

## Аннотация дисциплины Б.1.1.28 Дисциплина. Методы и средства защиты компьютерной информации

Дисциплина "Методы и средства защиты компьютерной информации" изучается обучающимися по основной профессиональной образовательной программе "Разработка программных систем" направления подготовки "09.03.04 Программная инженерия".

Дисциплина изучается в 6 семестре. Общая трудоемкость дисциплины составляет 216/6 часов/з.ед. Самостоятельная работа заключается в выполнении работ, указанных в разделе 4.

В ходе изучения дисциплины осуществляется текущий контроль в форме технологии рейтингового контроля в соответствии с технологической карты дисциплины, размещенной на электронном курсе, а также промежуточный контроль в форме экзамен.

Целью изучения дисциплины является формирование следующих компетенций:

1. ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
2. ОПК-7 Способен применять в практической деятельности основные концепции, принципы, теории и факты, связанные с информатикой

В ходе изучения дисциплины последовательно рассматриваются темы:

1. Лекция №1. Понятие модели угроз. Классификация моделей угроз. Дисциплина МиСЗКИ как ответ на разрешимые формальные модели угроз. Традиционные нотации дисциплины. Отражение нотаций в УК РФ.
2. Лекция №2. Концепция симметричной криптографии. КС Цезаря: механическая нотация. КС Вижинера: нотация в терминах одномодульной системы вычетов. Виды ключей. Понятие криптоанализа. Атака на шифр Цезаря-Вижинера с короткопериодическим ключом. Результат К. Шеннона (1947).
3. Лекция №3. Генераторы случайных равномерно распределенных чисел. Физические датчики энтропии. Системотехнические принципы генерации равномерно распределенных чисел.
4. Лекция №4. ПСЧ и практически стойкие КС. Понятие практической стойкости. ГПСЧ: история, ЛКДПСЧ, выбор параметров ЛКДПСЧ.
5. Лекция №5. Асимметричные КС: идеи, свойства. Криптосистема RSA: принципы, генерация ключей, стойкость. Варианты использования. Идея ЭП.
6. Лекция №6. Понятие криптографической хеш-функции.
7. Лекция №7. Криптографические протоколы. Основной тезис. Классический метод перебора. Верификация криптографических протоколов. Пример: протокол аналогового голосования. Пример полной реализации механизма ЭП.
8. Лекция №8. Субъектно-объектный подход к анализу ВС. Теорема об отсутствии доверенных субъектов в ВС с архитектурой фон Неймана. Понятие доверенной аппаратной компоненты.
9. Лекция №9. Знакомство с концепцией и технологий TPM.

Основными стратегическими образовательными технологиями являются: лекционные занятия, практические и лабораторные занятия, процедуры самообучения.

В рамках указанных технологий применяются тактические образовательные технологии: задания, классическая лекция, проблемная лекция.