

Аннотация к рабочей программе дисциплины

Автор: В.С Болотова

Наименование дисциплины: Б1.Б.1.28 Техническая защита информации

Цель освоения дисциплины:

- теоретически и практически подготовить студентов к организации и проведению мероприятий по выявлению возможных технических каналов утечки информации на объектах информатизации и в выделенных помещениях.

1. Требования к результатам освоения дисциплины:

Индекс и содержание компетенции	Знания	Умения	Навыки и (или) опыт деятельности
ОПК-8 - Способностью к освоению новых образцов программных, технических средств и информационных технологий	Этап 1 Новые образцы программных средств	Этап 1 Умения освоения новых образцов программных, технических средств и информационных технологий	Этап 1 Навыки работы с новой литературой по освоению новых образцов программных, технических средств и информационных технологий
ОПК-8 - Способностью к освоению новых образцов программных, технических средств и информационных технологий	Этап 2 Новые образцы технических средств информационных технологий	Этап 2 Умения классификации новых образцов программных, технических средств и информационных технологий	Этап 2 Навыки внедрения полученных знаний в профессиональной деятельности
ПК-17 - Способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации	Этап 1 Знать текущее состояние ИБ в организации с целью разработки требований к разрабатываемым процессам управления ИБ	Этап 1 Определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите	Этап 1 Навыки анализа информационной инфраструктуры автоматизированной системы и ее безопасности
ПК-17 - Способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации	Этап 2 Знать цели и задачи, решаемые разрабатываемыми процессами управления ИБ	Этап 2 Оценивать информационные риски в автоматизированных системах	Этап 2 Навыки и метод мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем, методы оценки информационных рисков

2. Содержание дисциплины:

Раздел 1 Основные понятия и определения.

Тема 1 Термины и определения в области технической защиты информации.
Тема 2 Классификация технических каналов утечки информации.
Раздел 2 Технические каналы утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами.
Тема 3 Общая характеристика и классификация технических каналов утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами.
Тема 4 Акустические (речевые) каналы утечки информации.
Тема 5 Оптические каналы утечки информации.
Тема 6 Радиоэлектронные каналы утечки информации.
Тема 7 Материально-вещественные каналы утечки информации.
Раздел 3 Системный подход к инженерно-технической защите информации.
Тема 8 Способы и средства защиты информации, обрабатываемой средствами вычислительной техники и автоматизированными системами.
Тема 9 Способы и средства защиты выделенных помещений от утечки речевой информации по техническим каналам.
Тема 10 Методы и средства контроля эффективности технической защиты информации, обрабатываемой средствами вычислительной техники и автоматизированными системами.
Тема 11 Методы и средства контроля эффективности защиты выделенных помещений от утечки речевой информации по техническим каналам.
Тема 12 Методы и средства выявления электронных устройств негласного получения информации.
Раздел 4 Основные этапы проектирования системы защиты информации техническими средствами.
Тема 13 Организация технической защиты информации.
Тема 14 Лицензирование деятельности по технической защите информации.

3. Общая трудоёмкость дисциплины: 4 ЗЕ