4.1. Назва: **Асиметрична криптографія та криптосистеми з відкритим ключем** (системний аналіз).

4.2. Анотація навчальної дисципліни: навчальна дисципліна знайомить з теоретичними основами криптографії з відкритими ключами, асиметричними системами шифрування, системами цифрового підпису, автентифікації, різноманітними криптографічними протоколами, їх застосуванням у системах захисту інформації у різноманітних сферах, де використовуються інформаційні технології, а також з новими перспективними напрямками розвитку методів криптографічного захисту інформації.

4.3. Тип: дисципліна вільного вибору студента (за блоками).

4.4. Термін вивчення: 8-й семестр.

4.5. Кількість кредитів: 2 кредити.

4.6. ПІБ лектора: професор Савчук Михайло Миколайович.

4.7. Мета навчальної дисципліни: дати студентам знання в галузі криптографії з відкритим ключем. Дисципліна знайомить з теорією складності функцій та алгоритмів, важкооборотними функціями та їх застосуванням для побудови асиметричних криптосистем, різноманітними криптографічними протоколами, зокрема з протоколами автентифікації, цифрового підпису тощо. У курсі розглядаються приклади застосування криптографічних протоколів у електронній комерції. Значна увага приділена криптосистемам на еліптичних кривих.

4.8. Попередні вимоги: забезпечується курсами дискретна математика, алгебра та геометрія, теорія чисел, теорія імовірностей та математична статистика, теорія інформації та кодування, програмування та алгоритмічні мови, випадкові процеси, симетрична криптографія.

4.9. Методи викладання: заняття проводяться у формі лекцій.

5.0. Методи оцінювання: оцінюється за модульно-рейтинговою системою. Результати навчальної діяльності студентів оцінюються за 100-бальною шкалою і закінчуються заліком

5.1. Мова викладання: українська.