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

ЗАТВЕРДЖУЮ
Проректор з науково-педагогічної
роботи, к.т.н., доцент
_____ С.О. Слободян
«___» _____ 2023 р.

*РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ*

*Program of the Academic Discipline*

# Математичні основи криптографії та стеганографії

# *Mathematical foundations of cryptography and steganography*

Рівень вищої освіти перший (бакалаврський)
Тип дисципліни вибіркова
Мова викладання українська

Миколаїв – 2023

Робоча програма навчальної дисципліни «Математичні основи криптографії та стеганографії» є однією зі складових комплексної підготовки фахівців на першому (бакалаврському) рівні технічних спеціальностей.
«2» 02 2023 р. – 15 с.

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

Проєкт робочої програми навчальної дисципліни «Математичні основи криптографії та стеганографії» розглянуто на засіданні кафедри КТІБ.
Протокол від «2» 02 2023 р. № 7.

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

Проєкт робочої програми навчальної дисципліни «Математичні основи криптографії та стеганографії» розглянуто методичною комісією Навчально-наукового інституту автоматики і електротехніки.
Протокол від «14» 02 2023 р. № 6.

Голова, к.т.н., доцент _____ Д.О. Жук

Проєкт робочої програми навчальної дисципліни «Математичні основи криптографії та стеганографії» погоджено з навчальним відділом.

Начальник навчального відділу, к.т.н., доцент _____ А.В. Лабарткава

Робочу програму навчальної дисципліни «Математичні основи криптографії та стеганографії» затверджено Навчально-методичною радою НУК ім. адм. Макарова.
Протокол від «22» 02 2023 р. № 1.

Голова Навчально-методичної ради НУК ім. адм. Макарова,
д.т.н., професор _____ С.І. Трушляков

© Козирєв С.С., 2023 рік
© НУК, 2023 рік

## Анотація

Навчальна дисципліна «Математичні основи криптографії та стеганографії» є вибірковою навчальною дисципліною та забезпечує набуття знань з базових математичних основ аналізу та синтезу сучасних криптографічних та стеганографічних систем у відповідності до задач та вимог щодо захисту інформації.

В наш час використання та розробка криптографічних та стеганографічних систем захисту інформації є невід'ємною складовою науково-технічного процесу. Курс знайомить студентів з умовами стійкості шифрів, функціями хешування, криптосистемами, елементами теорії чисел. Ознайомлення студентів з математичними основами побудови сучасних криптографічних та стеганографічних систем, з їх призначенням та можливостями, а також областями функціонування дасть змогу обирати та розробляти більш надійні інформаційні системи, які на даний час широко використовуються в усіх науково-технічних галузях.

Отримані навички надають основу для подальшого освоєння методів побудови криптографічних та стеганографічних систем захисту інформації більш високого рівня.

Курс призначений для студентів всіх спеціальностей.



**Ключові слова:** криптографія, стеганографія, хеш-функції, стійкість шифрів.



## Abstract

The discipline "Mathematical foundations of cryptography and steganography" is a selective educational discipline and ensures the acquisition of knowledge of the basic mathematical foundations of the analysis and synthesis of modern cryptographic and steganographic systems in accordance with the tasks and requirements for information protection.

Nowadays, the use and development of cryptographic and steganographic information protection systems is an integral part of the scientific and technical process. The course introduces students to the strength conditions of ciphers, hashing functions, cryptosystems, and elements of number theory. Acquainting students with the mathematical foundations of building modern cryptographic and steganographic systems, with their purpose and capabilities, as well as with areas of their operation allows them to choose and develop more reliable information systems, which are currently widely used in all scientific and technical fields.

The acquired skills provide a basis for further mastering the methods of building cryptographic and steganographic information security systems of a higher level.

The course is intended for students of all majors.



**Keywords:** cryptography, steganography, hash functions, strength of ciphers.

**ЗМІСТ**

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 ..... 7
6. Методи навчання, засоби діагностики результатів навчання та методи їх демонстрування ..... 11
7. Форми поточного та підсумкового контролю ..... 12
8. Критерії оцінювання результатів навчання ..... 14
9. Засоби навчання ..... 14
10. Рекомендовані джерела інформації ..... 15

## 1. Опис навчальної дисципліни

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, напрям підготовки, освітньо-кваліфікаційний рівень</td><td colspan="2">Характеристика навчальної дисципліни</td></tr>
<tr><td>Денна форма навчання</td><td>Заочна форма навчання</td></tr>
<tr><td>Кількість кредитів – 5</td><td rowspan="3">–</td><td colspan="2">Вибіркова</td></tr>
<tr><td>Модулів – 1</td><td colspan="2">Рік підготовки</td></tr>
<tr><td>Змістових модулів – 2</td><td>1-й</td><td>–</td></tr>
<tr><td rowspan="6">Електронна адреса РПНД на сайті Університету<br>_____<br>Індивідуальне науково-дослідне завдання не передбачено</td><td rowspan="6">–</td><td colspan="2">Семестр</td></tr>
<tr><td>2-й</td><td>–</td></tr>
<tr><td colspan="2">Лекції</td></tr>
<tr><td>30 год.</td><td>–</td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td>–</td><td>–</td></tr>
<tr><td rowspan="2">Загальна кількість годин – 150</td><td rowspan="2">–</td><td colspan="2">Практичні</td></tr>
<tr><td>30 год.</td><td>–</td></tr>
<tr><td rowspan="5">Тижневих годин для денної форми навчання:<br>- аудиторних: 4;<br>- самостійної роботи: 6.</td><td rowspan="5">Рівень вищої освіти:<br>перший (бакалаврський)</td><td colspan="2">Самостійна робота</td></tr>
<tr><td>90</td><td>–</td></tr>
<tr><td colspan="2">Індивідуальне завдання не передбачено</td></tr>
<tr><td colspan="2">Вид контролю:<br>залік.</td></tr>
<tr><td colspan="2">Форма контролю:<br>усна, письмова.</td></tr>
</table>

Співвідношення кількості годин аудиторних занять до самостійної роботи становить:

- для денної форми навчання – 2:3.

## 2. Мета вивчення навчальної дисципліни

Метою вивчення навчальної дисципліни «Математичні основи криптографії та стеганографії» є набуття знань з базових математичних основ аналізу та синтезу сучасних криптографічних та стеганографічних систем у відповідності до задач та вимог щодо захисту інформації в професійній сфері. Формування у здобувачів вищої освіти відповідних компетентностей.

Компетентності та результати навчання :

- здатність застосовувати відповідний математичний апарат для вирішення завдань з захисту інформації у професійній сфері;
- здатність здійснювати раціональний вибір засобів забезпечення інформаційної безпеки телекомунікаційних систем з урахуванням пред'явлених до них вимог якості функціонування;
- знати моделі шифрів і математичні методи їх дослідження;
- знати методи побудови криптографічних та стеганографічних систем захисту інформації;
- уміти застосовувати математичні методи опису і дослідження криптографічних систем;

## 3. Передумови для вивчення навчальної дисципліни

Передумов для вивчення навчальної дисципліни «Математичні основи криптографії та стеганографії» немає.

## 4. Очікувані результати навчання

Програмні результати навчання полягають в наступному:

- знання елементів теорії чисел, основних алгоритмів і теорем, що використовуються в криптографії та стеганографії;
- знання методів модулярних обчислень, що використовуються в криптографії та стеганографії;
- знання методів обчислення в системі чисел з плаваючою точкою;
- знання умов стійкості шифрів, типів криптостійких систем;
- знання основних методів побудови криптосистем;
- уміння оцінювати криптостійкості систем;
- уміння здійснювати раціональний вибір криптографічних методів і засобів захисту інформації в телекомунікаційних системах.

## 5. Програма навчальної дисципліни

### Модуль 1

### Змістовий модуль 1. Елементи теорії чисел. Модулярні обчислення.

Тема 1. Елементи теорії чисел. Прості числа, визначення, перевірка на просте число. Теорема Ейлера. Теореми Ферма.

Тема 2. Основні алгоритми теорії чисел. Алгоритми Евкліда для багаточленів. Оцінка ефективності алгоритму.

Тема 3. Алгоритми факторизації. Оцінка ефективності алгоритмів.

Тема 4. Модулярні обчислення. Алгоритм ділення з остачею. Найбільший спільний дільник. Найменше спільне кратне. Методи розкладання на множники.

Тема 5. Генерація простих чисел. Класифікація алгоритмів генерування.

### Змістовий модуль 2. Математичні методи процесів шифрування.

Тема 6. Однонаправлені функції. Функції хешування, властивості, ступінь складності.

Тема 7. Псевдовипадкові послідовності в криптосистемах. Класифікація, основні методи побудови, оцінка якості.

Тема 8. Обчислення в системі чисел з плаваючою точкою. Похибки обчислень з плаваючою точкою.

Тема 9. Модель процесів шифрування-розшифрування.

Тема 10. Умови стійкості шифрів. Типи криптостійких систем. Оцінка криптостійкості систем.

**Тематичний план навчальної дисципліни**

| Назви змістових модулів і тем | Денна форма навчання | | | | | Заочна форма навчання | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Кількість годин | | | | | | | | | |
| | усього | у тому числі | | | | усього | у тому числі | | | |
| | | лек. | пр. | лаб. | с.р. | | лек. | пр. | лаб. | с.р. |
| **Змістовий модуль 1. Елементи теорії чисел. Модулярні обчислення.** | | | | | | | | | | |
| Тема 1. Елементи теорії чисел. Прості числа, визначення, перевірка на просте число. Теорема Ейлера. Теореми Ферма. | 20 | 4 | 4 | – | 12 | – | – | – | – | – |
| Тема 2. Основні алгоритми теорії чисел. Алгоритми Евкліда для багаточленів. Оцінка ефективності алгоритму. | 10 | 2 | 2 | – | 6 | – | – | – | – | – |
| Тема 3. Алгоритми факторизації. Оцінка ефективності алгоритмів. | 10 | 2 | 2 | – | 6 | – | – | – | – | – |
| Тема 4. Модулярні обчислення. Алгоритм ділення з остачею. Найбільший спільний дільник. Найменше спільне кратне. Методи розкладання на множники. | 20 | 4 | 4 | – | 12 | – | – | – | – | – |
| Тема 5. Генерація простих чисел. Класифікація алгоритмів генерування. | 15 | 3 | 3 | – | 9 | – | – | – | – | – |
| ***Разом за змістовим модулем 1*** | ***75*** | ***15*** | ***15*** | **–** | ***45*** | – | – | – | – | – |

| Назви змістових модулів і тем | Денна форма навчання | | | | | Заочна форма навчання | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Кількість годин | | | | | | | | | |
| | усього | у тому числі | | | | усього | у тому числі | | | |
| | | лек. | пр. | лаб. | с.р. | | лек. | пр. | лаб. | с.р. |
| **Змістовий модуль 2. Математичні методи процесів шифрування.** | | | | | | | | | | |
| Тема 6. Однонаправлені функції. Функції хешування, властивості, ступінь складності. | 20 | 4 | 4 | – | 12 | – | – | – | – | – |
| Тема 7. Псевдовипадкові послідовності в криптосистемах. Класифікація, основні методи побудови, оцінка якості. | 10 | 2 | 2 | – | 6 | – | – | – | – | – |
| Тема 8. Обчислення в системі чисел з плаваючою точкою. Похибки обчислень з плаваючою точкою. | 20 | 4 | 4 | – | 12 | – | – | – | – | – |
| Тема 9. Модель процесів шифрування-розшифрування. | 10 | 2 | 2 | – | 6 | – | – | – | – | – |
| Тема 10. Умови стійкості шифрів. Типи криптостійких систем. Оцінка криптостійкості систем. | 20 | 3 | 3 | – | 9 | – | – | – | – | – |
| ***Разом за змістовим модулем 2*** | ***75*** | ***15*** | ***15*** | – | ***45*** | – | – | – | – | – |
| **Разом за курсом** | **150** | **30** | **30** | – | **90** | – | – | – | – | – |

**Теми практичних занять**

| № | Назва теми | Кількість годин | |
|---|---|---|---|
| | | Денна форма навчання | Заочна форма навчання |
| **Змістовий модуль 1** | | | |
| 1 | Реалізація алгоритмів формування простого числа на мові програмування C++ або Python. Ймовірнісні алгоритми перевірки на простоту. | 4 | – |
| 2 | Реалізація алгоритму Евкліда для багаточленів. Оцінка ефективності алгоритму. | 2 | – |
| 3 | Реалізація алгоритмів факторизації на мові програмування C++ або Python. Оцінка ефективності. | 2 | – |
| 4 | Алгоритмічні структури повторення. Реалізація алгоритмів ділення з остачею, знаходження НСД, НСК. | 4 | – |
| 5 | Реалізація алгоритму генерації простих чисел на мові програмування C++ або Python. | 3 | |
| **Змістовий модуль 2** | | | |
| 6 | Хеш-функції. Побудова односпрямованої хеш-функції. Реалізація алгоритмів хешування. | 4 | – |
| 7 | Генератори псевдовипадкових чисел (ГПВЧ). Основні сфери застосування ГПВЧ. Застосування в криптографії. | 2 | – |
| 8 | Обчислення в системі чисел з плаваючою точкою. Способи машинної реалізації. | 4 | – |
| 9 | Модель процесів шифрування-розшифрування. Виконання шифрування та розшифрування. | 2 | – |
| 10 | Оцінка криптостійкості систем. Проведення оцінки криптографічної стійкості шифрів на основі порівняння множини ключів. | 3 | – |
| | **Разом** | **30** | |

За необхідністю можуть проводитись групові та індивідуальні консультації за розкладом кафедри в тому числі із застосуванням дистанційних технологій навчання. Це сприяє роз'ясненню найбільш складних питань дисципліни та підвищенню якості виконання завдань.

Практичні заняття проводяться в лабораторіях кафедри з використанням комп'ютерної техніки. Допускається виконання практичних завдань в дистанційному режимі із застосуванням персонального комп'ютерна за межами лабораторій кафедри.

## Самостійна робота

Самостійна робота здобувача вищої освіти є однією з форм організації навчання, основною формою оволодіння навчального матеріалу в час, вільний від обов'язкових навчальних занять.

Навчальний матеріал дисципліни, передбачений для засвоєння здобувачем вищої освіти в процесі самостійної роботи, включається в завдання поточного контролю разом із навчальним матеріалом, який опрацьовувався при проведенні навчальних занять.

*Денна форма навчання*

Розподіл годин самостійної роботи для денної форми навчання:

- підготовка до лекційних занять – 0,5 год. / 1 год. занять;
- підготовка та виконання практичних робіт – 3 год. /1 робота;
- підготовка до контрольних заходів – 10-15 год. на 1 захід.

*Заочна форма навчання*

Викладання навчальної дисципліни для здобувачів вищої освіти заочної форми навчання не передбачено.

## Завдання для самостійної роботи

| № | Вид роботи | Кількість годин | |
|---|---|---|---|
| | | Денна форма навчання | Заочна форма навчання |
| 1 | Підготовка до лекцій | 15 | – |
| 2 | Самостійне опрацювання окремих тем навчальної дисципліни | 15 | – |
| 3 | Виконання практичних робіт | 30 | – |
| 4 | Підготовка до модульних контрольних робіт | 30 | – |
| ***Усього годин за модуль 1 (разом за курсом)*** | | **90** | – |

## Індивідуальне науково-дослідне завдання

Виконання індивідуального науково-дослідного завдання робочою програмою не передбачено.

## 6. 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 цифрової стеганографії, їх закріплення;

- практична робота - вивчення в спеціалізованих лабораторіях методів і засобів цифрової стеганографії з використанням спеціального програмного забезпечення.

*Засобами* оцінювання результатів навчання є:

- звіти з практичних робіт;
- модульні контрольні роботи;
- залік.

*Методами* демонстрування результатів навчання є:

- усні відповіді;
- письмові відповіді;
- виконання завдань із застосуванням комп'ютерної техніки;
- оформлення звітів з практичних робіт;
- проходження поточного та підсумкового контролю.

Допускається застосування дистанційних технологій для діагностики результатів навчання.

## 7. 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.

*Поточний контроль* здійснюється в наступних формах:

- перевірка та проведення процедури захисту звітів з практичних робіт;
- проведення та перевірка модульних контрольних робіт;

*Підсумковий контроль* здійснюється в формі заліку – підсумкова оцінка формується як сума оцінок, отриманих в результаті поточного та підсумкового контролю і становить до 100 балів включно.

**Розподіл балів за формами контролю,**
**при яких результати навчання вважаються досягнутими**

| № | Форма контролю | Максимальна/мінімальна кількість балів | |
|---|---|---|---|
| | | Денна форма навчання | Заочна форма навчання |
| 1 | Перевірка та проведення процедури захисту звітів з практичних робіт | 60/36 | – |
| 2 | Проведення та перевірка модульних контрольних робіт (2 контрольні роботи) | 20/12 | – |
| 3 | Залік у формі тестування | 20/12 | – |
| | *Разом* | 100/60 | – |

| **Практична робота** | |
|---|---|
| Кількість балів | Критерії оцінювання |
| **6** | 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. |
| **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 при інтерпретації результатів допущено неточності. |
| **4** | Робота виконана з порушенням встановлених термінів. Студент виконує практичну роботу самостійно. складений звіт містить неточності у висновках. |
| **3** | Робота виконана з порушенням встановлених термінів. Студент виконує практичну роботу самостійно; складений звіт містить неточності у висновках та помилки. |
| **2** | Робота виконана з порушенням встановлених термінів. Складений звіт містить помилки, неточності у висновках та помилки. |
| **0** | Робота не виконана. |
| | *Максимальна кількість балів за даний компонент програми 60 балів (10 робіт по 6 балів).* |

**Поточний модульний контроль у формі тестування**

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

**Підсумковий контроль (залік у формі тестування)**

| Правильних відповідей, % | 100 | 90 | 80 | 70 | 60 | 50 | 40 | 30 | 20 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| Бал | 20 | 18 | 16 | 14 | 12 | 10 | 8 | 6 | 4 | 2 |

## 8. Критерії оцінювання результатів навчання

### Розподіл балів за змістовими модулями

| | | Вид роботи | Кількість балів |
|---|---|---|---|
| Змістовий модуль 1 | Тема 1 -7 | Практична робота № 1 | 6 |
| | | Практична робота № 2 | 6 |
| | | Практична робота № 3 | 6 |
| | | Практична робота № 4 | 6 |
| | | Практична робота № 5 | 6 |
| Поточний контроль | | Тестування | 10 |
| Змістовий модуль 2 | Тема 8-15 | Практична робота № 6 | 6 |
| | | Практична робота № 7 | 6 |
| | | Практична робота № 8 | 6 |
| | | Практична робота № 9 | 6 |
| | | Практична робота № 10 | 6 |
| Поточний контроль | | Тестування | 10 |
| Підсумковий контроль | | Залік у формі тестування | 20 |
| **Сума** | | | **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 |

## 9. Засоби навчання

Апаратне забезпечення, необхідне для вивчення навчальної дисципліни, включає персональний комп’ютер (настільний або ноутбук).

Системне програмне забезпечення, необхідне для вивчення навчальної дисципліни, включає операційну систему.

Прикладне програмне забезпечення, необхідне для вивчення навчальної дисципліни, що знаходяться у вільному доступі: Visual Studio Community Edition; Python. Текстовий процесор та редактор растрових зображень (для підготовки звітів з практичних робіт); pdf-, djv-переглядач (для ознайомлення з джерелами інформації, представленими в електронному вигляді).

## 10. Рекомендовані джерела інформації


*Основні:*

1. Жураковський Ю. П., Полторак В. П. Теорія інформації та кодування: Підручник. – К.: Вища шк., 2001. – 255 с.
2. Математичні основи криптографії: конспект лекцій / укладачі: В. А. Фільштінський, А. В. Бережний. – Суми: Сумський державний університет, 2011. – 138 с.
3. Кожевников, В.Л. Теорія інформації та кодування [Текст]: навч. посібник / В.Л. Кожевников, А.В. Кожевников. – Д.: Національний гірничий університет, 2011. – 108 с.
4. Стасюк, Марта. Елементи математичних основ криптографії: Навчальний посібник / Марта СТАСЮК – Львів: ЛДУ БЖД, 2021. – 216 с.

*Допоміжні:*

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.
6. Коробейников А. Г. Математичні основи криптографії: Навчальний посібник. – С. Пб: ГИТМО (ТУ), 2002. – 41 с.
7. В.Д. Бойко, М.Д. Василенко, В.М. Слатвінська Теорія інформації та кодування: навчально-методичні рекомендації. – Одеса: Видавничий дім «Гельветика», 2020. – 34 с.

*Інформаційні ресурси мережі Інтернет:*

1. Сайт персональних навчальних систем ХНЕУ ім. С. Кузнеця навчальної дисципліни “Математичні основи криптології” https://pns.hneu.edu.ua/course/view.php?id=5678
2. https://visualstudio.microsoft.com
3. https://www.python.org


Доцент кафедри КТІБ,
к.т.н., доцент _____ С.С. Козирєв