КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ТОРГОВЕЛЬНО-ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ

СИСТЕМА УПРАВЛІННЯ ЯКІСТЮ
Система забезпечення якості освітньої діяльності та якості вищої освіти
сертифікована на відповідність ДСТУ ISO 9001:2015 / ISO 9001:2015

Кафедра інженерії програмного забезпечення та кібербезпеки

ЗАТВЕРДЖЕНО
вченою радою
(прот. № ____ від ____ 2021 р.)
Ректор
_____ А. А. Мазаракі

КРИПТОГРАФІЧНІ МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ /
CRYPTOGRAPHIC METHODS OF INFORMATION PROTECTION

РОБОЧА ПРОГРАМА /
COURSE OUTLINE

освітній ступінь	**Магістр** / Master
галузь знань	**12 Інформаційні технології** / Information Technologies
спеціальність	**124 Системний аналіз** / System Analysis
спеціалізація	**Інформаційні технології та бізнес-аналітика (Data Science)** / Information Technologies and Business Analytics (Data Science)

Київ 2021

Автори: Н.В. ЛУКОВА-ЧУЙКО, доктор технічних наук, професор
А.О. ФЕСЕНКО, кандидат технічних наук, доцент
Л.О. ВЛАСЕНКО, кандидат технічних наук, доцент
Т.В. САВЧЕНКО, кандидат технічних наук, доцент
М.В. САШНЬОВА, кандидат технічних наук, доцент
Ю.В. КОСТЮК, асистент

Робочу програму розглянуто та затверджено на засіданні кафедри інженерії програмного забезпечення та кібербезпеки 25 травня 2021 р., протокол № 9.

Рецензенти: А.М. Десятко, PhD
О.І. Бандак, Tech Lead, Senior Software Developer, SDK Finance

КРИПТОГРАФІЧНІ МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ /
CRYPTOGRAPHIC METHODS OF INFORMATION PROTECTION

РОБОЧА ПРОГРАМА /
COURSE OUTLINE

освітній ступінь	**магістр**	**/**	master
галузь знань	**12 Інформаційні технології**	**/**	Information Technologies
спеціальність	**124 Системний аналіз**	**/**	System Analysis
освітня програма	**Інформаційні технології та бізнес-аналітика (Data Science)**	**/**	Information Technologies and Business Intelligence (Data Science)

1. СТРУКТУРА ДИСЦИПЛІНИ ТА РОЗПОДІЛ ГОДИН ЗА ТЕМАМИ (ТЕМАТИЧНИЙ ПЛАН)

Назва теми	Кількість годин				Форми контролю
	Усього год/кредитів	Лекції	Лабораторні заняття	Самостійна робота студ.	
Тема 1. Історичний огляд криптографічних методів захисту інформації	32	4	4	20	УО, ЛР,
Тема 2. Сучасні криптографічні методи захисту інформації	32	4	2	20	УО, ЛР
Тема 3. Криптографія та криптоаналіз. Симетричні та асиметричні криптографічні перетворення	26	2	4	20	УО, ЛР
Тема 4. Криптографічні протоколи	24	4	2	20	УО, ЛР
Тема 5. Протоколи аутентифікації (ідентифікації)	22	2	2	20	УО, ЛР
Тема 6. Управління криптографічними ключами	22	2	4	20	УО, ЛР
Тема 7. Стеганографічний захист інформації	22	2	2	20	УО, ЛР, Т
Разом	**180/6**	**20**	**20**	**140**	
Підсумковий контроль – екзамен					

Примітка: УО – усне опитування; ЛР – захист лабораторних робіт;
Т – тестування.

2. Тематика та зміст лекційних та лабораторних занять, самостійної роботи студентів

Результати навчання	Навчальна діяльність*	Робочий час студента (год.)
Тема 1. Історичний огляд криптографічних методів захисту інформації		
Знати: Базові поняття криптографії. Поняття та види шифрів: шифр простої заміни, шифри перестановки, шифр багатоалфавітної заміни.	***План лекції*** 1. Історія криптографії. 2. Базові поняття криптографії. 3. Роль криптографії у захисті даних. **Список рекомендованих джерел:** *Основний: 1, 3, 4* *Додатковий: 10, 14, 15*.	2
	Завдання для самостійної роботи: Вивчення матеріалів лекції на основі самостійного опрацювання основних літературних джерел, зазначених у списку та електронних матеріалів, які надаються викладачем. Ознайомлення і оволодіння понятійним апаратом. Вивчення різних видів шифрів та особливостей їх використання. **Список рекомендованих джерел:** *Основний: 1, 3, 4* *Додатковий: 10, 14, 15*.	20
Вміти: *проводити шифрування і дешифрування тексту, написаного кирилицею і латиницею, «методом Цезаря»*	***Лабораторна робота*** ***Мета:*** оволодіння практичними навичками із застосування методів частотного аналізу до шифру Цезаря. ***Завдання:*** *Написати програму для шифрування тексту за допомогою методу «Шифр Цезаря». Необхідно реалізувати як шифрування, так і дешифрування текстів українською та англійською мовами. Знайти ключ, використовуючи оцінку логарифмічної функції правдоподібності*	4

Результати навчання	Навчальна діяльність*	Робочий час студента (год.)
	та розшифрувати текст, зашифрований на українській мові за алгоритмом Цезаря	
Знати: Базові поняття криптографії. Поняття та види шифрів: шифр простої заміни, шифри перестановки, шифр багатоалфавітної заміни.	***План лекції*** 1. Поняття та види шифрів. 2. Вимоги до шифрів - принцип Керхгоффса. 3. Шифрувальні машини та підходи до їх аналізу. 4. Ідеальний шифр і класи стійкості шифрів. **Список рекомендованих джерел:** *Основний: 1, 3, 4* *Додатковий: 10, 14, 15*.	2
Тема 2. Сучасні криптографічні методи захисту інформації		
Знати: основні криптографічні методи та їх особливості, симетричні та асиметричні методи шифрування інформації, поняття ключа, шифри	***План лекції*** 1. Основні види криптографічних методів 2. Реалізація криптографічних методів 3. Симетричні і асиметричні методи шифрування **Список рекомендованих джерел:** *Основний: 1, 2, 5* *Додатковий: 12, 17, 18* *Internet-ресурси: 19*	2

Результати навчання	Навчальна діяльність*	Робочий час студента (год.)
на основі мереж Фейстеля та SP, алгоритму DES.	**Завдання для самостійної роботи:** *Вивчення матеріалів лекції на основі самостійного опрацювання основних літературних джерел, зазначених у списку та електронних матеріалів, які надаються викладачем. Визначити різницю між закритими і відкритими ключами. Ознайомитись з особливостями шифрування і дешифрування шифрами на основі мережі Фейстеля та її модифікацій, SP-мережі та Data Encryption Standard* **Список рекомендованих джерел:** *Основний: 1, 2, 5* *Додатковий: 12, 17, 18* *Internet-ресурси: 19*	20
Вміти: *проводити шифрування і дешифрування українського тексту, зашифрованого стовпцевою перестановкою та подвійною перестановкою, а також за допомогою шифру S-DES*	***Лабораторна робота*** ***Мета:*** вивчення елементів частотного аналізу криптограми: частоти біграм, сполучність букв. ***Завдання:*** Розшифрувати вислів, зашифрований стовпцевою перестановкою (текст українською мовою). Для криптоаналізу використовуються таблиці біграм та сполучність букв. Розшифрувати вислів, зашифрований подвійною перестановкою (спочатку були переставлені стовпці, потім рядки; текст українською мовою).	2
	Лабораторна робота ***Мета:*** *вивчення структури DES — для шифрування і дешифрування з використанням блокових шифрів.* ***Завдання:*** написати програму, що реалізує процес шифрування та дешифрування даних за допомогою шифру S-DES в режимі Electronic Code Book (ECB).	2

Результати навчання	Навчальна діяльність*	Робочий час студента (год.)
Знати: основні криптографічні методи та їх особливості, симетричні та асиметричні методи шифрування інформації, поняття ключа, шифри на основі мереж Фейстеля та SP, алгоритму DES.	***План лекції*** 1. Шифри на основі мережі Фейстеля. Мережа Фейстеля. 2. Американський шифр DES. 3. Шифри на основі SP-мережі. **Список рекомендованих джерел:** *Основний: 1, 2, 5* *Додатковий: 12, 17, 18* *Internet-ресурси: 19*	2
Тема 3. Криптографія та криптоаналіз. Симетричні та асиметричні криптографічні перетворення		
Знати: види криптографічних перетворень, особливості застосування основних методів генерації псевдовипадкових числових послідовностей.	***План лекції*** 1. Криптографічне перетворення. 2. Симетричні криптографічні перетворення. 3. Методи генерації псевдовипадкових числових послідовностей. Модулярна арифметика. 4. Перспективи розвитку криптографії. 5. Створення комбінованих криптографічних засобів та нові підходи до побудови шифрів. **Список рекомендованих джерел:** *Основний:* 1, 2, 3. *Додатковий:* 8-10. *Інтернет-ресурси:* 19, 20, 21.	2
	Завдання для самостійної роботи: Вивчення матеріалів лекції на основі самостійного опрацювання	20

Результати навчання	Навчальна діяльність*	Робочий час студента (год.)
	основних літературних джерел, зазначених у списку та електронних матеріалів, які надаються викладачем. Ознайомлення з основами медулярної арифметики. Розглянути перспективи розвитку криптографії, підходи до створення комбінованих криптографічних підходів до шифрування. **Список рекомендованих джерел:** *Основний:* 1, 2, 3. *Додатковий:* 8-10. *Інтернет-ресурси:* 19, 20, 21.	
Вміти: *проводити шифрування і дешифрування українського тексту на основі алгоритмів блочного шифрування*	***Лабораторна робота*** ***Мета:*** отримати навички у реалізації на вибраній мові програмування алгоритму блочного шифрування даних ДСТУ ГОСТ 28147:2009. ***Завдання****: розробити на обраній мові програмування консольний або віконний додаток, що реалізує алгоритм ДСТУ ГОСТ 28147:2009 за такими режимами шифрування: режим простої заміни (з доповненням блоків); режим гамування; режим гамування зі зворотним зв'язком. Вхідні дані: вхідний текст у вигляді символів або байтів, ключ, вектор ініціалізації, режим роботи (шифрування або дешифрування), режим шифрування. Вихідні дані: для шифрування — послідовність байтів зашифрованого***.**	4
Тема 4. Криптографічні протоколи		
Знати: призначення криптографічного протоколу, учасників протоколу, примітивні і прикладні	***План лекції*** 1. Поняття криптографічних протоколів. Їх опис. 2. Класифікація криптографічних протоколів. Властивості, що визначають безпеку криптографічних протоколів. 3. Атаки на протоколи.	2

Результати навчання	Навчальна діяльність*	Робочий час студента (год.)
криптографічні протоколи. класифікацію за кількістю учасників, за кількістю переданих повідомлень, за цільовим призначенням протоколу та типом використовуваних криптографічних систем, за способом функціонування та надійністю.	4. Аналіз та моделювання криптографічних протоколів. **Список рекомендованих джерел:** *Основний: 2 –4* *Додатковий: 6 – 8, 13, 15, 17* *Internet-ресурси:19*	
	Завдання для самостійної роботи: Вивчення матеріалів лекції на основі самостійного опрацювання основних літературних джерел, зазначених у списку та електронних матеріалів, які надаються викладачем. Протоколи, що ґрунтуються на симетричних криптосистемах. Протоколи, що ґрунтуються на асимет-ричних криптосистемах. Протоколи обміну ключами. Квантовий розподіл ключів. Протокол розподілу ключів за допомогою еліптичних кривих. **Список рекомендованих джерел:** *Основний: 2 –4* *Додатковий: 6 – 8, 13, 15, 17* *Internet-ресурси:19*	20

Результати навчання	Навчальна діяльність*	Робочий час студента (год.)
Вміти: *проводити шифрування і дешифрування тексту, написаного кирилицею і латиницею, «методом Віженера»*	***Лабораторна робота*** ***Мета:*** *оволодіння практичними навичками із застосування методів частотного аналізу до шифру Віженера.* ***Завдання:*** *Знайти ключ, довжина якого відома та розшифрувати криптограму, яка зашифрована шифром Віженера (алфавіт – український із пропуском). Для криптоаналізу використовувати таблицю частот. Визначити довжину ключа, ключ та розшифрувати криптограму, яка зашифрована шифром Віженера (алфавіт — український із пропуском).*	2
Знати: призначення криптографічного протоколу, учасників протоколу, примітивні і прикладні криптографічні протоколи. класифікацію за кількістю учасників, за кількістю переданих повідомлень, за цільовим призначенням протоколу та типом використовуваних криптографічних систем, за способом	***План лекції*** 1. Протоколи електронного цифрового підпису. 2. Спеціальні види електронного підпису 3. Інтерактивні системи доведення 4. Поняття поділу секрету **Список рекомендованих джерел:** *Основний: 2 –4* *Додатковий: 6 – 8, 13, 15, 17* *Internet-ресурси:19*	2

Результати навчання	Навчальна діяльність*	Робочий час студента (год.)
функціонування та надійністю.		
Тема 5. Протоколи аутентифікації (ідентифікації)		
Знати: властивості, що визначають безпеку криптографічних протоколів.	***План лекції*** 1. Основні етапи аутентифікації та авторизації. 2. Чинники аутентифікації. 3. Класифікація видів аутентифікації 4. Розмежування доступу. 5. Моделі розмежування доступу. **Список рекомендованих джерел:** *Основний: 3, 4* *Додатковий: 7 – 9, 14, 15, 17* *Internet-ресурси:19*	2
	Завдання для самостійної роботи: Вивчення матеріалів лекції на основі самостійного опрацювання основних літературних джерел, зазначених у списку та електронних матеріалів, які надаються викладачем: аутентифікація на основі знань,	20

Результати навчання	Навчальна діяльність*	Робочий час студента (год.)
	аутентифікація на основі володіння, аутентифікація на основі ознак та дій, парольна аутентифікація, аутентифікація на основі коректної обробки алгоритмів, аутентифікація на основі електронних і фізичних ключів, протокол ідентифікації/аутентифікації на основі шифрування з відкритим ключем, біометрична аутентифікація. Дискреційна, мандатна та рольова моделі розмежування доступу. **Список рекомендованих джерел:** *Основний: 3, 4* *Додатковий: 7 – 9, 14, 15, 17* *Internet-ресурси:19*	
Вміти: *проводити аналіз та проектування корпоративних систем, визначати ролі у системі*	***Лабораторна робота*** ***Мета:*** *оволодіння практичними навичками із застосування методів аутентифікації та авторизації, розподілом прав доступу у системі.* ***Завдання:*** *Розробити проект корпоративної системи безпеки наданої користувачем. Запропонувати та обгрунтувати варіанти авторизації та ідентифікації користувача. Рзробити вимоги безпеки до парольної системи*	2
Тема 6. Управління криптографічними ключами		
Знати: Сутність управління ключами, стандарти генерації ключів, процедури зберігання та модифікації ключів	***План лекції*** 1. Сутність управління ключами. Принцип Керкгоффса. 2. Стандарти генерації ключів. Накопичення, розподілення, оновлення, зберігання, резервування ключів. 3. Генерація та модифікація ключа. 4. Зберігання та розподіл ключів. 5. Протоколи обміну ключами. 6. Протоколів, що ґрунтуються на симетричних криптосистемах	2

Результати навчання	Навчальна діяльність*	Робочий час студента (год.)
	7. Протоколи, що ґрунтуються на асиметричних криптосистемах **Список рекомендованих джерел:** *Основний: 1, 3, 4* *Додатковий: 7 – 9, 14, 15 – 18* *Internet-ресурси:19, 22*	
	Завдання для самостійної роботи: Вивчення матеріалів лекції. Трирівнева ієрархія розподілу ключів: головний ключ; ключ шифрування ключів; ключ шифрування даних (сеансовий ключ). Децентралізований та централізований розподіл ключів. Протокол Kerberos. Протокол Шаміра. Алгоритм Діффі-Хеллмана. **Список рекомендованих джерел:** *Основний: 1, 3, 4* *Додатковий: 7 – 9, 14, 15 – 18* *Internet-ресурси:19, 22*	20
Вміти: *проводити розробку та генерацію ключів у системі, програмування на мові Python*	***Лабораторна робота*** ***Мета:*** *оволодіння практичними навичками із застосування криптографічних ключів для захисту інформації.* ***Завдання:*** *Розробити та реалізувати на основі мові Python проект для генерації та перевірки криптографічних ключів.Реалізувати Протокол Kerberos та Протокол Шаміра. Реалізувати найпростіший варіант технології блокчейн для захисту інформації*	4
Тема 7. Стеганографічний захист інформації		
Знати: основні поняття стенографії, основні	***План лекції*** 1. Історичний огляд стеганографії.	2

Результати навчання	Навчальна діяльність*	Робочий час студента (год.)
загрози безпеки стеганографічних систем, класи порушників та типи атак, сфери застосування методів стеганографічного захисту інформації	2. Стеганографічна система. Стеганографічний контейнер. 3. Виявлення стеганографічного каналу. 4. Типи та класи порушників безпеки стеганографічних систем. 5. Типи атак на стеганографічні системи. 6. Комп'ютерна та цифрова стеганографія. **Список рекомендованих джерел:** *Основний: 1 – 5* *Додатковий: 6 – 9, 11, 13 – 17* *Internet-ресурси: 19 – 22*	
	Завдання для самостійної роботи: Вивчення матеріалів лекції. Основи стенографії, поняття стенагрофічної системи, контейнеру, каналу; три класи порушників: пасивний, активний та зловмисник; типи атак на стеганографічні системи: атака з відомим контейнером; атака з вибором контейнера; атака з відомим повідомленням; атака з вибором повідомлення; атака, що направлена на руйнування повідомлення. **Список рекомендованих джерел:** *Основний: 1 – 5* *Додатковий: 6 – 9, 11, 13 – 17* *Internet-ресурси: 19 – 22*	20
Вміти:	***Лабораторна робота*** ***Мета:*** *оволодіння практичними навичками із застосування стенографічного захисту інформації.* ***Завдання:*** *Провести аналіз програмних засобів для стенографічного захисту інформації. З допомогою мови Python провести аналіз наданої викладачем на практичне заняття інформацією наданої викладачем.*	2

Результати навчання	Навчальна діяльність*	Робочий час студента (год.)
	Провести її шифрування та дешифрування.	
Разом		**180 годин/ 6 кредитів**
Підсумковий контроль		**Письмовий екзамен**

* *Всі лабораторні завдання виконуються на основі інтерактивних методів навчання у комп'ютерному середовищі.*

3. *СПИСОК РЕКОМЕНДОВАНИХ ДЖЕРЕЛ*

Основний

1. Бабак В. П. Теоретичні основи захисту інформації : підручник // Бабак В. П. – Книжкове видавництво НАУ, 2008. – 752 с.
2. *Основи криптографічного захисту інформації : підручник / авт.: Г.М. Гулак, В.А. Мухачов, В.О. Хорошко, Ю.Є. Яремчук. – Вінниця : ВНТУ, 2011. – 94 с.*
3. Основи захисту інформації : навч. посібн. / О. А. Смірнов, Л. Г. Віхрова, С. І. Осадчий та ін. – Кіровоград, 2010. – 322 с.
4. Основи інформаційної безпеки / С. В. Кавун, О. А. Смірнов, В. Ф. Столбов – Кіровоград : Вид. КНТУ, 2012. – 414 с.
5. Фаль О. М. Криптографія : основні ідеї та застосування / О. М. Фаль. – К. : ІВЦ Видавництво «Політехніка», 2003. – 28 с.

Додатковий

6. Блінцов В. С. Захист програмних продуктів : навчальний посібник / В. С. Блінцов, С. С. Козирев. – Миколаїв : НУК, 2010. – 146 с.
7. Голубєв В. О. Інформаційна безпека : проблеми боротьби з кіберзлочинами : монографія / В. О. Голубєв. – Запоріжжя : ГУ «ЗІДМУ», 2003. – 250 с.
8. Гулак Г. Н. Основы криптографической защиты информации / Г. Н. Гулак. – К. : Вид. ГУІКТ, 2009. – 228 с.
9. Довгий С. О. Сучасні телекомунікації : Мережі, технології, безпека, економіка, регулювання: монографія / С. О. Довгий, П. П. Воробієнко, К. Д. Гуляєв; За загальною ред. С. О. Довгого. – [2-ге видання (доповнене)]. – К. : Аимут-Україна, 2013. – 608 с.
10. Защита компьютерной информации. Эффективные методы и средства / Шаньгин В. Ф. – К. : ДМК Пресс, 2008. – 544 с.
11. Інформаційний та кіберпростори : проблеми безпеки, методи та засоби боротьби : посібник / В. Л. Бурячок, С. В. Толюпа, В. В. Семко та ін. – К. : ДУТ – КНУ, 2016. – 178 с.
12. Кавун С. В. Інформаційна безпека : підручник / С. В. Кавун. – Харків: Вид. ХНЕУ, 2009. – 368 с.
13. Конахович Г. Ф. Захист інформації в мережах передачі даних : підручник / Г. Ф. Конахович. – К. : Видавництво ТОВ НВП «ІНТЕРСЕРВІС», 2009. – 714 с.
14. Криптографія [Електронний ресурс]. – Режим доступу : http://uk.wikipedia.org/wiki/Криптографія.
15. Кузнецов О. О. Захист інформації в інформаційних системах / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2011. – 512 с.

16. Остапов С. Е. Технології захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с. Правовий захист інформації : навчальний посібник / Н. І. Логінова, Р. Р. Дробожур. – Одеса : Фенікс, 2015. – 264 с.
17. Смит Р. Є. Аутентификация: от паролей до открытых ключем / Р. Є. Смит. – К. : Видавничий дім «Вільямс», 2002. – 432 с.
18. Столлингс В. Криптография и защита сетей : принципы и практика / В. Столлингс. – К. : Видавничий дім «Вільямс», 2001. – 672 с.

Internet-ресурси

19. Державна служба спеціального зв'язку та захисту інформації України http://www.dsszzi.gov.ua/dsszzi/control/uk/index
20. Захист інформації http://jrnl.nau.edu.ua/index.php/ZI
21. Бизнес и безопасность www.bsm.com.ua
22. Офіційний вебпортал парламенту України http://www.rada.gov.ua

**Курсивом зазначені джерела, що є в наявності в бібліотеці КНТЕУ*