звуковий підсилювач та аудіосистема); • комутатор мережевий для доступу до мережі Internet. • Мікрокомпютери Rasperry Pi 4 model B

	• ІЧ детектори руху • Детектори затоплення • Smart камери відеоспостереження ICSEE
Критерії оцінювання (окремо для кожного виду навчальної діяльності)	Оцінювання проводиться упродовж семестру за 100-бальною шкалою. Бали нараховуються за такими видами робіт з наступним співвідношенням: • лабораторні роботи: 40% семестрової оцінки; максимальна кількість балів 40. • контрольні заміри (2 модулі): 20% семестрової оцінки; максимальна кількість балів 20. • іспит: 40% семестрової оцінки; максимальна кількість балів 40. Загалом упродовж семестру 100 балів. **Контрольні заміри проводяться у формі контрольних завдань. Академічна доброчесність**: Очікується, що лабораторні та контрольні роботи студентів будуть їх оригінальними дослідженнями чи міркуваннями. Відсутність посилань на використані джерела, фабрикування джерел, списування, втручання в роботу інших студентів становлять приклади можливої академічної недоброчесності. Виявлення ознак академічної недоброчесності в 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 і лабораторні заняття курсу. Студенти мають інформувати викладача про неможливість відвідати заняття. Студенти зобов'язані дотримуватися усіх термінів визначених для виконання усіх 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 на 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. **Критерії оцінювання результатів неформальної освіти**: Нарахування балів відбувається за написання студентом тез доповідей на конференціях, наукових статей, участь у діяльності наукових гуртків, участь у наукових семінарах та круглих столах, конкурсах, участь у заходах неформальної освіти за отримання сертифікатів про проходження навчання на різних освітніх платформах (Coursera, Prometheus тощо), курсах на провідних ІТ компаніях за тематикою навчальної дисципліни. Кількість балів визначається відсотком покриття результатів відповідної активності до вимог результатів навчання з навчальної дисципліни.

Питання до модульного контролю	Перелік питань та завдань для проведення підсумкової оцінки знань певних тем до контрольних робіт розміщені на веб-сторінці та авторському посібнику.
Опитування	Анкету-оцінку з метою оцінювання якості курсу буде надано по завершенню курсу.

СХЕМА КУРСУ

Тиж.	Тема, план, короткі тези	Форма діяльності (заняття)	Література. Ресурси в Інтернеті	Завдання (лабораторна робота), год	Термін виконання
1	**Тема 1.** Вступ. Методологія захисту інформації та її структура. Система електронного документообігу. Закон України про захист інформації. Огляд систем захисту інформації, доступу та аутентифікації.	Лекція	1, 2, 3, 4, 5, 6. 8, 9	Системи захисту інформації, доступу та аутентифікації. Закон України про захист інформації Вибір індивідуальних завдань, 2 год	2 тиж. семестру
2	**Тема 2.** Моделі захисту. Механізми і політика розмежування прав доступу. Методи та пристрої забезпечення захисту і безпеки.	Лекція	1, 2, 3, 4, 8, 9	.	3 тиж. семестру
3	**Тема 3.** Криптологія та криптоаналіз. Класична криптографія. Шифри підстановки та перестановки. Шифри Віженера та комбіновані шифри. Методи криптоаналізу.	Лекція	1, 2, 3, 6, 7	Програмна реалізація алгоритмів класичної криптографії , 4 год.	4 тиж. семестру
4	**Тема 4.** Статистична обробки інформації. Поліалфавітні шифри.	Лекція	1, 2, 5, 6, 8		5 тиж. семестру
5	**Тема 5.** Подання інформації у цифровій формі. Шифр одноразового блокноту. Основні напрямки розвитку сучасної криптографії.	Лекція	1, 2, 3, 4, 5, 8	Програмна реалізація алгоритмів класичної криптографії Бібліотека Open SSL	6 тиж. семестру
6	**Тема 6.** Симетричні криптосистеми та алгоритми DES, AES, ГОСТ. Математичний підхід в криптографії. Алгоритм Евкліда.	Лекція	1, 2, 3, 4, 6, 8	Системи блочного шифрування DESX, DES100, Krypton, 4 год.	7 тиж. семестру
7	**Тема** 7. Розклад на множники, конгруенції. Кільце лишків.	Лекція	1, 2, 4, 5, 6, 7	Бібліотека Open SSL, 2 год	8 тиж. семестру
8	**Тема 8.** Афінні шифри, функція Ойлера. Асиметричні криптосистеми та алгоритми. Важкооборотні функції. Системи RSA/DH.	Лекція	1, 2, 3, 5, 7, 8		9 тиж. семестру
9	**Тема 9.** Системи Рабіна та Ель Гамаля. Цифровий підпс. Функції хешування. Протоколи обміну ключами. Підпис на основі RSA/DH.	Лекція	1, 2, 3, 5, 6, 8	Криптографія відкритого ключа. Робота з пакетом PGP..Захист аудіозв'язку 4 год.	10 тиж. семестру
10	**Тема 10.** Генерування випадкових і псевдовипадкових послідовностей. Генератор BBS.	Лекція	1, 2, 3, 4, 5, 8		11 тиж. семестру
11	**Тема 11.** Сенсорні системи. Інфрачервоні пасивні системи захисту. Будова і принцип дії.	Лекція	1, 2, 3, 4	Системи технічного захисту інформаційних об'єктів (інфрачервоні датчики руху) , 4 год.	12 тиж. семестру
12,	**Тема 12.** Ультазвукові і комбіновані сенсорні системи захисту. Датчики задимлення, герконові датчики. Захист телефонних ліній.	Лекція	1, 2, 3, 5		13 тиж. семестру

13	**Тема 13.** Проектування системи захисту інформаційних об’єктів. Системи відеоспостереження. Охорона периметру. Фотоелектричні захисні системи.	Лекція	1, 2, 3, 6	Системи відеоспостереження (Videoinspector), 4 год.	14 тиж. семестру
14	**Тема 14.** Захист інформації в комп’ютерних мережах. Проксі-сервер і брандмауери. Антивірусний захист.	Лекція	1, 2, 4, 5, 6	Захист Skype. Захист месенджерів, 4 год.	15 тиж. семестру
15	**Тема 15.** Захист персональних комп’ютерів. Стеганографія та квантова криптографія – сучасні напрями захисту інформації.	Лекція	1, 2, 4, 5, 6, 8	Стеганографія. S-tools, 4 год.	16 тиж. семестру
16	**Тема 16.** Перспективи захисту інформаційних ресурсів. Банківські системи захисту.	Лекція	1, 2, 3, 4, 6, 8	Технічні системи захисту інформації. Презентація індивідуального завдання	Підсумки