Аннотация рабочей программы дисциплины
направление подготовки 27.03.03 Системный анализ и управление

Дисциплина: Б1.В.ДВ.13.2 Информационная безопасность открытых систем

Цели освоения дисциплины:
Цель дисциплины - подготовка квалифицированных специалистов по вопросу защиты информации.
Задачи дисциплины - освоение студентами необходимых знаний, умений и навыков для защиты компьютерной информации.

Формируемые компетенции:
ОК-6 – способностью использовать общеправовые знания в различных сферах деятельности
ОПК-2 – способностью применять аналитические, вычислительные и системно-аналитические методы для решения прикладных задач в области управления объектами техники, технологии, организационными системами, работать с традиционными носителями информации, базам

Планируемые результаты обучения:
В результате изучения дисциплины студент должен:
Знать:
– принципы информационной безопасности;
– основные угрозы информационной безопасности;
– структуру коммерческой тайны предприятия;
– отличия между коммерческой тайной и интеллектуальной собственностью предприятия;
– методы и критерии оценки эффективности мероприятий по защите информации.
Уметь:
– различать правовые, организационные и технические мероприятия по защите информации;
– выявлять и классифицировать угрозы информационной безопасности предприятия;
– планировать мероприятия по защите информации, исходя из известных угроз и финансовых возможностей предприятия;
– рассчитывать эффективность мероприятий по защите информации.
Владеть навыками:
– работы в сети Интернет;
– борьбы с компьютерными вирусами;
– организации раздельного доступа к файлам и папкам на компьютере.

Содержание дисциплины:
Тема 1 Защита компьютерной информации: понятия и определения, назначения. Защита информации в ЭВМ, в вычислительных сетях, в автоматизированных системах обработки информации.
Тема 2 Угрозы безопасности и нарушители. Политика безопасности.

Тема 3 Модели и механизмы безопасности. Методы и принципы защиты информации.
Тема 4 Вторжения и их обнаружения. Уязвимости. Атаки и вторжения.
Тема 5 Криптографические модели.
Тема 6 Алгоритмы шифрования.
Тема 7 Идентификация и аутентификация пользователей.
Тема 8 Защита информации в сетях.
Тема 9 Стандарты безопасности. Требования к системам защиты информации.

Виды учебной работы: лекции, лабораторные занятия, самостоятельная работа.

Используемые образовательные технологии: традиционные и инновационные.

Формы текущего контроля успеваемости: отчеты по лабораторным работам, тестирование.

Формы промежуточной аттестации: зачет(8).

Трудоемкость дисциплины: 2 ЗЕ.