4.1. Назва: **Симетрична криптографія** (системний аналіз).

4.2. Анотація навчальної дисципліни: навчальна дисципліна знайомить з класичними шифрами, теорією Шеннона, криптографічними властивостями булевих функцій, сучасними блоковими та потоковими системами шифрування, принципами їх побудови та способами застосування.

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

4.4. Термін вивчення: 7-й семестр.

4.5. Кількість кредитів: 2 кредити.

4.6. ПІБ лектора: професор Савчук Михайло Миколайович.

4.7. Мета навчальної дисципліни: дати знання в галузі теоретичної криптографії та основ криптоаналізу симетричних криптосистем. Дисципліна знайомить з основними принципами роботи симетричних криптографічних систем, математичними моделями джерел інформації, поняттями теоретичної та практичної стійкості, цілком таємними криптосистемами. Конкретні типи алгоритмів симетричного шифрування та криптографічних перетворень розглядаються у відповідності з їх класифікацією на класичні шифри, механічні та електромеханічні шифрувальні машини, системи потокового шифрування, системи блокового шифрування.

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

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.