

Аннотация рабочей программы дисциплины «Инженерно-техническая защита информации» для направления подготовки 09.03.01 Информатика и вычислительная техника, направленность (профиль) образовательной программы – Информатика и вычислительная техника

1. Цели и задачи освоения дисциплины

Цель дисциплины: Целью дисциплины является теоретическая и практическая подготовка студента к организации и проведению мероприятий по защите информации от утечки по техническим каналам на объектах информатизации, в выделенных помещениях.

Задачи дисциплины (модуля):

- изучение технических каналов утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами;
- изучение технических каналов утечки акустической (речевой) информации;
- изучение способов и средств защиты информации, обрабатываемой техническими средствами;
- изучение способов и средств защиты выделенных (защищаемых) помещений от утечки акустической (речевой) информации;
- освоение методов и средств контроля эффективности защиты информации от утечки по техническим каналам;
- освоение основ организации технической защиты информации на объектах информатизации.

2. Компетенции обучающегося, формируемые в результате освоения дисциплины

В процессе освоения данной дисциплины студент формирует и демонстрирует следующие профессиональные компетенции:

- способен обеспечивать информационную безопасность уровня баз данных (ПК-11);
- способен осуществлять администрирование безопасностью сетевых устройств и программного обеспечения; способен проводить регламентные работы на сетевых устройствах и программном обеспечении инфокоммуникационной системы (ПК-12).

В результате освоения дисциплины обучающийся должен демонстрировать следующие результаты образования:

знать: угрозы безопасности БД и способы их предотвращения, инструменты обеспечения безопасности БД и их возможности; знать архитектуру, устройство и функционирование вычислительных систем, коммуникационное оборудование, сетевые протоколы, методы обеспечения информационной безопасности.

уметь: выявлять угрозы безопасности на уровне БД, разрабатывать мероприятия по обеспечению безопасности на уровне БД; подготавливать протоколы мероприятий.

владеть: навыками анализа возможных угроз для безопасности данных, навыками выбора средств поддержки информационной безопасности на уровне БД; практическими навыками администрирования инфокоммуникационной системы, проведение регламентных работ на сетевых устройствах и программном обеспечении.

3. Содержание дисциплины

Особенности утечки информации по техническим каналам. Основные концептуальные положения защиты информации и главные аспекты информационной безопасности. Демаскирующие признаки объектов защиты информации. Акустическая разведка и звук. Способы и средства защиты информации от утечки по техническим каналам. Основные физические характеристики акустических волн и восприятие аудиоинформации человеком. Звуковое поле, создаваемое открытой с обеих сторон трубой, как физический базис групповых трубчатых направленных микрофонов. Методы и средства контроля эффективности технической защиты информации. Организация технической защиты информации.