Приложение
к приказу от 09. 02. 2016 № 22

Рекомендуемые темы квалификационных работ
по программе профессиональной переподготовки
«Информационная безопасность»

1. Особенности формирования требований к системе защиты информации в государственной информационной системе, содержащей персональные данные.
2. Особенности формирования требований к системе защиты информации в иных информационных системах персональных данных.
3. Разработка Частной модели угроз безопасности информации для территориального сегмента государственной информационной системы, отнесенной к ключевой системе информационной инфраструктуры.
4. Формирование требований по защите информации для территориального сегмента государственной информационной системы, отнесенной к ключевой системе информационной инфраструктуры.
5. Разработка организационно-распорядительного документа по защите информации, определяющего правила и процедуру управления (администрирования) системой защиты информации территориального сегмента государственной информационной системы.
6. Разработка организационно-распорядительного документа по защите информации, определяющего правила и процедуру выявления инцидентов информационной безопасности и реагирование на них в территориальном сегменте государственной информационной системы.
7. Разработка организационно-распорядительного документа по защите информации, определяющего правила управления конфигурацией аттестованной информационной системы и системы защиты информации в территориальном сегменте государственной информационной системы.
8. Разработка организационно-распорядительного документа по защите информации, определяющего правила и процедуру контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в территориальном сегменте государственной информационной системы.
9. Разработка организационно-распорядительного документа по защите информации, определяющего правила и процедуры защиты информации при выводе из эксплуатации территориального сегмента государственной информационной системы или принятии решения об окончании обработки информации.
10. Разработка Положения о порядке организации и проведения работ по защите конфиденциальной информации в организации (органе власти).
11. Структура, задачи и функции объектовой системы защиты информации. Требования к специалистам по технической защите информации.

12. Особенности формирования требований по защите персональных данных при их обработке в государственной информационной системе.
13. Требования по защите речевой конфиденциальной информации от ее утечки по техническим каналам. Порядок проведения организационных и технических мероприятий по созданию защищаемого помещения.
14. Порядок проведения организационных и технических мероприятий по защите конфиденциальной информации от ее утечки по техническим каналам и за счет несанкционированного доступа в иной (негосударственной) информационной (автоматизированной) системе.
15. Порядок проведения организационных и технических мероприятий по обеспечению безопасности персональных данных при их обработке в иной (негосударственной) информационной (автоматизированной) системе.
16. Порядок проведения мероприятий по аттестации распределенной государственной информационной системы, содержащей информацию ограниченного доступа, на соответствие обязательным требованиям.
17. Состав и содержание работ по оценке эффективности системы защиты персональных данных в иных (негосударственных) информационных системах персональных данных.
18. Особенности проведения работ по выбору и внедрению средств защиты информации в государственных информационных системах.
19. Особенности проведения работ по выбору и внедрению средств защиты информации в иных информационных системах персональных данных.
20. Защита информации ограниченного доступа от программно-математических воздействий и иных уязвимостей программных средств.
21. Защита информации при подключении информационных систем общего пользования к международной компьютерной сети «Интернет».
22. Ответственность за правонарушения в области защиты информации. Виды и формы правонарушений, потенциально возможные в вашей организации.
23. Особенности стандартизации и сертификации средств технической защиты информации и защищенных систем обработки информации, применяемых в вашей организации.
24. Методы и средства выявления угроз, реализуемых по техническим каналам утечки информации ограниченного доступа применительно к вашей организации.
25. Характеристика программно-математических воздействий и вредоносных программ, которым могут быть подвержены информационные системы в вашей организации.
26. Методы и средства выявления угроз несанкционированного доступа к информации и специальных воздействий на неё применительно к вашей организации.

27. Программно-технические способы и средства защиты информации от несанкционированного доступа при межсетевом взаимодействии и взаимодействии с информационными сетями общего пользования применительно к вашей организации.
28. Порядок организации и содержание мероприятий аттестации объектов информатизации по требованиям безопасности информации применительно к вашей организации.
29. Способы и средства технической защиты информации при её передаче по каналам связи применительно к вашей организации.
30. Порядок и механизм применения инфраструктуры открытых ключей (PKI) для защиты информации, передаваемой по компьютерным сетям применительно к вашей организации.
31. Криптографические способы и средства защиты информации, применяемые в вашей организации.

Примечание: текст «к вашей организации» необходимо заменить на название организации. Например, «применительно к межрайонной налоговой инспекции».

Проректор по учебной и научной работе И.В. Кожанова