Міністерство освіти і науки України
Харківський національний університет імені В.Н. Каразіна
Кафедра безпеки інформаційних систем і технологій

“ЗАТВЕРДЖУЮ”

Проректор з науково – педагогічної роботи

Олександр ГОЛОВКО

“___” _____2022 р.

Робоча програма навчальної дисципліни

«Безпека інформаційних систем»

рівень вищої освіти другий (магістерський)
галузь знань 012 - Інформаційні технології
спеціальність 122 – «Комп'ютерні науки»
освітня програма « Інформаційні управляючі системи та технології».
вид дисциплін обов'язкова
факультет комп'ютерних наук

2022 / 2023

2

Програму обговорено та рекомендовано до затвердження вченою радою факультету комп'ютерних наук "28 " червня 2022 року, протокол №10

РОЗРОБНИКИ ПРОГРАМИ:
Лисицька Ірина Вікторівна, доктор технічних наук, професор, професор кафедри безпеки інформаційних систем і технологій.

Програму схвалено на засіданні кафедри безпеки інформаційних систем і технологій
Протокол від " 23 " червня 2022 року № 10

Завідувач кафедри безпеки інформаційних систем і технологій

Сергій Рассомахін

Гарант освітньої (професійної/наукової) програми
(керівник проєктної групи) Стєрвоєдов Микола Григорович

Микола Стєрвоєдов

Програму погоджено методичною комісією факультету комп'ютерних наук
Протокол від "24 "червня 2022 року №9

Голова методичної комісії факультету комп'ютерних наук

Анатолій Бердников

ВСТУП

Програма навчальної дисципліни «Безпека інформаційних систем» складена відповідно до освітньо-професійної програми підготовки другого (магістерського) рівня «Інформаційні управляючі системи та технології» за спеціальністю 122 – Комп′ютерні науки .

.

1. Опис навчальної дисципліни

1.1. Мета навчальної дисципліни

Закласти термінологічний фундамент, навчити студентів правильно проводити аналіз погроз інформаційній безпеці, основним методам, принципам, алгоритмам захисту інформації в комп'ютерних системах з урахуванням сучасного стану розвитку методів, систем та засобів здійснення погроз зі сторони потенційних порушників.

1.2. Основні завдання дисципліни:

У цьому курсі передбачається формування у студентів певних знань та вмінь з теорії та практики захисту інформації.

1.3. Кількість кредитів – 3.

1.4. Загальна кількість годин – 90.

1.5. Характеристика навчальної дисципліни	
Нормативна	
Денна форма навчання	Заочна (дистанційна) форма навчання
Рік підготовки	
5-й	-й
Семестр	
9-й	-й
Лекції	
16 год.	год.
Практичні, семінарські заняття	
16 год.	год.
Лабораторні заняття	
	год.
Самостійна робота	
58 год.	год.
Індивідуальні завдання	

1.6. Заплановані результати навчання

За результатами вивчення дисципліни студенти повинні

ЗНАТИ:

вибрані питання теорії розширення полів та еліптичних кривих;

вибрані питання теорії випадкових підстановок;

положення нової методології прискореної оцінки стійкості симетричних криптосистем до атак диференціального та лінійного криптоаналізу.

ВМІТИ:

- застосовувати отримані теоретичні знання на практиці;
- досліджувати симетричні криптосистеми за допомогою нової методології оцінки стійкості до атак диференціального та лінійного криптоаналізу.

2. Тематичний план навчальної дисципліни

i. Розділ 1. Вибрані питання теорії розширення полів та еліптичних кривих.

ii. Тема 1. Прості алгебраїчні розширення полів**.**

iii. Зміст. . Алгебраїчні числа. Кінцеві розширення полів. Поле алгебраїчних чисел.

iv. *Тема 2.* Кінцеві поля засновані на кільцях многочленів.

v. Зміст. Структура кінцевого поля. Теореми про структуру кінцевого поля. Мінімальні многочлени. Властивості мінімальних многочленів. Як знаходити незвідні многочлени.

vi. Тема 3. Операції над розширеннями полів Галуа характеристики 2. **.**

vii. *Зміст.* Загальні відомості про сліди та базиси розширень полів. Поліноміальне надання. Оптимальне базисне надання.

viii. Тема 4. Операції над розширеннями полів Галуа характеристики 2. **.**

ix. *Зміст.* Множення в $\mathbf{F}_2^m$, яке використовує оптимальний нормальний базис. Структура множення. Переваги оптимального нормального базису.

x. Тема 5. Еліптичні криві та операції над ними.

xi. Зміст. Однородні координати та проективна площина. Криві в проективній площині.

Тема 6. Еліптичні криві над довільними полями.

Зміст. Арифметика еліптичних кривих. Порядок групи точок елиптичної кривої та порядок точки.

Тема 7. Еліптичні криві над полем характеристики 2.

Зміст. Закони додавання точок для суперсингулярних та сингулярних кривих. Використання оптимального нормального базису поля F_2^m при виконанні операцій в групах точок ЕК.

Тема 8. Перспективи розвитку криптографії на еліптичних кривих.

3. Структура навчальної дисципліни

Назва розділів і тем	Кількість годин					
	Денна форма					
	Усього	у тому числі				
		Л	ПЗ	Лаб.	Інд.	С.Р.
1	2	3	4	5	6	7
i. **Тема 1.** *Тема 1.* Прості алгебраїчні розширення полів**.**	11	2	2			7
Тема 2. Кінцеві поля засновані на кільцях многочленів.	11	2	2			7
Тема3. . Операції над розширеннями полів Галуа характеристики 2.	11	2	2			7
Тема4. Операції над розширеннями полів Галуа характеристики 2.	11	2	2			7

Тема 5. .Еліптичні криві та операції над ними.	11	2	2			7
Тема 6. Еліптичні криві над довільними полями.	11	2	2			7
Тема 7. Еліптичні криві над полем характеристики 2.	11	2	2			7
Тема 8. Перспективи розвитку криптографії на еліптичних кривих.	13	2	2			9
Усього годин	90	16	16			58

4. Теми практичних занять

№ з/п	Назва теми	Кількість Годин
1	Алгебраїчні розширення полів. Неприводимі многочлени над полем. Розкладання многочленів на неприводимі множники. Цілі і раціональні корені многочлена з цілими коефіцієнтами. Критерий Ейзенштейна.	2
2	Алгебраїчні розширення полів Алгебраїчні й трансцендентні числа. Побудова простого алгебраїчного розширения поля.	2
3	Кінцеві поля, засновані на кільцях многочленів. Поля Галуа.	2
4	Обчислення мінімальних многочленів.	2
5	Операції над розширеними полями характеристики 2. Сліди та базиси розширеного поля.	2
6	Поліноміальний та нормальний базиси. Оптимальний нормальний базис та його переваги.	2
7	Еліптичні криві над полями дійсних та раціональних чисел.	2
8	Елиптичні криві над простими полями Галуа.	2
	Разом	16

5. Завдання для самостійної робота

№ з/п	Види, зміст самостійної роботи	Кількість Годин
1	Підготовка до лекцій	8
2	Підготовка до практичних занять	8
3	Виконання контрольних робіт (2 контрольних)	20
4	Вивчення додаткових матеріалів за темою занять	17
5	Підготовка до заліку	5
	Разом	58

6. Індивідуальні завдання

Виконання двох індивідуальних контрольних робіт.

7. Методи навчання

Як правило лекційні та практичні заняття проводяться аудиторно. В умовах дії карантину заняття проводяться відповідно до Наказу ректора Харківського національного університету імені В.Н. Каразіна (аудиторне або дистанційно за допомогою платформ Google Meet або Zoom).

8. Методи контролю

Контроль засвоєння студентами навчального матеріалу на лекційному зайнятті здійснюється шляхом концентрації уваги студентів постановкою питань за раніше вивченим матеріалом, пов'язаним з тематикою лекції.

Присутність студента на лекційному занятті оцінюється в 1 бал. Максимальна кількість балів за присутність студента на лекційних заняттях (8 лекцій) – 8 балів.

На практичному зайнятті контроль знань студентів робиться методом проведення експрес-опитувань та рішення типових задач. Рівень знань, продемонстрований студентами на кожному практичному занятті оцінюється у 5 балів.

На протязі курсу студенти виконують дві контрольних роботи за темою занять. Кожна контрольна робота оцінюється у 26 балів.

Вивчення дисципліни передбачає проведення підсумкового контролю у вигляді заліку.

Наприкінці курсу підсумовуються бали, які студент набрав за лекційні, практичні заняття та контрольні роботи. Якщо оцінка студента влаштовує, бали заліку виставляються у залікову книжку та залікову відомість.

Якщо оцінка не влаштовує – складається залік. Студент повинен відповісти на два теоретичні питання, та вирішити практичне завдання згідно з білетом.

Максимальна кількість балів за результатами вивчення дисципліни складає 100 балів.

Критерії оцінювання знань студентів за виконання контрольної роботи

Визначення	Кількість балів
Дані повні відповіді на кожне питання показано тверде знання навчального матеріалу, розуміння суті поставлених питань, зроблені повні і правильні висновки	26
У відповідях на поставлені питання показано знання навчального матеріалу, розуміння суті поставлених питань за наявності незначних помилок зроблені достатньо повні і правильні висновки	20-25
У відповідях на поставлені питання показано достатньо знання навчального матеріалу при наявності суттєвих помилок, зроблені висновки	12-19
У відповідях показано розуміння суті поставлених питань за наявності принципових помилок при рішенні практичних завдань, відсутні висновки	6-11
У відповідях на поставлені питання показано слабкі знання навчального матеріалу при наявності принципових помилок, відсутні висновки	3-5

9. Схема нарахування балів

Поточний контроль, самостійна робота, індивідуальні завадання									Сума
Розділ 1								Контрольні роботи (2), передбачені навчальним планом	
Т1	Т2	Т3	Т4	Т5	Т6	Т7	Т8		
6	6	6	6	6	6	6	6	2*26=52	100

Т1, Т2 ... – теми розділів.

Шкала оцінювання

Сума балів за всі види навчальної діяльності протягом семестру	Оцінка	
	для екзамену	для заліку
90 – 100	відмінно	зараховано
70-89	добре	
50-69	задовільно	

Результати підсумкового контролю у вигляді заліку виставляються до залікової відомості та до індивідуального плану студента.

10. Рекомендована література

Основна література

1. Методичі вказівки до самостійної роботи студентів з дисципліни “Розширення полів та еліптичні криві”, Електрона версія. ХНУРЕ, 2005.

2. Клесов, О. І. Елементарна теорія чисел та елементи криптографії [Електронний ресурс] : підручник / О. І. Клесов. – Електронні текстові дані (1 файл: 5,35 Мбайт). – Київ : ТВіМС, 2016. – 412 с.

3. Андрійчук В.І., Забавський Б.В. Алгебра і теорія чисел // -Львів. -2005.

10. Посилання на інформаційні ресурси в Інтернеті, відео-лекції, інше методичне забезпечення

1. Закон України від 15 грудня 2005 року № 3200-IV "Про основи національної безпеки України".
2. Закон України "Про інформацію". Із змінами, внесеними згідно із Законом від 07.02.2002 № 3047-III-ВР.
3. Закон України "Про Національну програму інформатизації" Із змінами, внесеними згідно із Законом від 13.09.2001 № 2684-III-ВР.
4. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 31.05.2005 № 2594-IV.
5. Закон України «Про електронний цифровий підпис» від 22.05.2003 № 852-IX.
6. Закон України «Про електронний документ та електронний документообіг» від 22.05.2003 № 851-IV.