Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем та програмної інженерії
/назва факультету/

Кафедра кібербезпеки
/назва кафедри/

ЗАТВЕРДЖУЮ
Декан факультету
_____ Ігор БАРАН
«02» 09 2024 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«Захист інформації в інформаційно-комунікаційних системах»
/назва дисципліни/

галузь знань 12 Інформаційні технології
/шифр і назва галузі знань/

рівень вищої освіти перший (бакалаврський)
/назва/

спеціальність 123 - Комп'ютерна інженерія
/шифр і назва/

освітня програма Комп'ютерна інженерія
/назва/

спеціалізація _____
/назва/

вид дисципліни обов'язкова
/обов'язкова / вибіркова/

Тернопіль - 2024 рік

Робоча програма з навчальної дисципліни Захист інформації в інформаційно-комунікаційних системах
/назва дисципліни/

для студентів факультету комп'ютерно-інформаційних систем і програмної
/назва факультету(ів)/
інженерії_____

Розробник:

Асистент каф. Кібербезпеки _____ / Олександр МАКСИМЧУК /
/посада, науковий ступінь та вчене звання/ /підпис/ /ініціали та прізвище/

Робоча програма розглянута та схвалена
на засіданні кафедри _____Кібербезпеки_____
/назва/
Протокол від «__29__» ___серпня_____ 2024 року № _1_
Завідувач кафедри _Кібербезпеки_____ / __Наталія ЗАГОРОДНА___/
/підпис/ /ініціали та прізвище/

Робоча програма розглянута та схвалена НМК
факультету ____ комп'ютерно-інформаційних систем і програмної інженерії_
Протокол від «__02__» ___вересня_____2024 року № 1
Секретар НМК _____ / _____Богдана МЛИНКО_____ /
/підпис/ /ініціали та прізвище/

Робоча програма погоджена:

Спеціальність _____123 «Комп'ютерна інженерія» _____
/шифр і назва/

освітня програма _____123 «Комп'ютерна інженерія» _____
/назва/

Завідувач випускової кафедри _____ /__Галина ОСУХІВСЬКА__ /
/підпис/ /ініціали та прізвище/

Гарант освітньої програми _____ / ___Андрій ПАЛАМАР____ /
/підпис/ /ініціали та прізвище/

1. Структура навчальної дисципліни

Показник	Всього годин	
	Денна форма навчання (ДФН)	Заочна (дистанційна) форма навчання (ЗФН)
Кількість кредитів/год	4,5/135	4,5/135
Аудиторні заняття, год.	64	16
Самостійна робота, год.	71	119
Аудиторні заняття:		
– лекції, год.	32	8
– лабораторні заняття, год.	32	8
– практичні заняття, год.	–	–
– семінарські заняття, год.	–	–
Самостійна робота:		
опрацювання лекційного матеріалу	19	51
підготовка до лабораторних (практичних семінарських) занять, год.	16	32
опрацювання окремих розділів програми, які не виносяться на лекції, год.	–	–
виконання контрольних завдання, год.	–	–
виконання індивідуальних завдань, год.	–	–
виконання курсових проектів (робіт), год.	–	–
підготовка та складання заліків, екзаменів, контрольних робіт, рефератів, есе, тестування, год.	36	36
Екзамен	–	–
Залік	З	З

Частка годин самостійної роботи студента:
денна форма навчання – 53 %;
заочна (дистанційна) форма навчання – 88 %.

2. Мета та завдання навчальної дисципліни

2.1. Мета вивчення навчальної дисципліни

Метою викладання навчальної дисципліни «Захист інформації в інформаційно-комунікаційних системах» є формування у студентів теоретичних знань та практичних навичок щодо оцінки можливих небезпек, ступеня захищеності та ризику втрат інформації в інформаційно-комунікаційних системах (ІКС), уміння вирішувати задачі аналізу середовищ функціонування програмних та програмно-апаратних комплексів в ІКС, формування політики безпеки інформації в ІКС, застосовувати нормативно-правові, організаційні та технічні процедури підготовки до впровадження комплексних систем захисту інформації.

2.2. Завдання навчальної дисципліни

За результатами вивчення дисципліни студент повинен продемонструвати такі програмні результати навчання (ПРН) згідно освітньої програми:

ПР3. Знати новітні технології в галузі комп'ютерної інженерії.

ПР6. Вміти застосовувати знання для ідентифікації, формулювання і розв'язування технічних задач спеціальності, використовуючи методи, що є найбільш придатними для досягнення поставлених цілей.

ПР9. Вміти застосовувати знання технічних характеристик, конструктивних особливостей, призначення і правил експлуатації програмно-технічних засобів комп'ютерних систем та мереж для вирішення технічних задач спеціальності.

ПР11. Вміти здійснювати пошук інформації в різних джерелах для розв'язання задач комп'ютерної інженерії.

ПР20. Усвідомлювати необхідність навчання впродовж усього життя з метою поглиблення набутих та здобуття нових фахових знань, удосконалення креативного мислення.

ПР21. Якісно виконувати роботу та досягати поставленої мети з дотриманням вимог професійної етики.

Вивчення навчальної дисципліни передбачає формування та розвиток у студентів компетентностей:

загальних:

ЗК2. Здатність вчитися і оволодівати сучасними знаннями.

ЗК3. Здатність застосовувати знання у практичних ситуаціях.

ЗК4. Здатність спілкуватися державною мовою як усно, так і письмово.

ЗК7. Вміння виявляти, ставити та вирішувати проблеми.

фахових:

ФК1. Здатність застосовувати законодавчу та нормативно- правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі комп'ютерної інженерії.

ФК4. Здатність забезпечувати захист інформації, що обробляється в комп'ютерних та кіберфізичних системах та мережах з метою реалізації встановленої політики інформаційної безпеки.

ФК9. Здатність системно адмініструвати, використовувати, адаптувати та експлуатувати наявні інформаційні технології та системи.

ФК10. Здатність здійснювати організацію робочих місць, їхнє технічне оснащення, розміщення комп'ютерного устаткування, використання організаційних, технічних, алгоритмічних та інших методів і засобів захисту інформації.

ФК13. Здатність вирішувати проблеми у галузі комп'ютерних та інформаційних технологій, визначати обмеження цих технологій.

3. Опис навчальної дисципліни

3.1. Лекційні заняття

№	Тема заняття та короткий зміст	Кількість годин	
		ДФН	ЗФН
1.	Тема 1. Правові та організаційні засади захисту інформації в інформаційних системах.	2	0,5
2.	Тема 2. Основні загрози безпеці інформації в інформаційно-комунікаційних системах.	2	0,5
3.	Тема 3. Концепція побудови інформаційної безпеки.	2	0,5
4.	Тема 4. Засоби антивірусного захисту інформації.	2	0,5
5.	Тема 5. Системи контролю та керування доступом.	2	0,5
6.	Тема 6. Захист інформації на рівні операційної системи.	2	0,5
7.	Тема 7. Захист інформації в комп'ютерних мережах.	2	0,5
8.	Тема 8. Захист інформації в базах даних.	2	0,5
9.	Тема 9. Програмні методи та засоби захисту інформації в ІКС.	2	0,5
10.	Тема 10. Технічний захист інформації в ІКС.	2	0,5
11.	Тема 11. Апаратно-програмні методи та засоби захисту інформації в ІКС.	2	0,5
12.	Тема 12. Безпека програмного забезпечення, методологія безпечного програмування.	2	0,5
13.	Тема 13. Криптографічні методи захисту інформації.	2	0,5
14.	Тема 14. Стеганографічні методи захисту інформації.	2	0,5
15.	Тема 15. Управління інформаційною безпекою в ІКС.	2	0,5
16.	Тема 16. Проектування, введення в дію та супроводження захищених ІКС.	2	0,5
Усього годин		32	8

3.2. Практичні заняття

не передбачено

3.3. Лабораторні заняття

№	Тема заняття	Кількість годин	
		ДФН	ЗФН
1.	Ізольований запуск програм у Windows. Пісочниця Windows.	4	1
2.	Відновлення та знищення даних на електронних носіях.	4	1
3.	Захист веб-додатків від SQL-ін'єкцій.	4	1
4.	Налаштування параметрів безпеки Інтернет-браузерів.	4	1
5.	Захист інформації в архівах.	4	1
6.	Захист інформації на електронних носіях.	4	1
7.	Робота з електронними цифровими підписами.	4	1
8.	Аналіз ефективності парольного захисту PDF документів.	4	1
Усього годин		32	8

3.4. Самостійна робота

№	Найменування робіт	Кількість годин	
		ДФН	ЗФН
1.	Опрацювання лекційного матеріалу	19	51
2.	Підготовка до лабораторних занять	16	32
3.	Підготовка та складання тестування: - Тест модуль №1 - Тест модуль №2	36	36
Усього годин		71	119

4. Критерії оцінювання результатів навчання студентів

Форма підсумкового семестрового контролю – **залік**

Підсумкова семестрова оцінка складається з суми балів, отриманих студентом при проведенні проміжних (модульних) контролів рівня засвоєння теоретичних знань (за перший та другий модулі), отриманих балів за лабораторні роботи та оцінки за залік.

Захист звіту з лабораторної роботи оцінюється відповідною кількістю балів, поданою в таблиці.

Після проходження теоретичного матеріалу проводиться перевірка якості його засвоєння у вигляді тестування в рамках проміжного (модульного) контролю. Контроль здійснюється засобами електронного навчального курсу (ЕНК) на сервері дистанційного навчання.

МОДУЛЬ 1			МОДУЛЬ 2			ПІДСУМКОВА СЕМЕСТРОВА ОЦІНКА ЗА ЗАЛІК	РАЗОМ З ДИСЦИПЛІНИ
АУДИТОРНА ТА САМОСТІЙНА РОБОТА			АУДИТОРНА ТА САМОСТІЙНА РОБОТА				
ТЕОРЕТИЧНИЙ КУРС (ТЕСТУВАННЯ)	ЛАБОРАТОРНА РОБОТА		ТЕОРЕТИЧНИЙ КУРС (ТЕСТУВАННЯ)	ЛАБОРАТОРНА РОБОТА			
СЕМЕСТРОВА ОЦІНКА						25	100
20	17		20	18			
№ ЛЕКЦІЙ	ВИД РОБІТ	БАЛ	№ ЛЕКЦІЙ	ВИД РОБІТ	БАЛ	За кожних три бали семестрової оцінки студент отримує 1 бал підсумкової семестрової оцінки автоматично	
Тема 1	Лаб. роб. №1	4	Тема 9	Лаб. роб. №5	4		
Тема 2			Тема 10				
Тема 3	Лаб. роб. №2	4	Тема 11	Лаб. роб. №6	5		
Тема 4			Тема 12				
Тема 5	Лаб. роб. №3	5	Тема 13	Лаб. роб. №7	5		
Тема 6			Тема 14				
Тема 7	Лаб. роб. №4	4	Тема 15	Лаб. роб. №8	4		
Тема 8			Тема 16				

До підсумкового семестрового контролю (заліку) допускаються студенти, які протягом семестру виконали всі види навчальної роботи, успішно пройшли проміжні

(модульні) контролі і набрали не менше 45 балів семестрової бальної оцінки та за умови отримання не менше 60% (15) балів за результатами кожного проміжного (модульного) контролю рівня знань.

Підсумкова оцінка записується за 100-бальною шкалою із подальшим переведенням її у шкалу Європейської кредитно-трансферної системи (ECTS) відповідно A, B, C, D, E, F, FX при цьому чотирибальна шкала оцінок (з записом семестрової оцінки «відмінно» - A, «добре» - B,C, «задовільно» - D, E відповідають підсумковому результату «зараховано», «незадовільно» - F, FX відповідає підсумковому результату «незараховано»).

5. Навчально-методичне забезпечення

1. Козак Р.О., Хомишин В.Г., Максимчук О.О. Захист інформації в інформаційно-комунікаційних системах [електронний ресурс] // Інституційний репозиторій ATutor (код дисципліни ID 2335): офіційний сайт Тернопільського національного технічного університету імені Івана Пулюя – Тернопіль, 2014. – Режим доступу: https://dl.tntu.edu.ua/index.php .

2. Козак Р.О., Хомишин В.Г., Максимчук О.О. Конспект лекцій з дисципліни "Захист інформації в інформаційно-комунікаційних системах" для студентів денної та заочної форм навчання спеціальностей 122 "Комп’ютерні науки", 123 "Комп’ютерна інженерія" та 125 "Кібербезпека та захист інформації". Тернопіль: ТНТУ. 2023. – Режим доступу: https://dl.tntu.edu.ua/index.php.

3. Козак Р.О., Хомишин В.Г., Максимчук О.О. Методичні вказівки для виконання лабораторних робіт з дисципліни "Захист інформації в інформаційно-комунікаційних системах" для студентів денної та заочної форм навчання спеціальностей 122 "Комп’ютерні науки", 123 "Комп’ютерна інженерія" та 125 "Кібербезпека та захист інформації". Тернопіль: ТНТУ. 2023. – Режим доступу: https://dl.tntu.edu.ua/index.php.

4. Козак Р.О., Хомишин В.Г., Максимчук О.О. Методичні вказівки для виконання самостійної роботи з дисципліни "Захист інформації в інформаційно-комунікаційних системах" для студентів денної та заочної форм навчання

спеціальностей 122 "Комп'ютерні науки", 123 "Комп'ютерна інженерія" та 125 "Кібербезпека та захист інформації". Тернопіль: ТНТУ. 2023. – Режим доступу: https://dl.tntu.edu.ua/index.php.

6. Рекомендована література

Базова

1. Новітні технології захисту інформації: підручник / М.Г. Луцький , В.О. Хорошко, Ю.Є. Хохлачова та ін. – Київ: НАУ, 2023. – 310 с.

2. Бобало Ю.Я. Інформаційна безпека: навч. посібник / Ю.Я. Бобало, І.В. Горбатий, М.Д. Кіселичник та ін. – Львів: Видавництво Львівської політехніки, 2019. – 580 с.

3. Остроухов В.В. Інформаційна безпека. Підручник / В.В. Остроухов, М.М. Присяжнюк, О.І. Фармагей, М.М. Чеховська та ін.; під ред. В.В. Остроухова – К.: Видавництво «Ліра-К», 2021. – 412 с.

4. Кібербезпека: сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. / С.Е. Остапов, С.П. Євсеєв, О.Г. Король. – Львів: «Новий Світ – 2000», 2020. – 678 с.

5. Сагун А.В. Основи криптографічного та стеганографічного захисту інформації : навч. посіб. для студентів спец. 125 – «Кібербезпека», 12 «Інформаційні технології» всіх форм навчання. Ч. 1 : Криптографічний захист інформації / А.В. Сагун, О.М. Кулініч, В.В. Хайдуров. – Київ: НУБіП України, 2023. – 303 с.

6. Сагун А.В. Основи криптографічного та стеганографічного захисту інформації : навч. посіб. для студентів спец. 125 – «Кібербезпека», 12 «Інформаційні технології» всіх форм навчання. Ч. 2 : Стеганографічний захист інформації / А.В. Сагун, О.М. Кулініч, В.В. Хайдуров. – Київ: НУБіП України, 2023. – 144 с.

7. Грайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем. – К.: Видавнича група BHV, 2009. – 608 с.

Допоміжна

1. Технічний захист інформації: Навч. посіб. в 2 ч. Ч. 1: Основи технічного захисту інформації / В.М. Богуш, В.Д. Бровко, О.С. Кобус, В.Д. Козюра. – К.: Видавництво «Ліра-К», 2022. – 286 с.

2. Програмне забезпечення систем захисту інформації: підручник / Н.М. Блавацька, В.Д. Козюра, В.О. Хорошко. – К.: Вид. ДУПКТ, 2011. – 330 с.

3 Основи кіберпростору, кібербезпеки та кіберзахисту. Навч. посіб. / В.М. Богуш, В.В. Богуш, В.Д. Бровко, В.П. Настрадін; під. ред. В. М. Богуша. – К.: Видавництво «Ліра-К», 2020. – 554 с.

7. Інформаційні ресурси

1. Електронний навчальний курс «Захист інформації в інформаційно-комунікаційних системах» (ID: 2335), доступний за адресою: https://dl.tntu.edu.ua/bounce.php?course=2335

8. Зміни та доповнення до робочої програми навчальної дисципліни

№	Зміст внесених змін (доповнень)	Дата і № протоколу засідання кафедри	Примітки