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

Технології захисту інформації

рівень вищої освіти перший (бакалаврський)

галузь знань 12 «Інформаційні технології»

спеціальність 122 – «Комп'ютерні науки»

освітня програма «Комп'ютерні науки»

спеціалізація

вид дисципліни обов'язкова

факультет комп'ютерних наук

2022 / 2023

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 «Технології захисту інформації» складена відповідно до освітньо-професійної програми підготовки першого (бакалаврського) рівня «Комп′ютерні науки» за спеціальністю 122 – «Комп′ютерні науки та інформаційні технології»ю.

.

---

1. Опис навчальної дисципліни

1.1. Мета викладання 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 вивчення дисципліни

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

За результатами вивчення дисципліни студенти повинні

ЗНАТИ:

- сучасні погрози безпеці інформаційним системам;
- технічні методи і засоби захисту інформації;
- криптографічні методи захисту інформації;
- програмні методи і засоби захисту;
- організаційно-правове забезпечення захисту інформації.

ВМІТИ:

- аналізувати можливості несанкціонованого здобуття інформації потенційними порушниками;
- досліджувати стійкість криптографічних систем і протоколів;
- досліджувати симетричні та асиметричні криптосистеми.

1.3. Кількість кредитів 4

1.4. Загальна кількість годин 120

1.5. Характеристика навчальної дисципліни	
Нормативна	
Денна форма навчання	Заочна (дистанційна) форма навчання
Рік підготовки	
3-й	3-й
Семестр	
6-й	6-й
Лекції	
32 год.	32 год.
Практичні, семінарські заняття	
32 год.	32год.
Лабораторні заняття	
год.	год.

Самостійна робота	
56 год.	56 год.
Індивідуальні завдання	
14 год (в межах самостійної роботи)	

1.6. Заплановані результати навчання

У результаті вивчення даного курсу студент повинен:

знати:

За результатами вивчення дисципліни студенти повинні

ЗНАТИ:

- сучасні погрози безпеці інформаційним системам;
- технічні методи і засоби захисту інформації;
- криптографічні методи захисту інформації;
- програмні методи і засоби захисту;
- організаційно-правове забезпечення захисту інформації.

ВМІТИ:

- аналізувати можливості несанкціонованого здобуття інформації потенційними порушниками;
- досліджувати стійкість криптографічних систем і протоколів;
- досліджувати симетричні та асиметричні криптосистеми.

2. Тематичний план навчальної дисципліни

Розділ 1. Основні поняття та означення інформаційної безпеки та криптології.

Тема 1. Вступ до дисципліни. Основні поняття та означення інформаційної безпеки.

Актуальність та важливість забезпечення інформаційної безпеки. Типи загроз безпеці автоматизованої системи обробки інформації. Основні поняття та означення.

Тема 2. Основні поняття та означення криптології. (Криптографія та криптоаналіз, шифрування, розшифрування, ключ, основні типи шифрів, вимоги до шифрів, схема однобіччнго каналу захищеної передачі інформації).

Розділ 2. Класичні симетричні криптосистеми.

Тема 1. Класичні симетричні криптосистеми. Найпростіші шифри заміни і перестановки. Одноалфавітні криптосистеми.

Шифр Цезара, афінна система підстановок Цезара, шифр Цезара з ключовим словом, табличні шифри, криптосистема Хіла, подвійний квадрат Уінстона, шифр Трисемуса, система омофонів.

Тема 2. Класичні симетричні криптосистеми. Найпростіші шифри заміни і перестановки. Багатоалфавітні криптосистеми.

Шифр Віженера, Гронсфельда, шифрувальні прилади, решітки Кордано.

Тема 3. Класичні симетричні криптосистеми. Блоковий симетричний шифр DES та режими його роботи.

Поняття про гамування. Забезпечення криптографічної стійкості. Структура алгоритму. Режими роботи алгоритму. Використання алгоритму в різних режимах.

Тема 4. Класичні симетричні криптосистеми. Блоковий симетричний шифр ГОСТ 28-147-89 р.та режими його роботи.

Поняття про гамування. Забезпечення криптографічної стійкості. Структура алгоритму. Режими роботи алгоритму. Використання алгоритму в різних режимах.

Тема 5. Ключові дані симетричних алгоритмів.

Структура ключових даних БСШ. Вимоги до ключових послідовностей та їх формування.

Тема 6. Класичні симетричні криптосистеми. Блоковий симетричний алгоритм RIJNDAEL та режими його роботи.

Структура алгоритму. Перетворення алгоритму. Використання алгоритму в різних режимах.

Розділ 3. Класичні двоключові криптосистеми.

Тема 1. Класичні двоключові криптосистеми.

Концепція киптосистем з відкритим ключем. Алгоритми RSA та Ель Гамала в режимі шифування.

Тема 2. Проблема аутентифікації даних та електронний цифровий підпис.

Геш функції. Вимоги до них. Процедура постановки та перевірки підпису. Алгоритми RSA та Ель Гамала в режимі ЕЦП.

Тема 3. Криптоаналіз двоключових криптосистем та алгоритми факторизації.

Алгоритми Поларда та ρ-1 Поларда.

Тема 4. Криптоаналіз двоключових криптосистем та алгоритми факторизації.

Алгоритми Ферма та Діксона. Задача тестування на простоту та формування великих простих чісел.

Розділ 4. Криптоалгоритми засновані на перетвореннях у групі точок еліптичних кривих.

Тема 1. Поняття про еліптичні криві. Математика у групі точок еліптичних кривих.

Види ЕК. Поняття та визначення. Додавання та подвоєння точок. Прядок кривої та порядок точки кривої.

Тема 2. Сліди та базиси розширеного поля.

Поліноміальний та нормальний базиси. Надання кривій у різних координатних системах.

Тема 3. Оптимальний нормальний базис розширеного поля та його переваги.

Перехід від поліноміального базису до нормального. Добуток елементів у нормальному базисі. Переваги нормального базису.

Тема 4. Дискретне логарифмування у групі точок ЕК.

ρ метод Поларда дискретного логарифмування у групі точок ЕК.

3. Структура навчальної дисципліни

Назви розділів 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

Розділ 1. Основні поняття та означення інформаційної безпеки та криптології.												
Тема 1. Вступ до дисципліни. Основні поняття та означення інформаційної безпеки.	4	2	2			3						
Тема 2. Основні поняття та означення криптології.	4	2	2			3						
Разом за розділом 1	8	4	4			6						
Розділ 2. Класичні симетричні криптосистеми.												
Тема 1. Класичні симетричні криптосистеми. Найпростіші шифри заміни і перестановки. Одноалфавітні та багатоалфавітні криптосистеми.	4	2	2			3						
Тема 2. Математичні алгоритми, які найчастіше використовуються в криптографії.	4	2	2			3						
Тема 3. Класичні симетричні криптосистеми. Блоковий симетричний шифр DES та режими його роботи.	4	2	2			3						
Тема 4. Класичні симетричні криптосистеми. Блоковий симетричний шифр ГОСТ 28-147-89 р.та режими його роботи.	4	2	2			4						
Тема 5. Ключові дані симетричних алгоритмів.	4	2	2			4						

Тема 6. Класичні симетричні криптосистеми. Блоковий симетричний алгоритм RIJNDAEL та режими його роботи.	4	2	2			4						
Разом за розділом 2	24	12	12			21						
Розділ 3. Класичні двоключові криптосистеми.												
Тема 1. Класичні двоключові криптосистеми.	4	2	2			3						
Тема 2. Проблема аутентифікації даних та електронний цифровий підпис.	4	2	2			3						
Тема3. Криптоаналіз двоключових криптосистем та алгоритми факторизації.	4	2	2			3						
Тема 4. Криптоаналіз двоключових криптосистем та алгоритми факторизації (продовжння).	4	2	2			4						
Разом за розділом 3	16	8	8			13						
Розділ 4. Криптоалгоритми засновані на перетвореннях у групі точок еліптичних кривих.												
Тема 1. Поняття про еліптичні криві. Математика у групі точок еліптичних кривих.	4	2	2			4						
Тема 2. Сліди та базиси розширеного поля.	4	2	2			4						
Тема 3. Оптимальний нормальний базис розширеного поля та його переваги.	4	2	2			4						

Тема 4. Дискретне логарифмування у групі точок ЕК.	4	2	2			4						
Разом за розділом 4	16	8	8			16						
Усього годин	64	32	32			56						

4. Теми семінарських (практичних, лабораторних) занять

№ з/п	Назва теми	Кількість годин
1	Основні поняття та означення інформаційної безпеки та криптології	2
2	Найпростіші шифри заміни та перестановки	2
3	Найпростіші шифри заміни та перестановки	2
4	Математичні алгоритми, які найчастіше використовуються у криптографії.	2
5	Формування ключових даних для БСШ	2
6	Афінне перетворення алгоритму RIJNDAEL	2
7	Симетричні криптосистеми. Рішення задач.	2
8	Симетричні криптосистеми. Рішення задач.	2
9	Двоключові криптосистеми	2
10	Двоключові криптосистеми.	2
11	Алгоритми факторизації	2
12	Алгоритми факторизації	2
13	Операції у групах точок еліптичних кривих	2
14	Сліди та базиси розширеного поля	2
15	Добуток елементів у оптимальному нормальному базисі	2
16	Дискретне логарифмування у групі точок ЕК	2
	Разом	32

5. Завдання для самостійної робота

№ з/п	Види, зміст самостійної роботи	Кількість годин
1	Робота над лекційним матеріалом	16
2	Підготовка до практичних занять	16
3	Виконання індивідуальних завдань (контрольної роботи для КІ і КУ)	14
4	Підготовка до заліку	10
	Разом	56

6. Індивідуальні завдання

Згідно з варіантом кожен студент вирішує 2 індивідуальних завдання (для КС)

7. Методи навчання

Як правило лекційні та практичні заняття проводяться аудиторне. 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.

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 домашню контрольну роботу за темою занять. Контрольна робота оцінюється у 24 балів.

Вивчення дисципліни передбачає проведення підсумкового контролю у вигляді заліку.

Наприкінці курсу підсумовуються бали, які студент набрав за лекційні, практичні заняття та домашню контрольну роботу. 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.

9. Схема нарахування балів

Поточний контроль, самостійна робота, індивідуальні завадання																	Сума
Розділ 1		Розділ 2						Рзділ 3				Розділ 4				Інд. завд (к.р)	
Т1	Т2	Т1	Т2	Т3	Т4	Т5	Т6	Т1	Т2	Т3	Т4	Т1	Т2	Т3	Т4		
3	3	5	5	5	5	5	5	5	5	5	5	5	5	5	5	24	100

Т1, Т2 ... – теми розділів.

Критерії оцінювання

Критерії оцінювання знань студентів на практичному занятті

Визначення	Кількість балів
Повне та безпомилкове виконання завдання або відповідь на питання	5
Виконання завдання з незначними помилками	4
Завдання має певну кількість помилок, але рішення задачі йде у правильному напрямку.	3
Неправильна відповідь чи рішення, мають місце грубі помилки.	1-2
Нерозуміння суті питання або задачі	0

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	
1-49	незадовільно	не зараховано

10. Рекомендована література
Основна література

1. Горбенко І. Д. ″ Криптографічний захист інформації ″. Навч. посібник Харків, ХНУРЕ, 2004 р.
2. Вербіцький О. В. Всуп до криптології. - Львів.: Видавництво науково-технічної літератури, 1998. - 247 с.
3. А. Бессалов, А. Телиженко. Криптосистемы на эллиптических кривых. Киев, ″ Політехніка ″ , 2004, 223 с.

10. Посиланная 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.
7. FIPS PUB 186-3-2009. Digital signature standard: 2009. National Institute of standard and technology. – 2009.
8. НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу, затверджені наказом ДСТСЗІ СБУ від 28 квітня 1999 року № 22.
9. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу, затверджені наказом ДСТСЗІ СБУ від 28 квітня 1999 року № 22.
10. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу, затверджені наказом ДСТСЗІ СБУ від 28 квітня 1999 року № 22.