

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ імені ІВАНА ФРАНКА

Кафедра (циклова комісія) \_\_\_\_\_ радіоелектронних і комп'ютерних систем \_\_\_\_\_

**“ЗАТВЕРДЖУЮ”**

Декан факультету \_\_\_\_\_

доц. Юрій ФУРГАЛА

2019 року

**РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ**

\_\_\_\_\_ Інформаційна безпека програм та даних \_\_\_\_\_

(шифр і назва навчальної дисципліни)

спеціальність \_\_\_\_\_ 122 – Комп'ютерні науки \_\_\_\_\_

(шифр і назва спеціальності)

спеціалізація \_\_\_\_\_

(назва спеціалізації)

факультет \_\_\_\_\_ електроніки та комп'ютерних технологій \_\_\_\_\_

(назва інституту, факультету, відділення)

Робоча програма \_\_\_\_\_ “ Інформація безпека програм та даних ”  
\_\_\_\_\_ для студентів

(назва навчальної дисципліни)

галузі знань \_\_\_\_\_ “12 Інформаційні технології ”

за спеціальністю \_\_\_\_\_ “122 Комп’ютерні науки ”

Розробники: \_\_\_\_\_ Любомир Монастирський (професор кафедри радіоелектронних  
і комп’ютерних систем)

(вказати авторів, їхні посади, наукові ступені та вчені звання)

Робочу програму схвалено на засіданні кафедри (циклової комісії) \_\_\_\_\_  
\_\_\_\_\_ радіоелектронних і комп’ютерних систем

Протокол від “ 31 ” \_\_\_\_\_ 08 \_\_\_\_\_ 2019 року № 1/23

Завідувач кафедри \_\_\_\_\_ радіоелектронних і комп’ютерних систем

\_\_\_\_\_ (Ігор Оленич)  
(підпис) (прізвище та ініціали)

Ухвалено Вченою радою \_\_\_\_\_ факультету електроніки та комп’ютерних технологій

Протокол від “ 31 ” \_\_\_\_\_ 08 \_\_\_\_\_ 2019 року № 28/22

### 1. Опис навчальної дисципліни

Найменування показників	Галузь знань, освітньо-кваліфікаційний рівень	Характеристика навчальної дисципліни	
		денна форма навчання	заочна форма навчання
Кількість кредитів <b>3,5</b>	Галузь знань <u>12 Інформаційні технології</u> (шифр і назва)	Нормативна	
Модулів – <i>немає</i>	Спеціальність: <u>121 Інженерія програмного забезпечення</u>	Рік підготовки	
Змістових модулів – <b>2</b>		<b>4-й</b>	
Індивідуальне науково-дослідне завдання <u>немає</u> (назва)		Семестр	
Загальна кількість годин – <b>120</b>		<b>8-й</b>	
Тижневих годин для денної форми навчання: аудиторних – <b>4</b> самостійної роботи студента – <b>3,5</b>	Освітній ступінь <u>бакалавр</u>	Лекції	
		<b>32 год.</b>	
		Практичні, семінарські <i>немає</i>	
		Лабораторні	
		<b>32 год.</b>	
		Самостійна робота	
		<b>56 год.</b>	
		Індивідуальні завдання: <i>немає</i>	
		Вид контролю: <i>екзамен</i>	

Примітка.

Співвідношення кількості годин аудиторних занять до самостійної і індивідуальної роботи становить

для денної форми навчання – 1,14

для заочної форми навчання – немає

### 2. Мета та завдання навчальної дисципліни

**Мета:** формування у студентів знань про сучасні стандарти, підходи, методи та засоби захисту програм та даних.

**Цілі:** забезпечити 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.

У результаті вивчення навчальної дисципліни студент повинен

**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;

**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 набувають таких Загальних та Фахових компетентностей та Програмних результатів навчання:

K01. Здатність до абстрактного мислення, аналізу та синтезу.

K02. Здатність застосовувати знання у практичних ситуаціях.

K03. Здатність спілкуватися державною мовою як усно, так і письмово.

K04. Здатність спілкуватися іноземною мовою мовою як усно, так і письмово.

K08. Здатність діяти на основі етичних міркувань.

K20. Здатність застосовувати фундаментальні і міждисциплінарні знання для успішного розв'язання завдань інженерії програмного забезпечення.

K26. Здатність до алгоритмічного та логічного мислення.

K27. Здатність здійснювати процес інтеграції системи, застосовувати стандарти і процедури управління змінами для підтримки цілісності, загальної функціональності і надійності 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.

ПРН23: Вміти документувати та презентувати результати розробки програмного забезпечення.

### **3. Програма навчальної дисципліни**

**Змістовий модуль 1. Інформаційна безпека. Криптографічні методи. Контроль доступу до інформаційних систем.**

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.

**Змістовий модуль 2. Безпека у інформаційних мережах. Використання штучного інтелекту для забезпечення інформаційної безпеки.**

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.

#### 4. Структура навчальної дисципліни

Назви змістових модулів і тем	Кількість годин											
	денна форма						заочна форма					
	усього	у тому числі					усього	у тому числі				
		л	п	лаб	інд	с. р.		л	п	лаб	інд	с. р.
1	2	3	4	5	6	7	8	9	10	11	12	13
<b>Змістовий модуль 1. Інформаційна безпека. Криптографічні методи. Контроль доступу до інформаційних систем.</b>												
Тема 1. Інформаційна безпека. Основні концепції, принципи, стратегії.		2		2		3,5						
Тема 2. Криптографічні методи.		2		2		3,5						
Тема 3. Симетричне шифрування та конфіденційність повідомлень.		2		2		3,5						
Тема 4. Шифрування з відкритим ключем і автентифікація повідомлень.		2		2		3,5						
Тема 5. Основні методи автентифікації користувача.		2		2		3,5						
Тема 6. Організація контролю доступу до інформаційних систем.		2		2		3,5						
Тема 7. Інформаційна безпека баз даних.		2		2		3,5						
Тема 8. Шкідливе програмне забезпечення.		2		2		3,5						
<b>Разом за змістовим модулем 1</b>		<b>16</b>		<b>16</b>		<b>28</b>						
<b>Змістовий модуль 2. Безпека у інформаційних мережах. Використання штучного інтелекту для забезпечення інформаційної безпеки.</b>												
Тема 9. Атаки типу «відмова в обслуговуванні».		2		2		3,5						
Тема 10. Брандмауери та системи запобігання вторгненням.		2		2		3,5						
Тема 11. Безпека програмного		2		2		3,5						

забезпечення та написання безпечного програмного коду.												
Тема 12. Організація інформаційної безпеки в операційних системах.		2		2		3,5						
Тема 13. Інформаційна безпека мережевих хмар та інтернету речей.		2		2		3,5						
Тема 14. Протоколи та стандарти безпеки в Інтернеті.		2		2		3,5						
Тема 15. Безпека бездротових мереж.		2		2		3,5						
Тема 16. Забезпечення інформаційної безпеки за допомогою штучного інтелекту і машинного навчання.		2		2		3,5						
Разом за змістовим модулем 2		<b>16</b>		<b>16</b>		<b>28</b>						
<b>Усього годин</b>		<b>32</b>		<b>32</b>		<b>56</b>						

### 5. Теми семінарських занять

### 6. Теми практичних занять

### 7. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1	<i>Основні бібліотеки для шифрування даних та написання етичних хакерських скриптів.</i>	2
2	<i>Лаб.1. Шифрування та дешифрування даних.</i>	2
3	<i>Лаб.2. Шифрування даних за допомогою методів симетричного шифрування.</i>	2
4	<i>Лаб.3. Шифрування даних за допомогою методів шифрування з відкритим ключем.</i>	2
5	<i>Лаб.4. Розробка програми генератора паролів.</i>	2
6	<i>Лаб.5. Отримання та розшифрування збережених паролів браузера Google Chrome.</i>	2
7	<i>Лаб. 6. Виявлення вразливості SQL-ін'єкцій.</i>	2
8	<i>Підсумкове заняття ЗМ 1</i>	2
9	<i>Лаб.7. Розробка шкідливої програми - вимагача, яка використовує симетричне шифрування.</i>	2
10	<i>Лаб.8. Створення сканера портів.</i>	2
11	<i>Лаб.9. Написання безпечної програмного коду.</i>	2
12	<i>Лаб.10. Виконання команд командного інтерфейсу операційної системи на віддаленому комп'ютері.</i>	2
13	<i>Лаб.11. Приховування даних у файлах зображень.</i>	2
14	<i>Лаб.12. Використання різних алгоритмів хешування, таких як SHA-2, SHA-3.</i>	2
15	<i>Підсумкове заняття ЗМ 2</i>	2
16	<i>Підсумкове заняття</i>	2
	<b>Разом</b>	<b>32</b>



## 8. Самостійна робота

№ з/п	Назва теми	Кількість годин
1	<i>Основні бібліотеки для шифрування даних та написання етичних хакерських скриптів.</i>	3,5
2	<i>Основні криптографічні методи.</i>	3,5
3	<i>Симетричне шифрування та конфіденційність повідомлень.</i>	3,5
4	<i>Шифрування з відкритим ключем і автентифікація повідомлень.</i>	3,5
5	<i>Основні методи автентифікації користувача.</i>	3,5
6	<i>Організація контролю доступу до інформаційних систем.</i>	3,5
7	<i>Інформаційна безпека баз даних.</i>	3,5
8	<i>Шкідливе програмне забезпечення.</i>	3,5
9	<i>Атаки типу «відмова в обслуговуванні».</i>	3,5
10	<i>Брандмауери та системи запобігання вторгненням.</i>	3,5
11	<i>Безпека програмного забезпечення та написання безпечного програмного коду.</i>	3,5
12	<i>Організація інформаційної безпеки в операційних системах.</i>	3,5
13	<i>Інформаційна безпека мережевих хмар та інтернету речей.</i>	3,5
14	<i>Протоколи та стандарти безпеки в Інтернеті.</i>	3,5
15	<i>Безпека бездротових мереж.</i>	3,5
16	<i>Забезпечення інформаційної безпеки за допомогою штучного інтелекту і машинного навчання.</i>	3,5
	<b>Разом</b>	<b>56</b>

## 9. Індивідуальні завдання

### 10. Методи навчання

Інформаційні методи (лекція, бесіда, ілюстрація, демонстрація); дедуктивні методи на основі узагальнень; евристичні методи (проблемна лекція); інтерактивні методи (дискусія).

### 11. Методи контролю

Поточний контроль здійснюється шляхом проведення усного опитування та написання письмових звітів по виконаних лабораторних роботах. У кінці курсу проводиться екзамен.

## 12. Розподіл балів, які отримують студенти

Поточне тестування та самостійна робота																Підсумковий тест (екзамен)	Сума
Змістовий модуль 1								Змістовий модуль 2								50	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		

T1, T2 ... T12 – теми змістових модулів.

### Шкала оцінювання: національна та ЄКТС

Оцінка ЄКТС	Сума балів за всі види навчальної діяльності	Оцінка за національною шкалою	
		для екзамену, курсового проекту (роботи), практики	для заліку
A	90 – 100	відмінно	зараховано
B	81-89	добре	
C	71-80		
D	61-70		
E	51-60	задовільно	
FX	21-50	незадовільно з можливістю повторного складання	не зараховано з можливістю повторного складання
F	0-20	незадовільно з обов'язковим повторним вивченням дисципліни	не зараховано з обов'язковим повторним вивченням дисципліни

\* кількість балів для оцінок «незадовільно» (FX і F) визначається Вченими радами факультетів (педагогічними радами коледжів).

## 13. Методичне забезпечення

## 14. Рекомендована література

### Основна

- 1) William Stallings, Lawrie Brown. Computer Security. Principles and Practice, 4th Edition. Pearson Education, 2018. - 1175p.
- 2) Laurent Gil, Allan Liska. Security with AI and Machine Learning. O'Reilly Media, 2019. - 63p.

### Допоміжна

- 1) David Kim, Michael G. Solomon. Fundamentals of Information Systems Security, 4th Edition. Jones & Bartlett Learning, 2021. - 543p.
- 2) Brij V. 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 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.
- 4) Кузнецов О. О. Захист інформації в інформаційних системах : навч. посіб. Х. : ХНЕУ, 2018. – 510 с.
- 5) John R. Vacca. Computer and Information Security Handbook, 3rd Edition. Morgan Kaufmann publishers, 2017. - 1239p.
- 6) Darren Death. Information Security Handbook. Packt Publishing, 2017. - 308p.
- 7) Сенів М.М., Яковина В.С. Безпека програм та даних / М.М. Сенів, В.С. Яковина. – Львів: Львівська політехніка, 2015. – 256 с.

## 15. Інформаційні ресурси

1. Internet – джерела.
2. Наукова бібліотека Львівського національного університету імені Івана Франка (<https://www.lnulibrary.lviv.ua/to-users-2/paid-services/internet/> ).
3. Львівська національна наукова бібліотека України імені Василя Стефаника (<https://www.lsl.lviv.ua/index.php/uk/elektronni-resursy1/> ).