

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ КОРАБЛЕБУДУВАННЯ
імені адмірала Макарова
Навчально-науковий інститут автоматики та електротехніки
Кафедра комп'ютерних технологій та інформаційної безпеки

Код за ОПІ
ПІ17

ЗАТВЕРДЖЕНО



Проректор
з науково-педагогічної роботи
Слободян С. О.
2023 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Program of the Discipline

**КРИПТОГРАФІЯ ТА СТЕГАНОГРАФІЯ
CRYPTOGRAPHY AND STEGANOGRAPHY**

Рівень вищої освіти перший (бакалаврський)
Тип дисципліни обов'язкова
Мова викладання українська

Галузь знань 12 Інформаційні технології
Спеціальність 125 Кібербезпека та захист інформації
Освітньо-професійна програма Системи технічного захисту інформації,
автоматизації її обробки

Робоча програма навчальної дисципліни «Криптографія та стеганографія» є однією зі складових комплексної підготовки фахівців галузі знань 12 «Інформаційні технології» спеціальності 125 «Кібербезпека та захист інформації» за освітньо-професійною програмою «Системи технічного захисту інформації, автоматизація її обробки»

«__»_____ 2023 р. – 17 с.

Розробник: к.т.н., доц. Козирев С. С., доцент кафедри комп'ютерних технологій та інформаційної безпеки (КТІБ).

Проект робочої програми навчальної дисципліни «Криптографія та стеганографія» узгоджено з гарантом освітньої програми.

Гарант освітньої програми «Системи технічного захисту інформації, автоматизація її обробки», к.т.н., доцент М. М. Нужний С. М. Нужний

Проект робочої програми навчальної дисципліни «Криптографія та стеганографія» розглянуто на засіданні кафедри КТІБ.

Протокол від «23» 06 2022 р. № 12.

Завідувач кафедри КТІБ, к.т.н., доцент М. М. Нужний С. М. Нужний

Проект робочої програми навчальної дисципліни «Криптографія та стеганографія» розглянуто методичною радою Навчально-наукового інституту автоматики і електротехніки.

Протокол від «30» 08 2023 р. № 1.

Голова, к.т.н., доцент Д. О. Жук Д. О. Жук

Проект робочої програми навчальної дисципліни «Криптографія та стеганографія» погоджено з навчальним відділом.

Начальник навчального відділу, к.т.н., доц. А. В. Лабарткава А. В. Лабарткава

Робочу програму навчальної дисципліни «Криптографія та стеганографія» затверджено Навчально-методичною радою НУК.

Протокол від «7» 09 2023 р. № 6.

Голова НМР НУК, д.т.н., професор Є. І. Трушляков Є. І. Трушляков

ЗМІСТ

Вступ.....	4
1. Опис навчальної дисципліни	5
2. Мета вивчення навчальної дисципліни.....	6
3. Передумови для вивчення навчальної дисципліни	6
4. Очікувані результати навчання.....	6
5. Програма навчальної дисципліни.....	6
6. Методи навчання, засоби діагностики результатів навчання та методи їх демонстрування	11
7. Форми поточного та підсумкового контролю.....	12
8. Критерії оцінювання результатів навчання.....	13
9. Засоби навчання.....	14
10. Рекомендовані джерела інформації.....	14

ВСТУП

Анотація

Навчальна дисципліна «Криптографія та стеганографія» є дисципліною професійної підготовки бакалаврів зі спеціальності 125 «Кібербезпека та захист інформації». Вона забезпечує формування досвіду і навичок аналізу та синтезу сучасних криптографічних та стеганографічних систем у відповідності до поставлених задач та вимог щодо захисту інформації.

Основним завданням навчальної дисципліни є вивчення математичних, алгоритмічних та технічних (апаратних) принципів та законів побудови сучасних криптографічних та стеганографічних систем, їх призначення та можливостей, а також області функціонування.

Основна увага приділяється здобуттю практичних навичок побудови надійних критичних інформаційних систем; вивчення сучасних крипто- та стегосистем, алгоритмів їх функціонування; знайомство з особливостями реалізації крипто- та стегоалгоритмів у різних умовах функціонування інформаційних систем та каналів зв'язку; огляд проблем та перспективних задач відповідного спрямування.

Ключові слова: криптографія, стеганографія, захист інформації, критичні інформаційні системи.

Abstract

The course "Cryptography and steganography" is a professional education discipline for bachelors of specialty 125 "Cybersecurity and information protection ". It provides the formation of experience and skills in the analysis and synthesis of modern cryptographic and steganographic systems in accordance with the tasks and requirements for information protection.

The main objective of the discipline is to study the mathematical, algorithmic and technical (hardware) principles and rules of building modern cryptographic and steganographic systems, their purpose and capabilities, as well as the area of operation.

The main attention is paid to obtaining practical skills in building reliable critical information systems; study of modern crypto- and steganosystems, algorithms for their functioning; familiarity with the aspects of the implementation of crypto- and stegoalgorithms in various conditions of the functioning of information systems and communication channels; review of problems and perspective goals of the course direction.

Key words: cryptography, steganography, information security, critical information systems.

1. Опис навчальної дисципліни

Найменування показників	Галузь знань, напрям підготовки, освітньо-кваліфікаційний рівень	Характеристика навчальної дисципліни	
		денна форма навчання	заочна форма навчання
Кількість кредитів – 8	Галузь знань: 12 Інформаційні технології Спеціальність: 125 Кібербезпека та захист інформації Освітня програма: Системи технічного захисту інформації, автоматизація її обробки	Обов’язкова	
Модулів – 3		Рік підготовки	
Змістових модулів – 4		3-й, 4-й	3-й, 4-й
Електронна адреса РПНД на сайті Університету: http://education.nuos.edu.ua/		Семестр	
		6-й, 7-й	6-й, 7-й
		Лекції	
Загальна кількість годин – 240		30 год.	8 год.
Тижневих годин для денної форми навчання: аудиторних – 4 год.; самостійної роботи – 4 год.		Лабораторні роботи	
		60 год.	8 год.
		Практичні роботи	
		30 год.	8 год.
		Самостійна робота	
		120 год.	216 год.
		Індивідуальне завдання не передбачено	
	Вид контролю: екзамен, екзамен		
	Форма контролю: комбінована		
	Освітній рівень: перший (бакалаврський)		

1. Мета вивчення навчальної дисципліни

Метою вивчення навчальної дисципліни «Криптографія та стеганографія» є формування у студентів відповідно до освітньо-професійної програми таких компетентностей:

Загальні компетентності:

ЗК 1 Здатність застосовувати знання у практичних ситуаціях.

ЗК 2 Знання та розуміння предметної області та розуміння професії.

Фахові компетентності:

ФК 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.

ФК 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.

2. Передумови для вивчення навчальної дисципліни

Передумовами для вивчення навчальної дисципліни є наступні дисципліни:

- Вища математика;
- Технології програмування систем автоматизованої обробки і захисту інформації;
- Теорія інформації, кодування та цифрова обробка інформації.

3. Очікувані результати навчання

Вивчення навчальної дисципліни передбачає формування та розвиток у студентів таких результатів навчання:

РН 20. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-комунікаційних системах;

РН 47. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації;

РН 48. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах.

4. Програма навчальної дисципліни

Модуль 1

Змістовний модуль 1. Криптографічні шифри

Тема 1.1. Історія криптографії та стеганографії. [1], С. 3-18; [2], С. 6-9.

Тема 1.2. Теоретичні оцінки надійності шифрів. [1], С. 140-150; [2], 44-50.

Тема 1.3. Класифікація шифрів та стегоінтервенцій. Принципи їх роботи. [2], С. 10-15; [3], С. 3-13; 40-45.

Змістовний модуль 2. Криптографічні алгоритми

Тема 2.1. Алгоритми симетричного шифрування. [3], С. 14-39.

Тема 2.2. Алгоритми асиметричного шифрування. [3], С. 56-71.

Тема 2.3. Алгоритми потокового шифрування. [3], С. 51-55.

Модуль 2

Змістовний модуль 3. Основи стеганографії

Тема 3.1. Термінологія та класифікація стеганографії. [2], С. 9-33.

Тема 3.2. Підсвідомий канал. [3], С. 56-64.

Тема 3.3. Динамічна стеганографія. [2], С. 33-39.

Змістовний модуль 4. Обчислювальна техніка і криптографія (ППП.28)

Тема 4.1. Особливості використання обчислювальної техніки в криптографії. [2], С. 51-62.

Тема 4.2. Цифрові стегоконтейнери. [2], С. 39-44.

Тема 4.3. Перспективні напрями криптографії та стеганографії. [2], С. 62-64.

Тематичний план навчальної дисципліни

Назви змістових модулів і тем	Денна форма					Заочна форма				
	Кількість годин									
	усього	у тому числі				усього	у тому числі			
		л	п	лаб	с.р		л	п	лаб	с.р
Модуль 1 (М1)										
Змістовий модуль 1. Криптографічні шифри										
Тема 1.1. Історія криптографії та стеганографії	18	2	-	2	14	20	2			18
Тема 1.2. Теоретичні оцінки надійності шифрів	20	2	2	4	12	20		2		18
Тема 1.3. Класифікація шифрів та стегоінтервенцій. Принципи їх роботи	22	4	4	6	8	20			2	18
Разом за змістовим модулем 1	60	8	6	12	34	60	2	2	2	54
Змістовий модуль 2. Криптографічні алгоритми										
Тема 2.1. Алгоритми симетричного шифрування	20	2	2	6	10	20		2		18
Тема 2.2. Алгоритми асиметричного шифрування	20	2	4	6	8	20			2	18
Тема 2.3. Алгоритми потокового шифрування	20	3	3	6	8	20	2			18
Разом за змістовим модулем 2	60	7	9	18	26	60	2	2	2	54
Разом за модулем 1	120	15	15	30	60	120	4	4	4	108

Назви змістових модулів і тем	Денна форма					Заочна форма				
	Кількість годин									
	усього	у тому числі				усього	у тому числі			
		л	п	лаб	с.р		л	п	лаб	с.р
Модуль 2 (М2)										
Змістовий модуль 3. Основи стеганографії										
Тема 3.1. Термінологія та класифікація стеганографії	18	2	2	2	12	20	2			18
Тема 3.2. Підсвідомий канал.	20	2	2	6	10	20		2		18
Тема 3.3. Динамічна стеганографія	22	4	4	6	8	20			2	18
Разом за змістовим модулем 3	60	8	8	14	30	60	2	2	2	54
Змістовний модуль 4. Обчислювальна техніка і криптографія										
Тема 4.1. Особливості використання обчислювальної техніки в криптографії.	20	2	2	4	12	20	2			18
Тема 4.2. Цифрові стегоконтейнери.	20	2	2	6	10	20			2	18
Тема 4.3. Перспективні напрями криптографії та стеганографії.	20	3	3	6	8	20		2		18
Разом за змістовим модулем 4	60	7	7	16	30	60	2	2	2	54
Разом за модулем 2	120	15	15	30	60	120	4	4	4	108
Разом за дисципліну	240	30	30	60	120	240	8	8	8	216

Примітка. Для студентів заочної форми навчання читаються оглядові лекції, проводяться практичні та лабораторні заняття за темами змістових модулів в обсягах відповідно до таблиці (розд. 5).

5. Теми практичних занять

№ з/п	Назва теми	Кількість годин
Змістовий модуль 1		
1	Ентропійні оцінки надійності.	2
2	Принципи шифрування. Переставні шифри.	2
3	Принципи стегоінтервенцій.	2
Змістовий модуль 2		
4	Алгоритми Віженера і Бофора.	2
5	Мережа Фейстеля.	2
6	Алгоритми Евкліда.	2
7	Перетворення у групі лишків. Генератор Блума-Блума-Шуба.	3
Змістовий модуль 3		
8	Класифікація стегоалгоритмів.	2
9	Підсвідомий канал (модулярні рівняння).	2
10	Розрахунок довжини динамічного контейнера. Оцінка надійності динамічної стегосистеми.	4
Змістовий модуль 4		
11	Обмеження пов'язані з переповненням. Вплив похибок округлення.	2
12	Оцінка ємності цифрового контейнера.	2
13	Квантова ідея факторизації.	3
Разом		30

6. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1	Вступне заняття. Інструктаж з техніки безпеки. Доведення плану робіт, вимог до звітів, принципів оцінювання. Ознайомлення з обладнанням та програмним забезпеченням лабораторії.	2
2	Шифр Playfair і шифр подвійного квадрата.	4
3	Оцінка надійності шифрів.	6
4	Розробка програмного коду для шифрування тексту шифром Цезаря. Шифрування методом Гронсфельда.	2
5	Шифрування за допомогою таблиці Віженера. Шифрування методом гамування.	4
6	Стандарт шифрування DES.	4
7	Криптосистема RSA.	4
8	Криптосистема Ель-Гамала.	4
9	Класифікація стегоалгоритму.	2
10	Реалізація підсвідомого каналу.	6
11	Реалізація динамічної стегосистеми.	6
12	Факторизація чисел із застосуванням р-алгоритму Полларда.	6
13	Розподіл ключів. Протокол Діффі-Хеллмана	4
14	Електронний цифровий підпис.	6
	Разом	60

Самостійна робота

Розподіл годин самостійної роботи для денної форми навчання:

- підготовка до лекційних занять – 0,5 год./1 год. занять;
- підготовка до практичних робіт – 1-2 год./ 1 робота;
- підготовка до лабораторних робіт – 2-3 год./1 робота;
- підготовка до контрольних заходів – 15-30 год.

Завдання для самостійної роботи

№	Вид роботи	Кількість годин	
		Денна форма навчання	Заочна форма навчання
1	Підготовка до лекцій	15	45
2	Підготовка до практичних занять	26	46
3	Підготовка до лабораторних робіт	42	90
4	Підготовка до модульних контрольних робіт	20	20
5	Підготовка до екзамену	17	15
Разом		120	216

5. Методи навчання, засоби діагностики результатів навчання та методи їх демонстрування

Методи навчання:

- лекція - усний виклад навчального матеріалу з використанням слайдів, інтернет-ресурсів, рекламних матеріалів виробників програмних продуктів, базових програмних засобів;
- робота з літературою - опрацювання різних видів джерел, спрямоване на формування нових знань у сфері захисту програмних продуктів, їх закріплення;
- практична робота - метод поглиблення і закріплення теоретичних знань та перевірки наукових висновків;
- лабораторна робота - вивчення в спеціалізованих лабораторіях методів і засобів захисту програмних продуктів з використанням спеціального програмного забезпечення.

Засоби оцінювання результатів навчання:

- звіти з виконання практичних завдань;
- звіти з лабораторних робіт;
- модульні контрольні роботи;
- екзамен.

Методи демонстрування результатів навчання:

- усні відповіді;
- виконання практичних розрахункових робіт;

- виконання завдань на лабораторному комп'ютерному комплексі, пов'язаних із здобуттям навичок стосовно принципів, методів і засобів технологічного та експлуатаційного захисту програмних продуктів;
- виконання модульних контрольних робіт;
- екзамен.

6. Форми поточного та підсумкового контролю

Досягнення здобувача вищої освіти оцінюються за 100-бальною системою Університету. Підсумкова оцінка навчального курсу включає в себе оцінки з поточного та підсумкового контролю.

Форми поточного контролю:

- захист звітів з виконання практичних завдань;
- захист звітів з лабораторних робіт;
- виконання модульних контрольних робіт;
- перевірка конспектів лекційного матеріалу.

Форми підсумкового контролю:

- екзамен.

Форми контролю результатів навчальної діяльності студентів та їх оцінювання

Практична робота	
Кількість балів	Критерії оцінювання
5	Робота виконана у встановлений термін. Виконана самостійно без помилок. Отримано вірні результати. Проведено коректні розрахунки, отримано вірні результати. Проведена коректна інтерпретація результатів.
4	Робота виконана у встановлений термін. Виконана самостійно без помилок. Отримано вірні результати. У висновках при інтерпретації результатів допущено неточності.
3	Робота виконана з порушенням встановлених термінів. Виконана самостійно, допущено незначні помилки. У висновках при інтерпретації результатів допущено неточності.
2	Робота виконана з порушенням встановлених термінів. Допущено помилки та неточності. У висновках при інтерпретації результатів допущено неточності.
1	Робота виконана з порушенням встановлених термінів. Допущено значні помилки. Отримано хибні результати.
0	Робота не виконана
	<i>Максимальна кількість балів за даний компонент програми 65 балів (13 робіт по 5 балів).</i>

Лабораторна робота	
Кількість балів	Критерії оцінювання
5	Робота виконана у встановлений термін. Виконана самостійно, чітко сформульовані мета та завдання досліджень. Коректно застосовано необхідне програмне забезпечення. Досягнуто результатів, що відповідають поставленому завданню. У висновках проведена коректна інтерпретація результатів.
4	Робота виконана у встановлений термін. Виконана самостійно згідно з інструкцією, чітко сформульовані мета та завдання досліджень. Коректно застосовано необхідне програмне забезпечення. Досягнуто результатів, що відповідають поставленому завданню. У висновках при інтерпретації результатів допущено неточності.
3	Робота виконана з порушенням встановлених термінів. Студент виконує лабораторну згідно з інструкцією; складений звіт містить неточності у висновках.
2	Робота виконана з порушенням встановлених термінів. Студент виконує лабораторну згідно з інструкцією; складений звіт містить неточності у висновках та помилки.
1	Робота виконана з порушенням встановлених термінів. Студент виконує лабораторну з порушенням інструкції; складений звіт містить неточності у висновках та помилки.
0	Робота не виконувалася.
<i>Максимальна кількість балів за даний компонент програми 70 балів (14 робіт по 5 балів).</i>	

Модульна контрольна робота

Правильних відповідей, %	100	90	80	70	60	50	40	30	20	10
Бал	10	9	8	7	6	5	4	3	2	1

Форма контролю	Максимальна кількість балів
Виконання практичних робіт	13 x 5 = 65 балів
Виконання лабораторних робіт	14 x 5 балів = 70 балів
Перевірка конспектів лекційного матеріалу	5 балів
Поточний модульних контроль	2 x 10 балів = 20 балів
Екзамен	40 балів
Всього за 2 семестри	2 x 100=200

7. Критерії оцінювання результатів навчання

№	Форма контролю	Максимальна кількість балів
Модуль 1		
1	Перевірка звітів з практичних робіт	7х5 бали = 35 балів
2	Перевірка та проведення процедури захисту звітів з лабораторних робіт	8х5 балів = 40 балів
3	Перевірка конспектів лекційного матеріалу	5 балів
4	Проведення та перевірка модульних підсумкових робіт (змістовий модуль 1, 2)	2х10 балів = 20 балів
Разом		100
Модуль 2		
1	Перевірка звітів з практичних робіт	6х5 балів = 30 балів
2	Перевірка та проведення процедури захисту звітів з лабораторних робіт	6х5 балів = 30 балів
3	Екзамен	40
Разом		100

Шкала оцінювання: національна та ECTS

Сума балів за результатом підсумкового контролю	Оцінка ECTS	Оцінка за національною шкалою
90 – 100	A	Відмінно
82 – 89	B	Дуже добре
74 – 81	C	Добре
64 – 73	D	Посередньо
60 – 63	E	Достатньо
35 – 59	FX	Незадовільно з можливістю повторного складання
0 – 34	F	Незадовільно з обов'язковим повторним вивченням дисципліни

8. Засоби навчання

Апаратне забезпечення, необхідне для вивчення навчальної дисципліни, включає персональний комп'ютер або ноутбук, підключені до локальної комп'ютерної мережі. Використовуються апаратні та програмні можливості лабораторій №130, №129 кафедри КТІБ ННІАЕ НУК.

Використовуються проспекти фірм-виробників обладнання та програмних засобів для криптографічного захисту інформації в телекомунікаційних мережах та системах, нормативно-правові документи, що знаходяться у спеціалізованих лабораторіях кафедри КТІБ.

9. Рекомендовані джерела інформації

Основні джерела інформації

1. Блінцов В. С., Гальчевський Ю. Л. Математичні основи криптології. – Миколаїв: НУК, 2006. – 232 с.
2. Самойленко Д. М. Динамічна текстова стеганографія. – Миколаїв: НУК, 2016. – 68 с.
3. Блінцов В.С., Гальчевський Ю.Л. Практикум з криптології // Навч. посібник. – Миколаїв: НУК, 2005. – 172 с.
4. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. [Текст] / Горбенко І.Д., Горбенко Ю.І. – Харків: Форт. – 2012, – 867 с.
5. Математичні основи криптографії: конспект лекцій / укладачі: В. А. Фільштинський, А. В. Бережний. – Суми: Сумський державний університет, 2011. – 138 с.
6. Стасюк, Марта. Елементи математичних основ криптографії: Навчальний посібник / Марта Стасюк – Львів: ЛДУ БЖД, 2021. – 216 с.
7. Стеганографія: навч. посібн. / О.О. Кузнецов, С.П. Євсєєв, О.Г. Король. – Харків: Вид. ХНЕУ, 2011. – 232 с.
8. В.Д. Бойко, М.Д. Василенко, В.М. Слатвінська Теорія інформації та кодування: навчально-методичні рекомендації. – Одеса: Видавничий дім «Гельветика», 2020. – 34 с.

Додаткові джерела інформації

1. Кожевников, В.Л. Теорія інформації та кодування [Текст]: навч. посібник / В.Л. Кожевников, А.В. Кожевников. – Д.: Національний гірничий університет, 2011. – 108 с.
2. Богуш В. М. Криптографічні застосування елементарної теорії чисел : Навч. посібник / Богуш В. М., Мухачов В. А. / Державний ун-т інформаційно-комунікаційних технологій. – К.: ДУІКТ, 2006. – 126с
3. Задірака В. К. Комп'ютерна криптологія : Підручник / Задірака В. К., Олексюк О. С. – Тернопільська академія народного господарства; НАН України; Інститут кібернетики ім. В.М.Глушкова. – К., 2002. – 504с.

4. Захист інформації. Криптографічні методи : Підруч. для вищ. навч. закл. / І. І. Маракова, А. І. Рибак, Ю. С. Ямпольський. – Одес. держ. Політехн. ун-т, Ін-т радіоелектрон. і телекомунікацій. – Одеса, 2001. – 174 с.

5. Термінологічний довідник з питань технічного захисту інформації / В. О. Хорошко, І. М. Огаркова, Д. В. Чирков та ін. ; за ред. проф. Хорошка В. О. – 3-тє вид., доп. і перероб. – К.: ТОВ "ПоліграфКонсалтинг", 2003. – 286 с.

Інформаційні ресурси мережі Інтернет

1. uaToken- українська система аутентифікації і захисту інформації
<http://www.uatoken.kiev.ua/>
2. <https://visualstudio.microsoft.com>
3. <https://www.python.org>
4. <https://www.openstego.com/>
5. <https://achorein.github.io/silenteye/>
6. https://embeddedsd.net/OpenPuff_Steganography_Home.html
7. <https://www.ghisler.ch/wiki/index.php/DarkCryptTC>

Доцент кафедри КТІБ,
к.т.н., доц.

_____ С.С. Козирєв