

Программа повышения квалификации

«Основные аспекты защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну»

Продолжительность: 5 дней (72 академических часа, из них 40 часов – аудиторные занятия, 32 часа – самостоятельная подготовка по выданным учебным материалам).

Категория слушателей – руководители и специалисты, работающие в области технической защиты информации (ТЗИ).

Содержание программы

Тема 1. Планирование и организация работ по ТЗИ

1. Цели и задачи ТЗИ

- 1.1. Правовые основы защиты информации.
- 1.2. Документы в области технического регулирования и стандартизации.
- 1.3. Ответственность за правонарушения в области защиты информации.

2. Защищаемые информационные ресурсы.

- 2.1. Понятие защищаемой информации. Объект защиты
- 2.2. Понятие, классификация и технологии построения информационных систем.

3. Угрозы безопасности информации.

- 3.1. Понятие и классификация угроз безопасности информации
- 3.2. Методы определения возможных способов реализации угроз безопасности информации и последствий от их реализации
- 3.3. Модель угроз безопасности информации.

4. Методы выявления и оценки возможности реализации угроз безопасности информации.

- 4.1. Анализ угроз безопасности информации и уязвимостей программного обеспечения с помощью банка данных угроз безопасности информации.
- 4.2. Разработка модели угроз безопасности информации, обрабатываемой в автоматизированной системе.

5. Организация работ по ТЗИ.

- 5.1. Планирование работ по ТЗИ.
- 5.2. Требования по защите информации и созданию системы защиты информации.
- 5.3. Создание и функционирование системы защиты информации ограниченного доступа.

6. Разработка технического задания на создание системы защиты информации.

- 6.1. Основные разделы ТЗ.
- 6.2. Заполнение ТЗ.

7. Обеспечение безопасности критической информационной инфраструктуры.

- 7.1. Нормативно-правовые акты и методические документы в области безопасности КИИ.
- 7.2. Правила и порядок категорирования объектов КИИ. Определение объектов, подлежащих категорированию. Определение значимости объектов КИИ.
- 7.3. Ответственность за нарушение мер, правил и требований по обеспечению безопасности КИИ.

Тема 2. Выполнение мероприятий по ТЗИ и применение технических средств в интересах ТЗИ

8. Меры и средства ТЗИ.

- 8.1. Основные меры, способы и средства защиты информации от утечки по техническим каналам.
- 8.2. Основные меры, способы и средства защиты информации от НСД.
- 8.3. Основные меры, способы и средства защиты информации от программно-математических воздействий (ПМВ).

9. Разработка организационно-распорядительных документов по ТЗИ.

10. Персонал предприятия как фактор риска утечки защищаемой информации.

- 10.1. Угрозы информационной безопасности предприятия, исходящие от персонала.
- 10.2. Технические и программные средства обеспечения информационной безопасности предприятия.
- 10.3. Мониторинг профилей персонала предприятия в социальных сетях и сети Интернет с целью противодействия деструктивным действиям персонала.
- 10.4. Возможности DLP-систем для контроля информационных потоков на предприятии, электронной переписки, нарушения политики безопасности.
- 10.5. Проведение расследований и предупреждение противоправных действий с использованием возможностей DLP-систем.

11. Порядок применения средств защиты информации.

- 11.1. Порядок применения средств защиты информации, обрабатываемой техническими средствами, от утечки за счет ПЭМИН.
- 11.2. Порядок применения средств защиты акустической речевой информации от утечки по техническим каналам.
- 11.3. Порядок применения средств защиты информации от НСД.

Тема 3. Контроль состояния ТЗИ

12. Организация контроля и оценка состояния ТЗИ.

- 12.1. Основы организации контроля состояния ТЗИ.
- 12.2. Методы и средства контроля защищенности информации.

13. Аттестация объектов информатизации по требованиям безопасности информации.

- 13.1. Порядок проведения работ по аттестации объектов информатизации.
- 13.2. Типовое содержание аттестационных испытаний автоматизированной системы (АС).
- 13.3. Типовое содержание аттестационных испытаний защищаемого помещения (ЗП).
- 13.4. Документы по результатам аттестационных испытаний.
- 13.5. Сертификация средств защиты информации.

14. Итоговая аттестация.

При успешном прохождении итоговой аттестации по данной программе слушателям выдается **Удостоверение о повышении квалификации.**