ПРИЛОЖЕНИЕ 5

Аннотация государственной итоговой аттестации

Трудоемкость в зачетных единицах	**8 семестр – 6**
Часов (всего) по учебному плану	**216**
включая: подготовку к процедуре защиты и процедуру защиты выпускной квалификационной работы	 8 семестр – 216 часов

Цель государственной итоговой аттестации: оценка подготовленности обучающегося к решению задач профессиональной деятельности.

Примерная тематика выпускных квалификационных работ:

1. Защита информации в концепции стандарта ГОСТ Р 27001-2006 (на примере общественной организации);
2. Защита интеллектуальной собственности в организации;
3. Сертификация СМИБ по стандарту ГОСТ Р ИСО/МЭК 27001;
4. Аттестация системы информационной безопасности государственной информационной системы;
5. Разработка программного обеспечения выделения агрегатов рисков по общим угрозам, уязвимостям и активам;
6. Имитационное моделирование сценариев рисков информационной безопасности;
7. Мониторинг состояния объекта на основе оценки рисков;
8. Автоматизированный выбор мер и средств контроля и управления по заданным рискам с использованием нейронных сетей;
9. Моделирование рисков информационной безопасности в информационных системах, построенных по технологии блокчейн;
10. Инвентаризация и классификация информационных активов организации при оценке рисков;
11. Оценка и анализ рисков с использованием программного обеспечения CORAS;
12. Организация режима защиты конфиденциальной информации на предприятии государственного сектора экономики;
13. Моделирование угроз персональным данным в организации;
14. Обеспечение безопасности информации на объектах критической информационной инфраструктуры;
15. Инструментальные проверки персонала организации, использующего в работе конфиденциальную информацию;
16. Организация расследования инцидентов информационной безопасности на предприятии;
17. Организация специальных инструментальных проверок персонала для противодействия инсайдерству в финансовом учреждении (на предприятии энергетики);
18. Разработка проекта технической защиты конфиденциальной информации на предприятии от ее утечки по (конкретный вид) каналу;
19. Разработка проекта технической защиты информации на автоматизированном рабочем месте от ее утечки по (конкретный вид) каналу;

20. Проектирование системы охранного видеонаблюдения организации с использованием профессиональных графических инструментов;

21. Оценка защищенности помещения организации от утечки речевой конфиденциальной информации по акустическому (виброакустическому) каналу;

22. Оценка защищенности помещения организации от утечки речевой конфиденциальной информации по каналу электроакустических преобразований;

23. Оценка защищенности технических средств и систем организации, предназначенных для обработки, хранения и передачи по линиям связи конфиденциальной информации;

24. Оценка защищенности конфиденциальной информации организации, обрабатываемой в ТСПИ от утечки за счет наводок;

25. Разработка программы специального обследования по выявлению электронных устройств негласного получения информации в защищаемом помещении предприятия;

26. Разработка программы специального обследования по выявлению временно отключенных электронных устройств негласного получения информации в защищаемом помещении предприятия;

27. Разработка программы проведения радиомониторинга в защищаемом помещении организации;

28. Разработка программы специального обследования защищаемого помещения (кабинета, переговорной комнаты, конференц-зала и т.д.) предприятия (организации);

29. Разработка проекта технической защиты информации в кабинете руководителя организации от утечки по (конкретный вид) каналу;

30. Разработка технического задания на систему защиты информации в переговорной комнате (конференц-зале) организации от утечки по (конкретный вид ТКУИ) каналу;

31. Разработка программы специальной проверки технических средств и систем организации, обрабатывающих конфиденциальную информацию;

32. Разработка программы специального исследования защищенности ТСПИ и ВТСС в кабинете руководителя от утечки опасных сигналов ПЭМИН;

33. Внедрение методов и способов организации автоматизированного пропускного режима на предприятии;

34. Разработка программы специального исследования защищенности средств ВТСС в конференц-зале от утечки речевой информации по акустоэлектрическому каналу;

35. Разработка программы проведения аттестационных испытаний по оценке защищенности переговорной комнаты (конференц-зала и т.д.) от утечки информации по акустическому (виброакустическому, акустоэлектрическому, электроакустическому) каналу;

36. Разработка программы проведения аттестационных испытаний по оценке защищенности автоматизированного рабочего места от утечки информации по электромагнитному каналу;

37. Оценка защищенности автоматизированного рабочего места от утечки конфиденциальной информации по каналу ПЭМИ считывателя SD-карт;

38. Оценка защищенности АРМ от утечки конфиденциальной информации по каналу ПЭМИ матрицы монитора;

39. Оценка защищенности автоматизированного рабочего места от утечки конфиденциальной информации по каналу ПЭМИ при применении средств активной защиты;

40. Исследование уязвимостей системы радиотехнической идентификации систем и объектов;

41. Оценка защищенности помещения от утечки речевой информации по линиям охранно-пожарной сигнализации;

42. Разработка технического проекта создания защищаемого помещения в организации;

43. Разработка технического проекта системы защиты информации организации от утечки по постоянно действующим каналам связи;

44. Разработка программы проведения специального обследования помещения организации по выявлению акустопараметрического канала утечки информации;

45. Оценка защищенности планшетных компьютеров от утечки конфиденциальной информации по каналу ПЭМИ;

46. Разработка проекта системы защиты конфиденциальной информации в организации;

47. Разработка предложений по повышению защищенности вычислительной техники по каналу ПЭМИ пассивными методами;

48. Разработка рекомендаций по защите конфиденциальной информации от утечки по акустическому каналу из защищаемого помещения пассивными методами;

49. Разработка алгоритма поиска сигналов со сложными структурами в процессе радиомониторинга;

50. Разработка технического задания на проведение поисковых работ по обнаружению скрытых неизлучающих устройств утечки информации;

51. Автоматизация процесса подготовки отчетных документов по результатам проведения инструментального контроля уровня защищенности автоматизированного рабочего места;

52. Анализ методов обеспечения информационной безопасности в беспроводных сетях передачи информации;

53. Администрирование систем безопасности сетевого взаимодействия на основе технологии VPN;

54. Администрирование локальной вычислительной сети организации при использовании сервисов и ресурсов сети интернет;

55. Защита файлового архива организации средствами операционной системы;

56. Защита беспроводных подключений к локальной вычислительной сети при использовании точек доступа общего пользования;

57. Защита сетевого хранилища организации;

58. Разработка комплекса правил, процедур и практических приемов защиты информации в мобильных устройствах;

59. Администрирование программно-аппаратного комплекса «Аккорд» на рабочих станциях организации;

60. Программная защита информационной системы организации на основе возможностей операционной системы;

61. Организация программной защиты сервера с использованием возможностей ОС Microsoft Windows;

62. Разработка и внедрение электронной подписи в документооборот организации;

63. Обеспечение безопасности сетевого взаимодействия с использованием технологии OpenVPN;

64. Защита локальной вычислительной сети организации от несанкционированного доступа к её ресурсам с использованием маршрутизаторов уровня локальных сетей;

65. Защита информации в вычислительной сети организации с использованием возможностей провайдеров;

66. Применение межсетевых экранов экспертного уровня для защиты ресурсов локальной вычислительной сети в организации;

67. Администрирование системы резервного копирования для защиты информационных активов организации;

68. Внедрение системы антивирусной защиты в организации;

69. Защита сетевого хранилища средствами QNAP NAS от несанкционированного доступа и нарушения целостности данных;

70. Защита сетевого хранилища средствами Synology NAS от несанкционированного доступа и нарушения целостности данных;

71. Организация программной защиты файлового сервера с использованием возможностей операционной системы AstraLinux;

72. Организация программной защиты веб-сервера с использованием возможностей операционной системы AstraLinux;

73. Организация программной защиты файлового сервера с использованием возможностей операционной системы ALT Linux;

74. Организация программной защиты веб-сервера с использованием возможностей операционной системы ALT Linux;

75. Администрирование программно-аппаратного комплекса «Соболь» на рабочих станциях в организации;

76. Защита локальной вычислительной сети организации с использованием IDS/IPS систем;

77. Диагностика стеганографических возможностей и противодействие им при реализации информационных процессов в организации;

78. Разработка средств автоматизации для настройки средств защиты информации от несанкционированного доступа;

79. Разработка средств автоматизации для контроля защищенности автоматизированных систем по требованиям безопасности информации;

80. Разработка средств автоматизации для исследования программного обеспечения по требованиям безопасности информации;

81. Разработка системы диагностики наличия вредоносного программного обеспечения («в локальной сети организации» или «на сетях IoT-устройств» или «в промышленной сети организации»;

82. Обеспечение безопасного подключения рабочих станций (название организации), обрабатывающих конфиденциальную информацию, к сети Интернет;

83. Применение систем контроля и управления процессами («вывода на печать» или «вывода на внешние носители информации» или «отправки файлов через интернет» или «отправки файлов по электронной почте») в (название организации);

84. Защита от несанкционированных проводных подключений к локальной сети (название организации);

85. Организация аудита информационной безопасности организации с использованием специального программного обеспечения;

86. Применение технологии активного аудита информационной безопасности в организации;

87. Внедрение технологий предотвращения утечки информации (DLP-системы) в организации;

88. Внедрение технологии управления информацией и событиями безопасности (SIEM-системы) в организации;

89. Автоматизация процессов менеджмента информационной безопасности в организации;

90. Внедрение системы предотвращения утечки информации в финансово-кредитном учреждении;

91. Внедрение системы сбора и корреляции событий информационной безопасности в финансово-кредитном учреждении;

92. Организация центра управления информационной безопасностью в финансово-кредитном учреждении;

93. Внедрение системы мониторинга информационной безопасности в финансово-кредитном учреждении;

94. Расследование инцидентов информационной безопасности в организации;
95. Проведение аудита информационной безопасности организации с использованием сканера безопасности;
96. Аудит безопасности локальной вычислительной сети организации с использованием сканера безопасности;
97. Защита информации с использованием методов и технологий упрощенной криптографии в организации;
98. Криптографические способы контроля целостности и их практическая реализация;
99. Асимметричные криптосистемы и методы обеспечения конфиденциальности при их использовании;
100. Моделирование уязвимостей протоколов защиты TLS;
101. Моделирование уязвимостей протоколов защиты SSL;
102. Моделирование уязвимостей протоколов защиты информации в сетях Kerberos
103. Технология защиты авторских прав мультимедийных файлов с использованием цифровых водяных знаков;
104. Обеспечение информационной безопасности Интернета вещей в цифровой экономике;
105. Исследование механизмов целостности и доступности информации на платформе блокчейн;
106. Анализ технологий разработки смарт-контрактов и выявление их уязвимостей;
107. Оценка опасности уязвимостей смарт-контрактов в технологии блокчейн;
108. Оценка опасности уязвимостей беспроводных информационных технологий на основе Kali Linux;
109. Методы и технологии обнаружения скрытых контейнеров в сообщениях методами статистического анализа;
110. Методика инвентаризации, классификации и анализа информационных активов организации;
111. Методика генерации сценариев целевых атак на информационные системы;
112. Методика обоснования структуры службы информационной безопасности, функционального разделения обязанностей персона и степени их дублирования;
113. Разработка квестов по обучению технологии проникновения в защищенную сеть (этичный хакинг);
114. Технологии реверсинга (обратного программирования) и их применение при исследовании недекларированных функций программного обеспечения;
115. Применение технологий и средств информационно-аналитического обеспечения при расследовании инцидентов информационной безопасности