

АНОТАЦІЯ
вибіркової дисципліни
«Математичні основи захисту інформації»

Метою вивчення навчальної дисципліни є формування у здобувачів вищої освіти системного розуміння математичних основ забезпечення конфіденційності, цілісності та доступності інформації, а також оволодіння базовими моделями, методами й алгоритмами захисту інформації, що застосовуються в інформаційних та інформаційно-аналітичних системах, у тому числі у сфері правоохоронної діяльності.

У межах дисципліни розглядаються основи криптографічного захисту інформації, зокрема елементи теорії чисел і дискретної математики, модульна арифметика, криптографічні перетворення, симетричні та асиметричні алгоритми шифрування, хеш-функції, електронний цифровий підпис, а також базові математичні підходи до оцінювання криптостійкості алгоритмів і надійності інформаційних систем. Особлива увага приділяється практичному застосуванню математичних методів у задачах захисту даних.

Очікувані результати навчання: у результаті вивчення навчальної дисципліни здобувач вищої освіти повинен:

Знати:

- основні поняття та терміни у сфері математичних основ захисту інформації;
- елементи теорії чисел і дискретної математики, що використовуються в криптографії;
- принципи побудови та функціонування симетричних і асиметричних криптографічних алгоритмів;
- математичні основи хешування, електронного цифрового підпису та управління криптографічними ключами;
- базові підходи до оцінювання криптостійкості та надійності засобів захисту інформації.

Вміти:

- застосовувати математичні методи для розв'язання типових задач захисту інформації;
- виконувати елементарні криптографічні перетворення та аналізувати їх властивості;
- обґрунтовувати вибір криптографічних алгоритмів залежно від умов практичної задачі;
- аналізувати ризики порушення інформаційної безпеки з використанням простих математичних моделей;
- використовувати набуті знання при проєктуванні та експлуатації захищених інформаційних систем

Зміст програмного матеріалу.

Тема 1. Вступ до захисту інформації та роль математичних методів.

Тема 2. Математичні основи криптографії.

Тема 3. Елементи теорії чисел і дискретної математики.

Тема 4. Класичні та симетричні методи шифрування.

Тема 5. Основи асиметричної криптографії.

Тема 6. Хешування, електронний цифровий підпис та управління ключами.

Тема 7. Оцінювання захищеності інформації та практичне застосування методів захисту.

Обсяг дисципліни 3 кредити ЄКТС (90 годин)

Форма контролю залік

Викладання навчальної дисципліни забезпечує кафедра інформаційних технологій.