

Б1.Б.23 Безопасность сетей ЭВМ

Объем дисциплины (модуля) 7 ЗЕТ (252 час)

ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

Теоретическая и практическая подготовка выпускников в области построения сетей ЭВМ и обеспечения безопасности при эксплуатации сетей ЭВМ.

ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ

ОПК-2: Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности;

ОПК-2.2: Знает и применяет информационно-коммуникационные технологии, принципы организации информационных систем и сетей в соответствии с требованиями по защите информации для решения задач профессиональной деятельности

ОПК-2.3: Осуществляет меры противодействия нарушениям информационной безопасности с использованием различных программных и аппаратных средств защиты информации

ОПК-2.1: Знает аппаратные средства вычислительной техники, принципы построения информационных систем и сетей, принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации

ОПК-5: Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности;

ОПК-5.2: Применяет нормативные правовые акты и нормативные методические документы по информационной безопасности в профессиональной деятельности

ОПК(п)-2.2: Способен формировать предложения по оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы;

ОПК(п)-2.2.1: Знает методы деструктивных воздействия на информационные ресурсы

ОПК(п)-2.2.2: Знает методы оценки устойчивости объектов защиты к деструктивным воздействиям на информационные ресурсы

ОПК(п)-2.2.3: Формирует предложения по оптимизации структуры и функциональных процессов объекта защиты

В результате освоения дисциплины обучающийся должен

Знать: основы администрирования вычислительных сетей.

Уметь: формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе; осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты.

Владеть: методикой анализа сетевого трафика, результатов работы средств обнаружения вторжений; навыками выявления и уничтожения компьютерных вирусов.

СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Раздел 1. Основные понятия и анализ угроз информационной безопасности

Раздел 2. Политика информационной безопасности

Раздел 3. Криптографическая защита информации

Раздел 4. Идентификация, аутентификация и управление доступом

Раздел 5. Многоуровневая защита корпоративных информационных систем

Раздел 6. Протоколы защищенных каналов

Раздел 7. Технологии межсетевое экранирования

Раздел 8. Управление информационной безопасностью