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 РКС
факультету електроніки та комп'ютерних технологій
Львівського національного університету імені Івана Франка
(протокол № 1/20 від 31 серпня 2020 р.)

В.о. завідувача кафедри _____

Силабус з навчальної дисципліни «Захист інформації», що викладається в межах ОПП «Комп'ютерні науки та інформаційні технології» третього рівня вищої освіти для здобувачів з спеціальності 122 «Комп'ютерні науки та інформаційні технології»

Львів 2020

Назва дисципліни	Захист 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 та інформаційні технології
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://ami.lnu.edu.ua/wp-content/uploads/2021/05/Sylabus_Zahyst_Informacii_2020.pdf
Інформація про дисципліну	Дисципліна «Захист інформації» є нормативною дисципліною з спеціальності 122 Комп'ютерні науки та інформаційні технології для освітньої програми «Комп'ютерні науки та інформаційні технології», яка викладається в 4 семестрі в обсязі 3 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 основних типів сенсорів, перетворювачів та виконавчих механізмів, які використовуються в інформаційних системах і технологіях. Зокрема, розглянуто особливості застосування сенсорів у IoT, методи аналізу їх характеристик і методи створення інтерфейсних схем для зв'язку сенсорів і виконавчих механізмів.
Мета та цілі дисципліни	Метою вивчення нормативної дисципліни **«**Захист інформації» є виклад основ криптології, криптоаналізу, стеганографії та фізико-технічних методів захисту інформації.
Література для вивчення дисципліни	Основна література: 1. Технології захисту інформації [Електронний ресурс] : підручник для студ. спеціальності 122 «Комп'ютерні науки» / Ю. А. Тарнавський; КПІ ім. Ігоря Сікорського.– Київ : КПІ ім. Ігоря Сікорського, 2018. – 162 с. 2. Л.С. Монастирський. Системи і методи захисту інформації. Навчальний посібник – Львів: Львівський національний університет ім. І. Франка, 2013. – 172 с. 3. Основы информационной безопасности : учебное пособие для студентов вузов / Е.В. Вострецова.— Екатеринбург : Изд-во Урал. ун-та, 2019. – 204 с. 4. Криптологія у прикладах, тестах і задачах: навч. посібник / Т.В. Бабенко, Г.М. Гулак, С.О. Сушко, Л.Я. Фомичова. – Д.: Національний гірничий університет, 2013. – 318 с. 5. Защита информации в компьютерных системах / под ред. Е.В. Стельмашонок, И.Н. Васильевой. – СПб. : Изд-во СПбГЭУ, 2017. – 163 с.. Додаткова література: 6. В. Ємець, А. Мельник, Р. Попович. Сучасна криптографія. Основні погяття. Львів-2003, "Бак", -144с. 7. Л.С. Монастирський. Методичні вказівки з курсу.— Львів,

	Вид.центр ЛНУ, 2012, -166с. 8. Т. Корнієнко, А. Мельник, В. Мельник. Алгоритм та процеси симетричного блокового шифрування. Львів-2003, "Бак", -168с. 9. Kabbas A., Alharthi A, Munshi A. Artificial Intelligence Applications in Cybersecurity. IJCSNS International Journal of Computer Science and Network Security, VOL.20 No.2, Fabruary 2020. 120-124. 10. IBM QRadar Security Intelligence. [online] Ibm.com. Available at: https://www.ibm.com/security/security-intelligence/qradar [Accessed 6 Dec. 2019].
Обсяг курсу	48 годин аудиторних занять. З них 32 години лекцій, 16 годин практичних занять та 42 години самостійної роботи
Очікувані результати навчання	Після завершення цього курсу здобувач вищої освіти буде: - знати: основні поняття (означення) предмету; фундаментальні принципи криптології, криптоаналізу, квантової криптографії та стенографії; фізичні основи роботи сенсорних систем захисту інформації. - вміти: застосовувати крипто- та стеноалгоритми для захисту конкретних інформаційних об'єктів; вміти застосовувати сенсори та відеосистеми для захисту об'єктів
Ключові слова	Захист, шифр, алгоритм, обробка інформації, криптосистема, сенсорні системи
Формат курсу	Очний
	Проведення лекцій, виконання практичних завдань та консультації для кращого розуміння тем
Теми	Див. СХЕМА КУРСУ
Підсумковий контроль, форма	Іспит в кінці семестру
Пререквізити	Для вивчення курсу здобувачі вищої освіти потребують базових знань з дисциплін «Спеціалізовані комп'ютерні системи», «Програмування вбудованих систем»
Навчальні методи та техніки, які будуть використовуватися під час викладання курсу	Презентація, лекції, практичні завдання, обговорення.
Необхідне обладнання	Мультимедіа, платформа Moodle, комп'ютерне програмне забезпечення
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: • практична робота: 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 тестових завдань. Академічна доброчесність**: Очікується, що лабораторні та контрольні роботи здобувачів вищої освіти будуть їх оригінальними дослідженнями чи міркуваннями. Відсутність посилань на використані джерела, фабрикування джерел, списування, втручання в роботу інших здобувачів вищої освіти становлять, але не обмежують, приклади можливої академічної недоброчесності. Виявлення ознак академічної

	недоброчесності в роботі здлбувача вищої освіти є підставою для її незарахуванння викладачем, незалежно від масштабів плагіату чи обману. **Відвідання занять** є важливою складовою навчання. Очікується, що всі здобувачі вищої освіти відвідають усі лекції і практичні заняття курсу. Здобувачі вищої освіти мають інформувати викладача про неможливість відвідати заняття. Здобувачі вищої освіти зобов'язані дотримуватися усіх термінів визначених для виконання усіх видів робіт, передбачених курсом. **Література.** Уся література, яку здобувачі вищої освіти не зможуть знайти самостійно, буде надана викладачем виключно в освітніх цілях без права її передачі третім особам. Здобувачі вищої освіти 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 здобувача вищої освіти під час практичних занять; 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 контрольних робіт	Перелік питань та завдань для проведення підсумкової оцінки знань певних тем до контрольних робіт розміщені на веб-сторінці.
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, год	Термін виконання
1	**Тема 1.** Вступ. Методологія захисту інформації та її структура. Система електронного документообігу. Закон України про захист інформації. Огляд безпеки системи захисту, доступу та аутентифікації.	Лекція	1, 2, 3, 4, 5, 6	Захист комп'ютерних ОС та ПК (адміністрування).	2 тиж. семестру
2	**Тема 2.** Моделі захисту. Захист пам'яті. Механізми і політика розмежування прав доступу. Методи та пристрої забезпечення захисту і безпеки.	Лекція	1, 2, 3, 4, 8		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	Криптографія відкритого ключа. Робота з пакетом PGP-60. Бібліотека Open SSL	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	Системи блочного шифрування DESX, DES100, Krypton	6 тиж. семестру
6	**Тема 6.** Симетричні криптосистеми та алгоритми DES, AES, ГОСТ.	Лекція	1, 2, 3, 4, 6, 8	.	7 тиж. семестру

	Математичний підхід в криптографії. Алгоритм Евкліда.				
7	**Тема** 7. Розклад на множники, конгруенції. Кільце лишків.	Лекція	1, 2, 4, 5, 6, 7	Програмна реалізація алгоритмів класичної криптографії на мові Turbo Pascal.	8 тиж. семестру
8	**Тема 8.** Афінні шифри, функція Ойлера. Асиметричні криптосистеми та алгоритми. Важкооборотні функції. Системи RSA/ДН.	Лекція	1, 2, 3, 5, 7, 8		9 тиж. семестру
9	**Тема 9.** Системи Рабіна та Ель Гамаля. Цифровий підпс. Фукнції хешування. Протоколи обміну ключами. Підпис на основі RSA/ДН.	Лекція	1, 2, 3, 5, 6, 8	Захист аудіозв'язку (PGP Fone). Телеконференції (Net Meeting).	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).	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)	14 тиж. семестру
14	**Тема 14.** Захист інформації в комп'ютерних мережах. Проксі-сервер і брандмауери. Антивірусний захист.	Лекція	1, 2, 4, 5, 6		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, 9	Стеганографія. S-tools Технічні системи захисту інформації	16 тиж. семестру
16	**Тема 16.** Перспективи захисту інформаційних ресурсів. Банківські системи захисту.	Лекція	1, 2, 3, 4, 6, 8, 9, 10		