4.1. Название: **Асимметрическая криптография и криптосистемы с открытым ключём** (системный анализ).

4.2. Аннотация учебной дисциплины: учебная дисциплина знакомит с теоретическими основами криптографии с открытыми ключами, асимметричными системами шифрования, системами цифровой подписи, аутентификации, разнообразными криптографическими протоколами, их приложением в системах защиты информации в разнообразных сферах, где применяются информационные технологии, а также знакомит с новыми перспективными направлениями развития методов криптографической защиты информации.

4.3. Тип: дисциплина свободного выбора студента (по блокам).

4.4. Срок изучения: 8-й семестр.

4.5. Количество кредитов: 2 кредита.

4.6. ФИО лектора: профессор Савчук Михаил Николаевич.

4.7. Цель учебной дисциплины: дать студентам знания в отрасли криптографии с открытыми ключами. Дисциплина знакомит с теорией сложности функций и алгоритмов, односторонними функциями и их приложением для построения асимметричных криптосистем, разнообразными криптографическими протоколами, в частности, с протоколами аутентификации, цифровой подписи и другими. В курсе рассматриваются примеры применения криптографических протоколов в электронной коммерции. Значительное внимание уделено криптосистемам на эллиптических кривых.

4.8. Предварительные требования: обеспечивается курсами: дискретная математика, алгебра и геометрия, теория чисел, теория вероятностей и математическая статистика, теория информации и кодирования, программирование и алгоритмические языки, случайные процессы, симметричная криптография.

4.9. Методы преподавания: занятия проводятся в форме лекций.

5.0. Методы оценивания: оценивание по модульно-рейтинговой системе. Результаты учебной деятельности студентов оцениваются по 100-бальной шкале и заканчиваются зачетом.

5.1. Язык преподавания: украинский.