Приложение №3
УТВЕРЖДЕНО
Приказом Приволжского института
повышения квалификации ФНС России
от _____г. № ___

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. Формирование требований по защите информации для территориального сегмента государственной информационной системы.
4. Разработка организационно-распорядительного документа по защите информации, определяющего правила и процедуру управления (администрирования) системой защиты информации территориального сегмента государственной информационной системы.
5. 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.
6. Разработка организационно-распорядительного документа по защите информации, определяющего правила управления конфигурацией аттестованной информационной системы и системы защиты информации в территориальном сегменте государственной информационной системы.
7. 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.
8. 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.
9. Структура, задачи и функции объектовой системы защиты информации. Требования к специалистам по технической защите информации.
10. Требования по защите речевой конфиденциальной информации от ее утечки по техническим каналам. Порядок проведения организационных и технических мероприятий по созданию защищаемого помещения.
11. Порядок проведения организационных и технических мероприятий по защите конфиденциальной информации от ее утечки за счет несанкционированного доступа в иной (негосударственной) информационной системе.

12. Порядок проведения организационных и технических мероприятий по обеспечению безопасности персональных данных при их обработке в иной (негосударственной) информационной системе.

13. Порядок проведения мероприятий по аттестации распределенной государственной информационной системы, содержащей информацию ограниченного доступа, на соответствие обязательным требованиям.

14. Состав и содержание работ по оценке эффективности системы защиты персональных данных в иных (негосударственных) информационных системах персональных данных.

15. Особенности проведения работ по выбору и внедрению средств защиты информации в государственных информационных системах.

16. Особенности проведения работ по выбору и внедрению средств защиты информации в иных информационных системах персональных данных.

17. Защита информации ограниченного доступа от программно-математических воздействий и уязвимостей программных средств.

18. Защита информации при подключении информационных систем общего пользования к международной компьютерной сети «Интернет».

19. Особенности стандартизации и сертификации средств технической защиты информации и защищенных систем обработки информации, применяемых в вашей организации.

20. Методы и средства выявления угроз, реализуемых по техническим каналам утечки информации ограниченного доступа, потенциально возможных в организации.

21. Характеристика программно-математических воздействий и вредоносных программ, которым могут быть подвержены средства вычислительной техники и информационные системы в организации.

22. Методы и средства выявления угроз несанкционированного доступа к информации и специальных воздействий на неё применительно к вашей организации.

23. Программно-технические способы и средства защиты информации от несанкционированного доступа при межсетевом взаимодействии и взаимодействии с информационными сетями общего пользования применительно к вашей организации.

24. Порядок организации и содержание мероприятий аттестации объектов информатизации по требованиям безопасности информации применительно к вашей организации.

25. Способы и средства технической защиты информации в компьютерных сетях.

26. Способы применения средств межсетевого экранирования для защиты информации от несанкционированного доступа.

27. Порядок и механизм применения инфраструктуры открытых ключей (PKI) для защиты информации в организации.

28. Способы и средства криптографической защиты информации при её передаче по компьютерным сетям.

29. Разработка виртуальной защищенной сети организации на базе программного обеспечения ViPNet (или аналогичного программного обеспечения).

30. Порядок использования средств криптографической защиты информации в организации.

31. Оценка защищенности помещения хозяйствующего субъекта (на конкретном примере) от утечки речевой конфиденциальной информации по акустическому и виброакустическому каналам.

32. Организация безопасного удаленного доступа к ЛВС организации, предприятия.

33. Оценка эффективности применения средств и методов защиты информации на предприятии.

34. Применение DLP-систем как инструмента обеспечения информационной безопасности в организации.

35. Управление инцидентами информационной безопасности с использованием возможностей DLP-систем и средств активного аудита.

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

Проректор по учебной работе И.В. Кожанова