Приложение № 2
УТВЕРЖДЕНО
Приказом Приволжского института
повышения квалификации ФНС России
от 11.01.2023 № 2

Рекомендуемые темы выпускных квалификационных работ по программе профессиональной переподготовки «Информационная безопасность. Обеспечение защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, некриптографическими и криптографическими методами»

1. Формирование требований по защите информации для территориального сегмента государственной информационной системы.
2. Разработка организационно-распорядительного документа по защите информации, определяющего правила и процедуру управления (администрирования) системой защиты информации территориального сегмента государственной информационной системы.
3. 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.
4. Разработка организационно-распорядительного документа по защите информации, определяющего правила управления конфигурацией аттестованной информационной системы и системы защиты информации в территориальном сегменте государственной информационной системы.
5. 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.
6. 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.
7. Структура, задачи и функции объектовой системы защиты информации. Требования к специалистам по технической защите информации.
8. Требования по защите речевой конфиденциальной информации от ее утечки по техническим каналам. Порядок проведения организационных и технических мероприятий по созданию защищаемого помещения.
9. Порядок проведения организационных и технических мероприятий по защите конфиденциальной информации от ее утечки за счет несанкционированного доступа в иной (негосударственной) информационной системе.
10. Порядок проведения организационных и технических мероприятий по

обеспечению безопасности персональных данных при их обработке в иной (негосударственной) информационной системе.

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

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

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

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

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

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

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

18. Способы и средства выявления угроз несанкционированного доступа к информации и специальных воздействий на неё применительно к *вашей организации*.

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

20. Порядок организации и содержание мероприятий аттестации объектов информатизации по требованиям безопасности информации на примере *вашей организации.*

21. Способы и средства криптографической защиты информации, применяемые в компьютерных сетях.

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

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

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

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

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

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

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

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

30. Развертывание удостоверяющего центра на ОС UNIX (Linux) с использованием сертифицированных ФСБ криптосредств.

31. Использование защитных механизмов, встроенных в ОС GNU\Linux, для защиты информации в организации.

32. Способы и средства обнаружения несанкционированного доступа к информации, обрабатываемой в информационных системах.

33. Перспективы и инновации в технологиях криптографической защиты информации.

34. Порядок получения, ввод в эксплуатацию и использование средств криптографической защиты информации в организации.

35. Ответственность за правонарушения в области защиты информации. Виды и формы правонарушений, потенциально возможные в *вашей организации*.

36. Правонарушения в сфере защиты конфиденциальной информации, особенности их выявления в рамках служебных полномочий.

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

Проректор по учебной работе И.В. Кожанова