Б1.Б.17 Программно-аппаратные средства защиты информации

Объем дисциплины (модуля) **6 ЗЕТ (216 час)**

ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)
Цель дисциплины: Подготовить обучающегося к деятельности, связанной с эксплуатацией и обслуживанием аппаратуры и оборудования, содержащего современные средства вычислительной техники для организации защиты информации. Задачи дисциплины: Получить представление о существующих программно-аппаратных средствах защиты информационных систем; умет устанавливать, кофигурировать и обслуживать программно-аппаратные средства информационных систем; получить представление о функционировании программных и аппаратных средств защиты информации в информационных системах.

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-2.1: 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-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-2.4: Формирует и настраивает политику безопасности распространенных операционных систем, а также локальных вычислительных систем, построенных на их основе
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-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
ОПК-2.3: Способен разрабатывать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности;
ОПК(п)-2.3.3: Разрабатывает, внедряет и сопровождает комплекс мер по обеспечению безопасности объектов защиты различных видов
ОПК-2.4: Способен проводить аудит защищенности объекта информатизации в соответствии с нормативными документами;
ОПК(п)-2.4.2: Знает и применяет нормативные документы в области аудита защищенности объекта информатизации
ОПК(п)-2.4.1: Применяет методики аудита защищенности объекта информатизации

В результате освоения дисциплины обучающийся должен

Знать: аппаратные средства вычислительной техники; принципы построения информационных систем; принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации.
Уметь: осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты; выбирать необходимые инструментальные средства для разработки программ в различных операционных системах и средах.
Владеть: методикой анализа сетевого трафика, результатов работы средств обнаружения вторжений; навыками выявления и уничтожения компьютерных вирусов; методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов.

СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)
Раздел 1. Защита информации в автоматизированных системах
Раздел 2. Управление доступом в компьютерных системах
Раздел 3. Защита информации от разрушающего воздействия вредоносных программ
Раздел 4. Обеспечение целостности информации
Раздел 5. Программно-аппаратные средства шифрования
Раздел 6. Защита современных информационных систем и сетей
Раздел 7. Защита информации в электронных платежных системах