

АНОТАЦІЯ  
навчальної дисципліни  
**СУЧАСНА КРИПТОГРАФІЯ**

Дисципліна «Сучасна криптографія» має на меті вивчення теорії інформаційної безпеки комп'ютерних систем, необхідної для їх надійного і безпечного функціонування, принципів захисту інформації, що передається віддаленим користувачам, від несанкціонованого доступу, криптографічних методів захисту інформації; набуття навичок розробки криптографічних протоколів та їх реалізації.

Зокрема, ознайомлення з методами і алгоритмами класичної криптографії, вивчення принципів інформаційної безпеки комп'ютерних систем, криптографічних методів захисту інформації, симетричних та асиметричних криптографічних систем, криптографічних протоколів, методів ідентифікації та автентифікації, генерації та перевірки цифрових підписів, генерації ключової інформації, протоколів застосування ключів та керування ними для забезпечення цілісності інформації, ознайомлення з комп'ютерними вірусами, їх типами та принципами дії.

Оволодіння знаннями та навичками в області сучасної криптографії стане основою розвинення професійних компетенцій майбутніх магістрів.

## **ОЧІКУВАНІ РЕЗУЛЬТАТИ НАВЧАННЯ**

У разі успішного завершення курсу студент зможе:

- використовувати криптографічні системи;
- застосовувати алгоритми симетричного шифрування до будь-якої інформації;
- застосовувати алгоритми асиметричного шифрування до будь-якої інформації;
- виконувати ідентифікацію та автентифікацію;
- генерувати криптографічні ключі;
- застосовувати технології розробки криптографічних протоколів;
- за допомогою існуючих (вбудованих) або розроблених криптографічних засобів виконувати безпечний інформаційний обмін.