Міністерство освіти і науки України

Харківський національний університет імені В.Н. Каразіна

Кафедра безпеки інформаційних систем і технологій

"ЗАТВЕРДЖУЮ"

Проректор з науково-педагогічної роботи

А.В. Пантелеймонов

"___" _____ 2019 р.

Робоча програма навчальної дисципліни

Технології захисту інформації

рівень вищої освіти перший (бакалаврський)

галузь знань 12 «Інформаційні технології»

спеціальність 123– «Комп'ютерна інженерія»,
151 «Автоматизація та комп'ютерно-інтегровані технології».

освітня програма – «Комп'ютерна інженерія»,
«Автоматизація та комп'ютерно-інтегровані технології».

спеціалізація

вид дисципліни обов'язкова

факультет комп'ютерних наук

2019 / 2020 навчальний рік

Програму обговорено та рекомендовано до затвердження вченою радою факультету комп'ютерних наук

"28" серпня 2019 року, протокол № 3

РОЗРОБНИКИ ПРОГРАМИ:

Доктор технічних наук, професор, професор кафедри безпеки інформаційних систем і технологій **Лисицька Ірина Вікторівна.**

Програму схвалено на засіданні кафедри теоретичної та прикладної системотехніки

Протокол від "19" червня 2019 року № 13

Завідувач кафедри безпеки інформаційних систем і технологій

_____ Рассомахін С.Г.

Програму погоджено методичною комісією факультету комп'ютерних наук

Протокол від "20" червня 2019 року № 9

Голова методичної комісії факультету комп'ютерних наук

_____ Бердніков А. Г.

ВСТУП

Програма навчальної дисципліни «Технології захисту інформації» складена відповідно до освітньої програми підготовки першого (бакалаврського) рівня за спеціальністю 123, 151 – «Комп'ютерна інженерія», «Автоматизація та комп'ютерно інтегровані технології».

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 – 4.
1.4. Загальна кількість годин – 120.

1.5. Характеристика навчальної дисципліни	
Нормативна	
Денна форма навчання	Заочна (дистанційна) форма навчання
Рік підготовки	
4-й	-й
Семестр	
7-й	-й
Лекції	
32 год.	год.
Практичні, семінарські заняття	
32 год.	год.
Лабораторні заняття	
	год.
Самостійна робота	
56 год.	год.
Індивідуальні завдання	

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.

Зміст. .Основні поняття та означення інформаційної безпеки. Основні загрози безпеці АСОІ.

Тема 2. Основні поняття та означення криптології. Математична модель захищеної передачі інформації в каналі зв'язку.

Зміст. Основні поняття та означення криптології (криптографія, криптоаналіз, шифрування, розшифрування, ключ, криптограмма). Математична модель захищеної передачі інформації в каналі зв'язку. Основні групи шифрів.
Найпростіші шифри заміни та перестановки. Одноалфавітні та багато алфавітні криптосистеми.

Тема 3. 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 4. Математичні алгоритми, які найчастіше використовуються в криптографії.

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

Тема 5. Класичні симетричні криптосистеми. Стандарт блокового симетричного шифрування DES.

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

Тема 6. Класичні симетричні криптосистеми. Стандарт ГОСТ 28 147 89 р.

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

*Тема 7.*Класичні симетричні криптосистеми. Алгоритм RJNDAEL. та режими його роботи.

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

Тема 8. Блокові симетричні шифри у сучасній криптографії.

Зміст. Блокові симетричні шифри у сучасній криптографії. Напрямки розвитку сучасної симетричної криптографії.

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.

Тема 3. Загальні відомості відносно методів криптоаналізу двоключових криптосистем. Алгоритми факторизації.

Зміст. Алгоритми факторизації Ферма та Діксона.

Тема 4. Елиптичні криві та операції у групах точок еліптичних кривих.

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

Тема 5. 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 6. Оптимальний нормальний базис поля F_2^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 7. Проблема дискретного логарифмування у групі точок ЕК.

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

Тема 8. Проблеми сучасної криптографії та перспективи розвитку.

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.	6	2	2			3
Тема 2. Основні поняття та означення криптології. Математична модель захищеної передачі інформації в каналі зв'язку.	7	2	2			3
Тема 3. Найпростіші шифри заміни та перестановки.	7	2	2			4
Тема 4. Математичні алгоритми, які найчастіше використовуються в криптографії.	7	2	2			4
Тема 5. Класичні симетричні	7	2	2			4

криптосистеми. Стандарт блокового симетричного шифрування DES.						
Тема 6. Класичні симетричні криптосистеми. Стандарт ГОСТ 28 147 89 р.	7	2	2			3
Тема 7. Класичні симетричні криптосистеми. Алгоритм RJNDAEL. та режими його роботи.	7	2	2			4
Тема 8. Блокові симетричні шифри у сучасній криптографії.	7	2	2			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.	7	2	2			4
Тема 2. Загальні відомості відносно методів криптоаналізу двоключових криптосистем.Алгоритми факторизації.	7	2	2			3
Тема 3. Загальні відомості відносно методів криптоаналізу двоключових криптосистем.Алгоритми факторизації (продовження).	7	2	2			4
Тема 4. Елиптичні криві та операції у групах точок еліптичних кривих.	7	2	2			3
Тема 5. Сліди і базиси розширеного поля. Надання точок кривій у різних координатних системах.	7	2	2			4
Тема 6. Оптимальний нормальний базис поля F_2^m та його переваги.	7	2	2			3
Тема 7. Проблема дискретного логарифмування у групі точок ЕК.	7	2	2			4
Тема 8. Проблеми сучасної криптографії та перспективи розвитку.	6	2	2			3
Усього годин	120	32	32			56

4. Теми практичних занять

№ з/п	Назва теми	Кількість Годин
1	Основні поняття та означення інформаційної безпеки та криптології.	2
2	Найпростіші шифри заміни та перестановки. Одноалфавітні криптосистеми. Рішення задач.	2
3	Найпростіші шифри заміни та перестановки. Багатоалфавітні криптосистеми. Рішення задач.	2
4	Алгоритми, які найчастіше використовуються в криптографії.	2

5	Класичні симетричні криптосистеми. Рішення задач.	2
6	Класичні симетричні криптосистеми. Рішення задач.	2
7	Афінне перетворення алгоритму RJNDAEL. Рішення задач.	2
8	Ітогове заняття за розділом 1.	2
9	Класичні.двоключові криптосистеми. Рішення задач.	2
10	Алгоритми факторизації. Рішення задач.	2
11	Алгоритми факторизації. Рішення задач.	2
12	Операції у групі точок ЕК. Рішення задач.	2
13	Сліди і базиси розширеного поля.	2
14	Оптимальний нормальний базис поля F_2^m та його переваги.	2
15	Проблема дискретного логарифмування у групі точок ЕК.	2
16	Ітогове заняття за розділом 2.	2
	Разом	32

5. Завдання для самостійної роботи

№ з/п	Види та зміст завдання	Кількість годин
1	Підготовка до лекцій	16
2	Підготовка до практичних занять	16
3	Читання додаткової літератури	15
4	Підготовка до заліку	9
	Разом	56

6. Індивідуальні завдання

Кожен студент на протязі курсу виконує індивідуальне завдання. До завдання включені типові задачі за темами занять.

7. 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 (16 лекцій) – 16 балів.

На практичному зайнятті контроль знань студентів робиться методом проведення експрес-опитувань та рішення типових задач згідно з варіантом. Рівень знань, продемонстрований студентами на кожному практичному занятті оцінюється у 3 бали.

На протязі курсу студенти виконують індивідуальні завдання за темою занять. Виконання індивідуальних завдань контролюється двічі в межах загального обсягу годин. Перша частина завдання присвячена задачам симетричної криптографії оцінюється у 18 балів та виконання цього індивідуального завдання контролюється на 8-му практичному занятті (перша частина курсу), друга частина завдання присвячена задачам двоключової криптографії оцінюється у 18 балів та виконання цього індивідуального завдання контролюється на 16-му практичному занятті (друга частина курсу).

Вивчення дисципліни передбачає проведення підсумкового контролю у вигляді заліку.

Наприкінці курсу підсумовуються бали, які студент набрав за лекційні, практичні заняття та індивідуальне завдання. 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.

8. Схема нарахування балів

Бали за поточний контроль знань по розділу 1 протягом семестру (по темах)																Індивідуальне завдання	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	Т 13	Т 14	Т 15	Т 16	36	100
4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4		

Т1, Т2, Т3, Т4 ... – теми занять.

Критерії оцінювання

Критерії оцінювання знань студентів на практичному занятті

Визначення	Кількість балів
Повне та безпомилкове виконання завдання згідно з варіантом	3
Виконання відповіді з незначними помилками	2
Відповідь є з певною кількістю помилок, які не заважають достатньо повному висвітленню питання	1
Неправильна відповідь, мають місце грубі помилки, нерозуміння суті питання	0

Шкала оцінювання

Сума балів за всі види навчальної діяльності протягом семестру	Оцінка
	для чотирирівневої шкали оцінювання (залік)
90 – 100	відмінно (зараховано)
70-89	добре (зараховано)
50-69	задовільно (зараховано)
1-49	Незадовільно (не зараховано)

9. 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. Есин В. И., Кузнецов А. А., Сорока Л. С. Безопасность информационных систем и технологий – Х.:ООО «ЭДЭНА», 2010.-656с.

Допоміжна література

1. Задірака В. Компьютерная криптологія. Підручник. К, 2002 ,504с.
2. Бембо Мао. Современная криптографія. Теорія и практика. Москва. 2005.
3. Брюс Шнайер. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. Изд. Триумф. М., 2003 г. 815 с.
4. Б. Шнайер . Безопасность данных в цифровом мире. Изд. Питер. Харьков. 2003 г. 367 с.
5. В. Столлингс. Криптография и защита сетей. Принципы и практика. Изд. "Вильямс". К. 2001. 669 с.
6. Шеннон К. Работы по теории информации и кибернетике, М., ИЛ, 1963, с. 333-369 (Також «Введение в криптографию» под ред. В. В. Ященко // http://nature.web.ru/db/msg.html?mid=1157083&uri=node1.html).
7. А. Менезис, П. Ван Аршот, С. Ватсон. Руководство по прикладной криптографии CRC Press, 1997, электронная копия, 662 с.
8. Бессалов А., Телиженко А. Криптосистемы на эллиптических кривых.– К.: «Політехніка», 2004. – 224 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. ГОСТ Р 34.10-2001. Информационная технология. Криптографическая защита информации. Процедуры формирования и проверки электронной цифровой подписи. – М.: Госстандарт России, 2001. – 20 с.
9. 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.
10. 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.
11. 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.
12. Введение в криптографию под ред. В. В. Ященко // http://nature.web.ru/db/msg.html?mid=1157083&uri=node1.html
13. Казарин О. В. Безопасность программного обеспечения компьютерных систем // http://citforum.ru/security/articles/kazarin
14. Ростовцев А. Г., Михайлова Н. В. Методы криптоанализа классических шифров//http://www.ssl.stu.neva.ru/psw/crypto/rostovtsev/cryptoanalysis.html
15. Федотов Н. Н. Защита информации (Учебный курс) // http://www.college.ru/UDP/texts/index.html