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.

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	
4-й	-й
Семестр	
7-й	-й
Лекції	
36 год.	год.
Практичні, семінарські заняття	

12 год.	год.
Лабораторні заняття	
	год.
Самостійна робота	
42 год.	год.
Індивідуальні завдання	
домашня контрольна робота 10 год.	

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. Інформаційна безпека та криптологія. Класичні симетричні криптосистеми.

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

Зміст. .Основні поняття та означення інформаційної безпеки. Основні загрози безпеці АСОІ. Основні поняття та означення криптології. Математична модель захищеної передачі інформації в каналі зв'язку. Основні поняття та означення криптології (криптографія, криптоаналіз, шифрування, розшифрування, ключ, криптограмма). Математична модель захищеної передачі інформації в каналі зв'язку. Основні групи шифрів.

Тема 2. Найпростіші шифри заміни та перестановки.

Зміст. Одноалфавітні шифри (Цезара, Афінна система підстановок Цезара, шифр Цезара з ключем, криптосистема Хіла, одноразовий блокнот тощо). Багатоалфавітні шифри (Віженера, Гронсфельда).

Тема 3. Математичні алгоритми, які найчастіше використовуються в криптографії.

Зміст. (Алгоритм Евкліда, розширений алгоритм Евкліда, алгоритм Монтгомері тощо)

Тема 4. Класичні симетричні криптосистеми. Стандарт блокового симетричного шифрування DES.

Зміст. Загальна характеристика алгоритму DES та режими його роботи. Криптостійкість та використання стандарту .

Тема 5. Класичні симетричні криптосистеми. Алгоритм IDEA Криптостійкість та використання стандарту .

*Тема 6.*Класичні симетричні криптосистеми. Алгоритм RJNDAEL. та режими його роботи.

Зміст. Загальна характеристика алгоритму RJNDAEL та режими його роботи. Криптостійкість та використання алгоритму.

Розділ 2. Класичні двоключові криптосистеми та їх використання. Проблеми автентифікації даних та ЕЦП.

Тема1. Вступ в теорію асиметричних криптоперетворень. Концепція криптосистем з відкритим ключем.

Зміст. Криптосистеми RSA та Ель Гамала. Система Діфі – Гелмана. Види зловмисних дій, проти котрих можна захиститися з використанням ЕЦП. ЕЦП RSA та Ель Гамала. Переваги та недоліки.

Тема 2. Загальні відомості відносно методів криптоаналізу двоключових криптосистем. Алгоритми факторизації.

Зміст. Алгоритми факторизації Поларда та (ρ-1) Поларда. Алгоритми факторизації Ферма та Діксона.

Тема 3. Елиптичні криві та операції у групах точок еліптичних кривих.

Зміст. Поняття еліптичної кривої, класифікація. Операції у групі точок ЕК.

Тема 4. Сліди і базиси розширеного поля. Надання точок кривій у різних координатних системах.

Зміст. Поняття про сліди і базиси. Сліди і базиси розширеного поля. Побудова поліноміального та нормального базису.

Тема 5. Оптимальний нормальний базис поля $F2^m$ та його переваги.

Зміст. Оптимальний нормальний базис. Знаходження добутку двох елементів оптимального нормального базису. Простота піднесення до степені та вилучення кореня квадратного у оптимальному нормальному базисі.

Тема 6. Проблема дискретного логарифмування у групі точок ЕК.

Зміст. Алгоритм Поларда вирішення задачі дискретного логарифму у групі точок ЕК.

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

Розділ 1. Інформаційна безпека та криптологія. Класичні симетричні криптосистеми. **Тема 1.** Вступ до дисципліни. Основні поняття та означення інформаційної безпеки та криптології.	7	3	1			3
Тема 2. Найпростіші шифри заміни та перестановки.	7	3	1			3
Тема3. Математичні алгоритми, які найчастіше використовуються в криптографії.	7	3	1			3
Тема4. Класичні симетричні криптосистеми. Стандарт блокового симетричного шифрування DES.	7	3	1			3
Тема 5. Класичні симетричні криптосистеми. Алгоритм IDEA.	7	3	1			3
Тема 6. Класичні симетричні криптосистеми. Алгоритм RJNDAEL. та режими його роботи.	7	3	1			3
Розділ 2. Класичні двоключові криптосистеми та їх використання. Проблеми автентифікації даних та ЕЦП. **Тема 1.** Вступ в теорію асиметричних криптоперетворень. Концепція криптосистем з відкритим ключем.	8	3	1			4

Тема 2. Загальні відомості відносно методів криптоаналізу двоключових криптосистем.Алгоритми факторизації.	8	3	1			4
Тема 3. Елиптичні криві та операції у групах точок еліптичних кривих.	8	3	1			4
Тема 4. Сліди і базиси розширеного поля. Надання точок кривій у різних координатних системах.	8	3	1			4
Тема 5. Оптимальний нормальний базис поля $F2^m$ та його переваги.	8	3	1			4
Тема 6. Проблема дискретного логарифмування у групі точок ЕК.	8	3	1			4
Усього годин	90	36	12			42

4. Теми практичних занять

№ з/п	Назва теми	Кількість Годин
1	Основні поняття та означення інформаційної безпеки та криптології.	1
2	Найпростіші шифри заміни та перестановки. Одноалфавітні криптосистеми. Багатоалфавітні криптосистеми. Рішення задач.	1
3	Алгоритми, які найчастіше використовуються в криптографії.	1
4	Класичні симетричні криптосистеми. Рішення задач.	1
5	Афінне перетворення алгоритму RJNDAEL. Рішення задач.	1
6	Ітогове заняття за розділом 1.	1
7	Класичні.двоключові криптосистеми. Рішення задач.	1

8	Алгоритми факторизації. Рішення задач.		1
9	Операції у групі точок ЕК. Рішення задач.		1
10	Сліди і базиси розширеного поля.		1
11	Оптимальний нормальний базис поля $F2^m$ та його переваги.		1
12	Ітогове заняття за розділом 2.		1
	Разом		12

5. Завдання для самостійної роботи

№ з/п	Види та зміст завдання	Кількість годин
1	Підготовка до лекцій	12
2	Підготовка до практичних занять	12
3	Читання додаткової літератури	6
4.	Виконання контрольної роботи.	10
4	Підготовка до заліку	2
	Разом	42

6. Індивідуальні завдання (домашня контрольна робота)

Кожен студент на протязі курсу виконує домашню контрольну роботу. До завдань контрольної роботи включено типові задачі за темами занять.

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.

Присутність студента на лекційному занятті оцінюється в 1 бал. Максимальна кількість балів за присутність студента на лекційних заняттях (12 лекцій) – 12 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 домашню контрольну роботу за темою занять. Контрольна робота оцінюється у 28 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 дисципліні складає 100 балів.

9. Схема нарахування балів

Бали за поточний контроль знань по розділу 1 протягом семестру (по темах)												Домашня контрольна робота	Загальна сума балів
Т 1	Т 2	Т 3	Т 4	Т 5	Т 6	Т 7	Т 8	Т 9	Т 10	Т 11	Т 12		

												28	100
6	6	6	6	6	6	6	6	6	6	6	6		

Т1, Т2, Т3, Т4 ... – теми занять.

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 дворівневої шкали оцінювання (залік)
90 – 100	відмінно (зараховано)
70-89	добре (зараховано)
50-69	задовільно (зараховано)
1-49	незадовільно (незараховано)

10. Рекомендована література

Базова література

1. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Електронний підручник. Харків, ХНУРЕ, 2011 р.

2. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Електронний конспект лекцій. Харків, ХНУРЕ, 2011 р.

3. Горбенко І. Д. Гриненко Т. О. Захист інформації в інформаційно-телекомунікаційних системах: Навч. посібник. Ч.1. Криптографічний захист інформації - Харків: ХНУРЕ, 2004 - 368 с.

4. Горбенко Ю.І., Горбенко І.Д. Інфраструктури відкритих ключів . Системи ЕЦП. Теорія та практика. Харків. Форт. 2010 , 593с.

5. Задірака В. Комп'ютерна криптологія. Підручник. К, 2002 ,504с.

10.1 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.

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.