

Аннотация рабочей программы дисциплины «Инженерно-техническая защита информации» для направления подготовки 09.03.01 Информатика и вычислительная техника
Направленность (профиль) образовательной программы – Автоматизированные системы обработки информации и управления

1. Цели и задачи дисциплины

Цель дисциплины: теоретическая и практическая подготовка студентов по вопросам защиты информации от утечки по инженерно-техническим каналам (техническая защита информации) на объектах информации и в выделенных помещениях.

Задачи дисциплины: 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

Вместе с другими дисциплинами ОП дисциплина «Инженерно-техническая защита информации» обеспечивает формирование следующих компетенций бакалавров:

Способность обеспечивать информационную безопасность уровня баз данных (ПК-11).

Способность 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:

знать угрозы безопасности БД и способы их предотвращения, инструменты обеспечения безопасности БД и их возможности; 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

Технические каналы утечки информации. Способы и средства защиты информации от утечки по техническим каналам. Методы и средства контроля эффективности технической защиты информации. Организация технической защиты информации.