Форма № Н - 3.04

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)

2019

Робоча програма “ Інформаціна 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

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, освітньо-кваліфікаційний рівень</td><td colspan="2">Характеристика навчальної дисципліни</td></tr>
<tr><td>денна форма навчання</td><td>заочна форма навчання</td></tr>
<tr><td>Кількість кредитів
3,5</td><td>Галузь знань

<u>12 Інформаційні технології</u>
(шифр і назва)</td><td colspan="2">Нормативна</td></tr>
<tr><td>Модулів – немає</td><td rowspan="4">Спеціальність:

<u>121 Інженерія програмного забезпечення</u></td><td colspan="2">Рік підготовки</td></tr>
<tr><td>Змістових модулів – 2</td><td>4-й</td><td></td></tr>
<tr><td>Індивідуальне науково-дослідне завдання <u>немає</u>
(назва)</td><td colspan="2">Семестр</td></tr>
<tr><td>Загальна кількість годин – 120</td><td>8-й</td><td></td></tr>
<tr><td rowspan="13">Тижневих годин для денної форми навчання:
аудиторних – 4
самостійної роботи студента – 3,5</td><td rowspan="13">Освітній ступінь
<u>бакалавр</u></td><td colspan="2">Лекції</td></tr>
<tr><td>32 год.</td><td></td></tr>
<tr><td colspan="2">Практичні, семінарські</td></tr>
<tr><td>немає</td><td></td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td>32 год.</td><td></td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td>56 год.</td><td></td></tr>
<tr><td colspan="2">Індивідуальні завдання:</td></tr>
<tr><td>немає</td><td></td></tr>
<tr><td colspan="2">Вид контролю:</td></tr>
<tr><td>екзамен</td><td></td></tr>
</table>

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; організовувати 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:

К01. Здатність до абстрактного мислення, аналізу та синтезу.
К02. Здатність застосовувати знання у практичних ситуаціях.
К03. Здатність спілкуватися державною мовою як усно, так і письмово.
К04. Здатність спілкуватися іноземною мовою мовою як усно, так і письмово.
К08. Здатність діяти на основі етичних міркувань.
К20. Здатність застосовувати фундаментальні і міждисциплінарні знання для успішного розв’язання завдань інженерії програмного забезпечення.
К26. Здатність до алгоритмічного та логічного мислення.
К27. 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
Змістовий модуль 1. І***нформаційна безпека. Криптографічні методи. Контроль доступу до інформаційних систем.***												
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						
Разом за змістовим модулем 1		**16**		**16**		**28**						
Змістовий модуль 2. ***Безпека у інформаційних мережах. Використання штучного інтелекту для забезпечення інформаційної безпеки.***												
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		**16**		**16**		**28**						
Усього годин		**32**		**32**		**56**						

5. Теми семінарських занять

6. Теми практичних занять

7. Теми лабораторних занять

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

8. Самостійна робота

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

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
Т1	Т2	Т3	Т4	Т5	Т6	Т7	Т8	Т9	т10	Т11	Т12	Т13	Т14	Т15	Т16		
2	2	3	3	3	4	4	4	4	3	3	3	3	3	3	3		

Т1, Т2 ... Т12 – 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	задовільно	
E	51-60		
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 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 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. Нємкова, 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/).