Аннотация рабочей программы дисциплины «Информационная безопасность»

Целью освоения дисциплины «Информационная безопасность» является формирование у студентов системы знаний в области информационной безопасности и применения на практике методов и средств защиты информации.

Задачи

- формирование умения обеспечить защиту информации и объектов информатизации;
- формирование умения составлять заявительную документацию в надзорные государственные органы инфокоммуникационной отрасли;
- формирование навыков выполнения работ в области технического регулирования, сертификации технических средств, систем, процессов, оборудования и материалов;
- формирование навыков обеспечения защиты объектов интеллектуальной собственности, результатов исследований и разработок как коммерческой тайны предприятия.

Содержание дисциплины:

1.Введение в информационную безопасность

1) Информационная безопасность. Основные понятия. Модели информационной безопасности.
2) Виды защищаемой информации.
3) Использование баз данных для нахождения и изучения нормативных документов в области информационной безопасности

2.Правовое обеспечение информационной безопасности

1) Основные нормативно-правовые акты в области информационной безопасности.
2) Правовые особенности обеспечения безопасности конфиденциальной информации и государственной тайны

3.Анализ способов нарушений информационной безопасности.

1) Анализ различных способов нарушений информационной безопасности.
2) Хакерские атаки, отказы оборудования в обслуживании, внешние факторы, влияющие прямо на информационную безопасность систем

3.Технические средства и методы защиты информации

1) Инженерная защита объектов.
2) Защита информации от утечки по техническим каналам.

4. Программно-аппаратные средства и методы обеспечения информационной безопасности

1) Основные виды сетевых и компьютерных угроз.
2) Средства и методы защиты от сетевых компьютерных угроз.
3) Создание удостоверяющего центра, генерация открытых и секретных ключей, создание сертификатов открытых ключей, создание электронной подписи, проверка электронной подписи.
4) Использование средств стеганографии для защиты файлов. Изучение настроек средств антивирусной защиты информации.

5. Криптографические методы защиты информации

1) Симметричные и ассиметричные системы шифрования.
2) Цифровые подписи (Электронные подписи).
3) Инфраструктура открытых ключей.
4) Криптографические протоколы.
5) Создание зашифрованных файлов и криптоконтейнеров и их расшифрование.
6) Создание защищенного канала связи средствами виртуальной частной сети.

Объем дисциплины – 3 з.е.

Форма промежуточного контроля – зачет