

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 від 31.08, 2022 р.)

Завідувач кафедри:


_____ Ігор ОЛЕНИЧ

Силабус з навчальної дисципліни
“Інформаційна безпека програм та даних”,
що викладається в межах ОПП
“Інженерія програмного забезпечення”
першого (бакалаврського) рівня вищої освіти для здобувачів з
спеціальності 121 – Інженерія програмного забезпечення

Львів 2022 р.

Назва дисципліни	Інформаційна безпека програм та даних
Адреса викладання дисципліни	Корпус факультету електроніки та комп'ютерних технологій, Львівський національний університет імені Івана Франка, вул. Драгоманова 50, м. Львів, 79005, вул. Ген. Тарнавського 107, м. Львів, 79011
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 121 – Інженерія програмного забезпечення
Викладачі дисципліни	Монастирський Л.С., доктор фізико-математичних наук, професор, професор кафедри радіоелектронних і комп'ютерних систем Павлик М.Р., канд. фіз.-мат. наук, асистент кафедри радіоелектронних і комп'ютерних систем
Контактна інформація викладачів	lyubomyr.monastyrskyy@lnu.edu.ua , https://electronics.lnu.edu.ua/employee/monastyrskyy-lyubomyr-stepanovych , mykhailo.pavyk@lnu.edu.ua , https://electronics.lnu.edu.ua/employee/pavlyk-m-r
Консультації з питань навчання по дисципліні відбуваються	Консультації в день проведення лекцій/лабораторних занять (за попередньою домовленістю): ауд. 101, корпус факультету електроніки та комп'ютерних технологій, вул. Драгоманова 50, м. Львів
Сторінка курсу	https://e-learning.lnu.edu.ua/course/view.php?id=5344
Коротка анотація дисципліни	Дисципліна “Інформаційна безпека програм та даних” є нормативною дисципліною з спеціальності 121 – Інженерія програмного забезпечення для освітньої програми “Інформаційні системи та технології”, яка викладається в 8-му семестрі в обсязі 3,5 кредитів (за Європейською Кредитно-Трансферною Системою ECTS).
Інформація про дисципліну	Курс розроблено для ознайомлення студентів з основними стандартами, методами та засобами захисту програм та даних.
Мета та цілі дисципліни	Метою вивчення дисципліни є формування у студентів знань про сучасні стандарти, підходи, методи та засоби захисту програм та даних. Програма дисципліни орієнтована на глибоке та ґрунтовне засвоєння студентами основних понять щодо програмно-апаратного захисту інформації, ідентифікації та аутентифікації користувачів комп'ютерних систем, засобів і методів контролю доступу до програм, методів та засобів криптографічного захисту інформації, написання безпечного коду.
Література для вивчення дисципліни	1. David Kim, Michael G. Solomon. Fundamentals of Information Systems Security, 4th Edition. Jones & Bartlett Learning, 2021. - 543p. 2. Brij B. Gupta, Dharma P. Agrawal, Haoxiang Wang. Computer and Cyber Security. Principles, Algorithm, Applications, and -Perspectives. CRC Press, 2019. - 665p. 3. Інформаційна безпека. За заг. ред. д-ра техн. наук, проф. Ю.Я. Бобала та

	<p>д-ра техн. наук, доц. І.В. Горбатого / Навчальний посібник / Ю.Я. Бобало, І.В. Горбатий, М.Д. Кіселичник, А.П. Бондарєв, С.С. Войтусік, А.Я. Горпенюк, О.А. Немкова, І.М. Журавель, Б.М. Березюк, Є.І. Яковенко, В.І. Отенко, І.Я. Тишик. Львів: Видавництво Львівської політехніки, 2019. 580с.</p> <p>4. Laurent Gil, Allan Liska. Security with AI and Machine Learning. O'Reilly Media, 2019. - 63p.</p> <p>5. Кузнецов О. О. Захист інформації в інформаційних системах : навч. посіб. Х. : ХНЕУ, 2018. – 510 с.</p> <p>6. William Stallings, Lawrie Brown. Computer Security. Principles and Practice, 4th Edition. Pearson Education, 2018. - 1175p.</p> <p>7. John R. Vacca. Computer and Information Security Handbook, 3rd Edition. Morgan Kaufmann publishers, 2017. - 1239p.</p> <p>8. Darren Death. Information Security Handbook. Packt Publishing, 2017. - 308p.</p> <p>9. Сенів М.М., Яковина В.С. Безпека програм та даних / М.М. Сенів, В.С. Яковина. – Львів: Львівська політехніка, 2015. – 256 с.</p>
Обсяг курсу	Загальний обсяг: 120 годин. Аудиторних занять: 64 год., з них 32 год. лекційних та 32 годин лабораторних робіт. Самостійної роботи: 56 год.
Очікувані результати навчання	<p>У результаті вивчення даного курсу студент буде:</p> <p>знати: основні поняття, визначення і проблеми курсу; основні методи шифрування даних; типи шкідливих програм, принципи їх роботи; основи інформаційної безпеки баз даних, інформаційних мереж, операційних систем;</p> <p>вміти: застосовувати алгоритми шифрування даних; організувати контроль доступу до інформаційних систем; писати безпечний програмний код; Після вивчення даного курсу «Інформаційна безпека програм та даних» здобувачі набудуть таких Загальних та Фахових компетентностей та Програмних результатів навчання:</p> <p>ЗК1. Здатність до абстрактного мислення, аналізу та синтезу. ЗК2. Здатність застосовувати знання у практичних ситуаціях. ЗК4. Здатність спілкуватися іноземною мовою як усно, так і письмово. ЗК8. Здатність діяти на основі етичних міркувань. ФК18. Здатність аналізувати, вибирати і застосовувати методи і засоби для забезпечення інформаційної безпеки (в тому числі кібербезпеки). ФК20. Здатність застосовувати фундаментальні і міждисциплінарні знання для успішного розв'язання завдань інженерії програмного забезпечення. ФК27. Здатність використовувати для розробки програмного забезпечення перспективні засоби та технології, зокрема, науки про дані, штучного інтелекту, IoT, вбудованих систем тощо.</p> <p>ПРН4. Знати і застосовувати професійні стандарти і інші нормативно-правові документи в галузі інженерії програмного забезпечення. ПРН7. Знати і застосовувати на практиці фундаментальні концепції, парадигми і основні принципи функціонування мовних, інструментальних і обчислювальних засобів інженерії програмного забезпечення. ПРН21. Знати, аналізувати, вибирати, кваліфіковано застосовувати засоби забезпечення інформаційної безпеки (в тому числі кібербезпеки) і цілісності даних відповідно до розв'язуваних прикладних завдань та створюваних програмних систем.</p>

Ключові слова	Інформаційна безпека, криптографічні методи, протоколи та стандарти інформаційної безпеки, шкідливе програмне забезпечення.			
Формат курсу	Очний			
Теми	Тема 1. Інформаційна безпека. Основні концепції, принципи, стратегії. Тема 2. Криптографічні методи. Тема 3. Симетричне шифрування та конфіденційність повідомлень. Тема 4. Шифрування з відкритим ключем і автентифікація повідомлень. Тема 5. Основні методи автентифікації користувача. Тема 6. Організація контролю доступу до інформаційних систем. Тема 7. Інформаційна безпека баз даних. Тема 8. Шкідливе програмне забезпечення. Тема 9. Атаки типу «відмова в обслуговуванні». Тема 10. Брандмауери та системи запобігання вторгненням. Тема 11. Безпека програмного забезпечення та написання безпечного програмного коду. Тема 12. Організація інформаційної безпеки в операційних системах. Тема 13. Інформаційна безпека мережевих хмар та інтернету речей. Тема 14. Протоколи та стандарти безпеки в Інтернеті. Тема 15. Безпека бездротових мереж. Тема 16. Забезпечення інформаційної безпеки за допомогою штучного інтелекту і машинного навчання.			
Підсумковий контроль, форма	Екзамен у кінці семестру			
Пререквізити	Для вивчення даного курсу студентам потрібні базові знання з курсів: <ul style="list-style-type: none"> - алгоритми і структури даних; - об'єктно-орієнтоване програмування; - операційні системи, системне програмування; - комп'ютерні інформаційні мережі та системи; - бази даних; 			
Навчальні методи та техніки, які будуть використовуватися під час викладання курсу	Інформаційні методи (лекція, бесіда, ілюстрація, демонстрація); дедуктивні методи на основі узагальнень; евристичні методи (проблемна лекція); інтерактивні методи (дискусія).			
Необхідне обладнання	Комп'ютер із необхідним програмним забезпеченням, доступ до Internet мережі.			
Критерії оцінювання (окремо для кожного виду навчальної діяльності)	Оцінювання проводиться за 100-бальною шкалою. Бали нараховуються за наступним співвідношенням: <ul style="list-style-type: none"> • Змістовий модуль 1: 25% семестрової оцінки за виконані лабораторні роботи. • Змістовий модуль 2: 25% семестрової оцінки за виконані лабораторні роботи. • екзамен: 50% семестрової оцінки, максимальна кількість балів 50. Підсумкова максимальна кількість балів 100. <table border="1" style="width: 100%; margin-top: 5px;"> <tr> <td style="text-align: center;">Поточне тестування та самостійна робота</td> <td style="text-align: center;">Підсумк</td> <td style="text-align: center;">Сума</td> </tr> </table>	Поточне тестування та самостійна робота	Підсумк	Сума
Поточне тестування та самостійна робота	Підсумк	Сума		

Змістовий модуль 1								Змістовий модуль 2								овий тест (екзамени)	100
T1	T2	T3	T4	T5	T6	T7	T8	T9	T10	T11	T12	T13	T14	T15	T16		
2	2	3	3	3	4	4	4	4	3	3	3	3	3	3	3	50	100
<p>Академічна доброчесність: Очікується, що роботи студентів будуть оригінальними дослідженнями чи міркуваннями. Списування та втручання в роботу інших студентів становлять, але не обмежують, приклади можливої академічної недоброчесності. Виявлення ознак академічної недоброчесності в написанні завдань є підставою для її незарахування викладачем, незалежно від масштабів плагіату чи обману.</p> <p>Відвідання занять 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 робіт, передбачених курсом.</p> <p>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.</p> <p>Політика виставлення балів. Враховуються бали, набрані при поточному контролі та бали підсумкового тестування. При цьому обов'язково враховуються присутність на заняттях та активність студента під час практичного 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>																	
Питання до заліку чи екзамену.		Перелік питань на екзамен розміщений на веб-сторінці курсу.															
Опитування		Анкету-оцінку з метою оцінювання якості курсу буде надано по завершенню курсу.															

**Схема курсу “Інформаційна безпека програм та даних”
для студентів спеціальності 121 – Інженерія програмного забезпечення**

Тиж.	Тема, план, короткі тези	Форма діяльності (заняття)* *лекція, самостійна, дискусія, групова робота)	Література.** * Ресурси в інтернеті	Завдання, год	Термін виконання
1	Інформаційна безпека. Основні концепції, принципи, стратегії.	Лекція	[1], [2], [3], [6], Сайт курсу	2	кінець поточного тижня
1	Основні бібліотеки для шифрування даних та написання етичних хакерських скриптів.	Лабораторна робота	Сайт курсу	2	кінець поточного тижня
2	Криптографічні методи.	Лекція	[1], [2], [3], [6] Сайт курсу	2	кінець поточного тижня
2	Лаб.1. Шифрування та дешифрування даних.	Лабораторна робота	Сайт курсу	2	кінець поточного тижня
3	Симетричне шифрування та конфіденційність повідомлень.	Лекція	[1], [2], [6], Сайт курсу	2	кінець поточного тижня
3	Лаб.2. Шифрування даних за допомогою методів симетричного шифрування.	Лабораторна робота	Сайт курсу	2	кінець поточного тижня
4	Шифрування з відкритим ключем і автентифікація повідомлень.	Лекція	[1], [2], [6], Сайт курсу	2	кінець поточного тижня
4	Лаб.3. Шифрування даних за допомогою методів шифрування з відкритим ключем.	Лабораторна робота	Сайт курсу	2	кінець поточного тижня
5	Основні методи автентифікації користувача.	Лекція	[1], [2], [6], Сайт курсу	2	кінець поточного тижня
5	Лаб.4. Розробка програми генератора паролів.	Лабораторна робота	Сайт курсу	2	кінець поточного тижня
6	Організація контролю доступу до інформаційних систем.	Лекція	[1], [2], [3], [6] Сайт курсу	2	кінець поточного тижня
6	Лаб.5. Отримання та розшифрування збережених паролів браузера Google Chrome.	Лабораторна робота	Сайт курсу	2	кінець поточного тижня
7	Інформаційна безпека баз даних.	Лекція	[1], [2], [5], [6], Сайт курсу	2	кінець поточного тижня
7	Лаб. 6. Виявлення вразливості SQL-ін'єкцій.	Лабораторна робота	Сайт курсу	2	кінець поточного тижня
8	Шкідливе програмне забезпечення.	Лекція	[1], [2], [6], [7], Сайт курсу	2	кінець поточного тижня
8	Підсумкове заняття ЗМ 1	Лабораторна робота	Сайт курсу	2	кінець поточного тижня

9	Атаки типу «відмова в обслуговуванні».	Лекція	[1], [2], [3], [6], Сайт курсу	2	Кінець поточного тижня
9	Лаб.7. Розробка шкідливої програми - вимагача, яка використовує симетричне шифрування.	Лабораторна робота	Сайт курсу	2	кінець поточного тижня
10	Брандмауери та системи запобігання вторгненням.	Лекція	[1], [2], [6],[8], Сайт курсу	2	кінець поточного тижня
10	Лаб.8. Створення сканера портів.	Лабораторна робота	Сайт курсу	2	кінець поточного тижня
11	Безпека програмного забезпечення та написання безпечного програмного коду.	Лекція	[1], [2], [6], Сайт курсу	2	кінець поточного тижня
11	Лаб.9. Написання безпечного програмного коду.	Лабораторна робота	Сайт курсу	2	кінець поточного тижня
12	Організація інформаційної безпеки в операційних системах.	Лекція	[1], [2], [6], [8], Сайт курсу	2	кінець поточного тижня
12	Лаб.10. Виконання команд командного інтерфейсу операційної системи на віддаленому комп'ютері.	Лабораторна робота	Сайт курсу	2	кінець поточного тижня
13	Інформаційна безпека мережевих хмар та інтернету речей.	Лекція	[1], [2], [6], [8], Сайт курсу	2	кінець поточного тижня
13	Лаб.11. Приховування даних у файлах зображень.	Лабораторна робота	Сайт курсу	2	кінець поточного тижня
14	Протоколи та стандарти безпеки в Інтернеті.	Лекція	[1], [2], [6], [7], Сайт курсу	2	кінець поточного тижня
14	Лаб.12. Використання різних алгоритмів хешування, таких як SHA-2, SHA-3.	Лабораторна робота	Сайт курсу	2	кінець поточного тижня
15	Безпека бездротових мереж.	Лекція	[1], [2], [5], [6] Сайт курсу	2	кінець поточного тижня
15	Підсумкове заняття ЗМ 2	Лабораторна робота	Сайт курсу	2	кінець поточного тижня
16	Забезпечення інформаційної безпеки за допомогою штучного інтелекту і машинного навчання.	Лекція	[4] Сайт курсу	2	кінець поточного тижня
16	Підсумкове заняття	Лабораторна робота	Сайт курсу	2	кінець поточного тижня