МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Львівський національний університет імені Івана Франка
Факультет електроніки та комп'ютерних технологій
Кафедра оптоелектроніки та інформаційних технологій

Затверджено
На засіданні кафедри радіофізики та комп'ютерних технологій
факультету електроніки та комп'ютерних технологій
Львівського національного університету імені Івана Франка
(протокол №12/23 від 20 червня 2023 р.)

Завідувач кафедри _____ Іван КАРБОВНИК

Силабус з навчальної дисципліни
«Високорівневі системи комп'ютерного захисту»,
що викладається в межах ОП «Комп'ютерні науки»
другого (магістерського) рівня вищої освіти
для здобувачів зі спеціальності
122 – Комп'ютерні науки

Львів 2023

Назва дисципліни	Високорівневі системи комп’ютерного захисту
Адреса викладання дисципліни	м. Львів, вул. Тарнавського, 107
Факультет та кафедра, за якою закріплена дисципліна	Факультет електроніки та комп’ютерних технологій, кафедра радіофізики та комп’ютерних технологій
Галузь знань, шифр та назва спеціальності	12 Інформаційні технології, 122 Комп’ютерні науки
Викладачі дисципліни	Назаркевич Марія Андріївна, докт. тех. наук, проф., проф.
Контактна інформація викладачів	mariia.nazarkevych@ lnu.edu.ua https://electronics.lnu.edu.ua/employee/nazarkevych-mariia-andriivna
Консультації з питань навчання по дисципліні відбуваються	Консультації в день проведення лекційних занять (за попередньою домовленістю): кімн. 310, корпус факультету електроніки та комп’ютерних технологій, м. Львів, вул. Тарнавського, 107. Он-лайн консультації можливі через MS Teams. Для погодження часу он-лайн консультацій слід писати на електронну пошту викладача.
Сторінка дисципліни	https://e-learning.lnu.edu.ua/course/view.php?id=4878 https://electronics.lnu.edu.ua/course/systemy-kompyuternoji-matematyky
Інформація про дисципліну	Дисципліна «Високорівневі системи комп’ютерного захисту» є вибірковою дисципліною зі спеціальності 122 Комп’ютерні науки для освітньої програми «Комп’ютерні науки», яка викладається в 2 семестрі в обсязі 6,0 кредитів (за Європейською Кредитно-Трансферною Системою – ECTS).
Коротка анотація дисципліни	**Предметом** вивчення навчальної дисципліни "Високорівневі системи комп'ютерного захисту" є вивчення технологій захисту з машинним навчанням. Навчальну дисципліну розроблено для одержання студентами теоретичних знань з пбуи систем комп'ютерного захисту та нчнню рботи з подібними системами, а також для формування в них навичок ефективного застосовування засвоєних знань і методів у розв’язанні прикладних задач експлуатації захищених систем. Представлено теоретичні основи машинного навчання, нейронних мереж, архітектури систем захисту, класифікація та огляд особливостей відомих продуктів для подібного роду систем, основи криптології та шифрування в каналах зв’язку, а також відповідні комп’ютерні алгоритми і засоби опрацювання даних.
Мета та цілі дисципліни	**Метою** вивчення дисципліни «Високорівневі системи комп'ютерного захисту» є набуття теоретичних знань і практичних навичок постановки та проектування систем захисту, побудовою архітектури систем захисту, програмуванням захищених систем. Вона присвячена розгляду стандартів, методів та засобів проектування, впровадження та підтримки захищених інформаційних систем. Як **ціль**, у курсі розглядаються сучасні підходи до забезпечення захисту інформаційних активів, приділяється певна увага процесам оцінки захищеності систем і технологій обробки інформації. Розглянуті складові комплексних систем захисту інформації. Надані певні відомості про методи протидії актуальним кіберзагрозам.
Література для вивчення дисцип-	**Основна література:** 1. Бурячок В. Л. Основи інформаційної та кібернетичної безпеки.

ліни	[Навчальний посібник]. / В. Л. Бурячок , Р. В. Киричок, П. М. Складанний – К. , 2018. – 320 с. 2. Сучасні інформаційні технології в кібербезпеці : монографія / А. С. Довбиш, В. К. Ободяк, І. В. Шелехов та ін. ; за ред. В. К. Ободяка, І. В. Шелехова. – Суми : Сумський державний університет, 2021. – 348 с. 3. https://www.st.com/resource/en/datasheet/dm00037051.pdf 4. Грайворонський М.В., Новіков О.М Безпека інформаційно-комунікаційних систем. – К.: Видавнича група BHV, 2009. – 608 с. 5. Криптологія у прикладах, тестах і задачах : навч. посіб./ Т. В. Бабенко, Г. М. Гулак, С. О. Сушко, Л. Я. Фомичова; М-во освіти і науки України, Держ. вищий навч. закл. “Нац. гірн. унт”.- Д.: НГУ, 2013. 6. Захист інформації в комп'ютерних системах та мережах : навч. посібник / С. Г. Семенов [та ін.] ; Нац. техн. ун-т "Харків. політехн. ін-т". – Харків : НТУ "ХПІ", 2014. – 251 с. 7. Кібербезпека: сучасні технології захисту. Навчальний посібник для вищих навчальних закладів. / Остапов С.Е., Євсеєв С.П., Король О.Г. – Львів: «Новий світ-2000», 2019. – 678 с. 8. Cyber Security Demand 2023: Skills to Learn URL: https://www.knowledgehut.com/blog/security/cyber-security-demand **Додаткова література:** 1.ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT). 2.Горпенюк А.Я., Зеляновський Ю.Є. Навчальний посібник для проектування ПЛІС Altera (FPGA) у середовищі Quartus® II. 3.IEEE 1364-2005 4.IEEE 1800-2012 5.IEEE Standard for SystemVerilog
Обсяг курсу	Сумарно 180 годин. Із них 32 години лекцій, 32 годин лабораторних робіт і 116 годин самостійної роботи
Очікувані результати навчання	Після завершення цього курсу студент буде: - знати основні методи комп’ютерного захисту та побудову систем захисту, основні теорії, моделі та алгоритми розроблення систем із різними ступенями захисту і опису архітектури цих систем, інформаційного пошуку та інтелектуального аналізу різних даних; - вміти аналізувати моделі для створення високорівневих систем захисту, працювати з відповідними програмними продуктами, застосовувати комп’ютерну техніку для вирішення задач, пов’язаних з захистом, розробляти та реалізувати відповідні алгоритми, писати прикладні програми та користуватися ними. Після вивчення курсу здобувачі набудуть таких компетентностей і програмних результатів: ЗК2. Здатність застосовувати знання у практичних ситуаціях. СК1. Усвідомлення теоретичних засад комп’ютерних наук. СК3. Здатність використовувати математичні методи для аналізу формалізованих моделей предметної області. СК11. Здатність ініціювати, планувати та реалізовувати процеси розробки інформаційних і комп’ютерних систем та програмного забезпечення, включно з його розробкою, аналізом, тестуванням, системною інтеграцією, впровадженням і супроводом. СК12. Здатність поєднувати програмні підходи з оптимальними апаратними рішеннями та базовими знаннями електроніки у створенні інтелектуальних, високорівневих вбудованих та спеціалізованих комп’ютерних систем.

	СК13. Здатність застосовувати методи і підходи штучного інтелекту, інтелектуального аналізу та науки про дані та підходів оптимізації до розв'язання конкретних проблем комп'ютерних наук. РН1. Мати спеціалізовані концептуальні знання, що включають сучасні наукові здобутки у сфері комп'ютерних наук і є основою для оригінального мислення та проведення досліджень, критичне осмислення проблем у сфері комп'ютерних наук та на межі галузей знань. РН3. Зрозуміло і недвозначно доносити власні знання, висновки та аргументацію у сфері комп'ютерних наук до фахівців і нефахівців, зокрема до осіб, які навчаються. РН4. Управляти робочими процесами у сфері інформаційних технологій, які є складними, непередбачуваними та потребують нових стратегічних підходів. РН11. Створювати нові алгоритми розв'язування задач у сфері комп'ютерних наук, оцінювати їх ефективність та обмеження на їх застосування. РН13. Оцінювати та забезпечувати якість інформаційних та комп'ютерних систем різного призначення. РН15. Виявляти потреби потенційних замовників щодо автоматизації обробки інформації. РН17. Виявляти та усувати проблемні ситуації в процесі експлуатації програмного забезпечення, формулювати завдання для його модифікації або реінжинірингу. РН18. Збирати, формалізувати, систематизувати і аналізувати потреби та вимоги до інформаційної або комп'ютерної системи, що розробляється, експлуатується чи супроводжується. РН19. Аналізувати сучасний стан і світові тенденції розвитку комп'ютерних наук та інформаційних технологій. РН20. Володіти методами та засобами штучного інтелекту, інженерії та аналізу даних, розпізнавання образів і адаптивного опрацювання інформації, аналізу та обробки природної мови, моделювання та оптимізації. РН21. Створювати нові системи даних, високорівневі вбудовані системи, спеціалізовані комп'ютерні системи та інтелектуальні системи із застосуванням базових знань апаратного і програмного забезпечення мікроконтролерів і мікрокомп'ютерів.
Ключові слова	Захищена система, архітектура системи, кібербезпека, кіберзахист, машинне навчання, біометрія, аналіз і синтез системи
Формат курсу	Очний
	Проведення лекцій, лабораторних робіт та консультації для поглибленого розуміння тем
Теми	Див. СХЕМА КУРСУ
Підсумковий контроль, форма	Залік вкінці семестру
Пререквізити	Для вивчення курсу студенти потребують базових знань у галузі 12 – Інформаційні технології, зокрема з дисциплін «Вища математика», «Дискретна математика», «Алгоритми та структури даних», «Чисельні методи», «Теорія ймовірності та математична статистика», «Об'єктно-орієнтоване програмування», «Бази даних».
Навчальні методи та техніки, які будуть використовуватися під час викладання курсу	Лекції, презентації, лабораторні роботи, індивідуальні практичні завдання, обговорення, дискусії.

Необхідне обладнання	Мультимедіа, платформи Microsoft Teams, Moodle і Zoom, комп'ютерне програмне забезпечення: Python з бібліотеками OpenCV, Tenzoflow і Matlotlib
Критерії оцінювання (окремо для кожного виду навчальної діяльності)	Оцінювання проводиться упродовж семестру та під час екзаменаційної сесії за 100-бальною шкалою. Бали нараховуються за такими видами робіт із таким співвідношенням: • 13 лабораторних або 2 індивідуальні практичні роботи: 40% оцінки; максимальна кількість балів: 13x3+1=40 (де 1 бал надається за якісне виконання усіх лабораторних) або 2x20=40. • 1 контрольний замір знань на лекціях: 10% оцінки; максимальна кількість балів 10. • залік: 50% оцінки; максимальна кількість балів 50. Загалом 100 балів. _____. **Контрольні заміри знань проводять у формі стандартних практичних завдань і теоретичних питань.** **Академічна доброчесність**: Очікується, що лабораторні та контрольні роботи студентів будуть їхніми оригінальними дослідженнями або 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 роботі сутдента є підставою для її незарахуванння викладачем, незалежно від масштабів плагіату або спроб обману. **Відвідування занять** є важливою складовою навчання. Очікується, що всі студенти відвідають усі лекції та лабораторні заняття курсу. Студенти мають інформувати викладача про неможливість відвідати заняття. Студенти зобов'язані дотримуватися всіх термінів, визначених для виконання 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 також заохочуються до використання іншої літератури та джерел, зокрема наукової літератури, яка відсутня серед обов'язкової та рекомендованої. **Політика виставлення балів.** Враховуються бали, набрані на поточному опитуванні, самостійній роботі та бали підсумкового контролю знань. Обов'язково враховуються присутність на заняттях та активність студента під час лабораторних занять; наголошується на неприпустимості пропусків або запізнень на заняття, користування мобільним телефоном, планшетом або іншими мобільними пристроями під час занять з метою, не пов'язаною з навчанням, списування та плагіату, несвоєчасного виконання поставлених завдань і т. ін. Жодні форми порушення академічної доброчесності не толеруються.
Питання до контрольних робіт	Перелік питань і завдань для проведення підсумкової оцінки знань усіх тем курсу до контрольних робіт розміщено на веб-сторінці https://e-learning.lnu.edu.ua/course/view.php?id=4878
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, самостійна робота, год.	Термін виконання

1, 2	**Вступ. Захист інформації. Кібербезпека. Атаки в кіберпросторі. Системи безпеки.** Забезпечення надійності програмного забезпечення. Шифрування по Шеннону. Програмна реалізація шифрування. Способи захисту для паперових носіїв інформації.	Лекція	2, 3, 7	Вступне заняття. Академічна доброчесність. Розв'язання типових задач на Python Функції на Python Розробити парсер на Python	1, 2 тиж. семестру
3, 4	Системи машинного навчання щодо побудови захищених систем Модель і метод машинного навчання для розпізнавання шкідливого програмного забезпечення в пристроях Інтернету речей Криптосистеми на основі логарифмічних підписів для постквантової криптографії. Проблеми управління ризиками інформаційної безпеки в автоматизованих системах	Лекція	2, 4, 7	Створити проект на django. Публічний сайт, інтерфейс адміністратора з можливістю голосування	3, 4 тиж. семестру
5, 6	**Теорія проектування паралельних спеціалізованих систем захисту.** Інформаційна безпека вебдодатків. Особливості управління інцидентами інформаційної безпеки	Лекція	1, 2, 8	ML без вчителя ML з вчителем Робота з бібліотекою_matlotlib. Візуалізація даних. Різні види візуалізації. Робота з бібліотекою OpenCV	5, 6 тиж. семестру
7, 8	**Процесори опрацювання сигналів та зображень** Процесори швидких ортогональних перетворень. Програмні та апаратні системи контролю і діагностики систем опрацювання сигналів	Лекція	1, 4, 8, 9	Захоплення відео-об'єктів. Проектування системи розпізнавання	7, 8 тиж. семестру
9, 10	**Теоретичні основи побудови та засоби практичної реалізації відмовостійких систем опрацювання сигналів та зображень.** Аналіз алгоритмів опрацювання сигналів та зображень стосовно забезпечених їх відмово стійкості. Розробка високопродуктивних обчислювальних структур опрацювання сигналів та зображень. Методи забезпечення гарантоздатності систем реального часу	Лекція	2, 4, 7	Розпізнавання обличчя. Програмування системи для розпізнавання обличчя	9, 10 тиж. семестру
11,12	**Процесори криптографічного захисту інформації** Розробка методів і засобів побудови пристроїв для формування цифрового підпису Методи та програми для побудови криптографічних систем з відкритим ключем	Лекція	1, 2, 90	Система розпізнавання на основі біометричних даних. Порівняння з шаблоном. Налаштування показників ERP та FAR, FRR	11, 12 тиж. семестру

	Протоколи захисту даних симетричними блоковими шифрами в локальних комп'ютерних мережах Принципи побудови систем захисту інформації, визначення стійкості до вторгнень, виявлення атак і доступу до інформації				
13, 14	**Ефективні методи опрацювання біометричних даних** Принципи побудови адаптивної біометричної системи Методи та засоби компресії біомедичних сигналів у реальному часі для дистанційного моніторингу	Лекція	1, 3, 4, 7, 9	Технології машинного навчання в системах захисту	13, 14 тиж. семестру
15, 16	**Автоматична система виділення та ідентифікації рухомих об'єктів в полі зору відеокамери** Розробка адаптивного інтерфейсу відеопроцесора Дослідження завадостійкості в системах опрацювання сигналів Підсистема визначення координат візуального об'єкта у просторі Модель автоматизованої системи опрацювання зображень відбитків пальців людини.	Лекція	1, 7, 8, 9	Метод k-means. Кластеризація даних. Прогнозування даних на основі нейронних мереж.	15, 16 тиж. семестру