

**ДИСЦИПЛІНА «ПРОБЛЕМИ КОДУВАННЯ ТА ЗАХИСТУ ІНФОРМАЦІЇ»/
PROBLEMS OF CODING AND INFORMATION PROTECTION**

Анотація. Дисципліна «Проблеми кодування та захисту інформації» спрямована на вирішення основних задач передачі та захисту інформації від похибок та несанкціонованого доступу. Вона забезпечує оволодіння сучасними методами стискання, виправлення похибок та криптографічних перетворень інформації. Стискання та виправлення похибок даються оглядово. Криптографія включає криптографію з відкритими ключами: основні протоколи, цифровий підпис, геш-функції, блок-чейн технологію, методи автентифікації, біт-коін та інші криптовалютні системи.

Annotation of the discipline: The discipline «Fundamentals of coding and cryptography» is aimed at solving the basic problems of transmitting and protecting information from errors and unauthorized access. It provides mastery of modern methods of compression, error correction and cryptographic transformation of information. Error compression and correction are given in a reviewing manner. Cryptography includes public-key cryptography: core protocols, digital signature, hash functions, blockchain technology, authentication methods, bit-coin and other cryptocurrency systems..

Мета навчальної дисципліни: Метою курсу «Проблеми кодування та захисту інформації» є ознайомлення та вивчення здобувачами третього (освітньо-наукового) рівня вищої освіти сучасних методів передачі та захисту інформації шляхом її перетворення у цифровому форматі.

The purpose of the discipline. The purpose of the course "Fundamentals of Coding and Cryptography" is to familiarize and study by postgraduate students modern methods of information transmission and protection through its transformation in digital format..

Попередні вимоги. Аспірант повинен:

- знати: основні поняття і методи дискретної математики, теорії чисел, математичного аналізу, алгоритміки, структур даних, програмування;
- вміти: по опису перетворень створювати алгоритми і програми, що їх реалізують.

Prerequisites for mastering or choosing a course:

- Know: basic concepts and methods of discrete mathematics, number theory, mathematical analysis, algorithms, data structures, programming.
- Be able to create algorithms and programs that implement **describing transformations**.

Змістовні модулі:

- Частина 1. Коди виправлення помилок/ Part 1. Error correction codes.
- Частина 2. Криптографія з відкритим ключем/ Part 2. «Public-key cryptography».

Мова викладання: українська, англійська.

Рік підготовки, шифр навчальної дисципліни: друге півріччя другого року навчання, ДВА.3.02.05

Кількість кредитів: 4

Форма заключного контролю: іспит

Структура навчальної дисципліни: загальний обсяг 120 годин, у тому числі 24 години аудиторних занять (18 год. – лекційні заняття, 4 год. – практичні заняття, 2 години – консультація), 96 годин самостійної роботи.

Викладач: Анісімов Анатолій Васильович, д.ф.-м.н., проф., чл.-кор. НАН України, декан факультету комп'ютерних наук та кібернетики.

Інформація про викладача: <http://csc.knu.ua/uk/person/anisimov>.