4.1. Название: **Симметричная криптография** (системный анализ)

4.2. Аннотация учебной дисциплины: учебная дисциплина знакомит с классическими шифрами, теорией Шеннона, криптографическими свойствами булевых функций, современными блочными и потоковыми системами шифрования, принципами их построения и способами применения.

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

4.4. Срок изучения: 7-й семестр.

4.5. Количество кредитов: 2 кредита.

4.6. ФИО лектора: профессор Савчук Михаил Николаевич.

4.7. Цель учебной дисциплины: дать знание в области теоретической криптографии и основ криптоанализа симметричных криптосистем. Дисциплина знакомит с основными принципами работы симметричных криптографических систем, математическими моделями источников информации, понятиями теоретической и практической стойкости, совершенно секретными криптосистемами. Конкретные типы алгоритмов симметричного шифрования и криптографических преобразований рассматриваются в соответствии с их классификацией на классические шифры, механические и электромеханические шифровальные машины, системы потокового шифрования, системы блочного шифровования.

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

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.