

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 защиту 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 персональных данных финансово-кредитной организации
2. Защита персональных данных в коммерческой организации
3. Защита персональных данных в организации с участием государства (муниципальном образовании)
4. Защита персональных данных в медицинских учреждениях
5. Защита электронного документооборота на предприятии
6. Инвентаризация информационных активов организации
7. Защита информации в концепции стандарта ГОСТ Р 27001-2006 (на примере организации малого (среднего) бизнеса)
8. Защита информации в концепции стандарта ГОСТ Р 27001-2006 (на примере финансово-кредитного учреждения)
9. Защита коммерческой тайны в организации
10. Защита информации в концепции стандарта ГОСТ Р 27001-2006 (на примере общественной организации)
11. Защита информации в концепции стандарта COBIT 5.0 (на примере некоммерческой организации)
12. Защита служебной тайны в организации
13. Защита интеллектуальной собственности в организации
14. Сертификация СМИБ по стандарту ГОСТ Р ИСО/МЭК 27001
15. Аттестация системы информационной безопасности государственной информационной системы
16. Разработка модели угроз информационной безопасности в финансово-кредитном учреждении
17. Разработка модели нарушителя информационной безопасности в организации
18. Разработка модели нарушителя информационной безопасности в организации, относящейся к критической информационной инфраструктуре
19. Разработка программного обеспечения выделения агрегатов рисков по общим угрозам, уязвимостям и активам
20. Имитационное моделирование сценариев рисков информационной безопасности
21. Анализ рисков информационной безопасности в информационной системе персональных данных
22. Мониторинг состояния объекта на основе оценки рисков

23. Автоматизированный выбор мер и средств контроля и управления по заданным рискам с использованием нейронных сетей
24. Моделирование рисков информационной безопасности в информационных системах, построенных по технологии блокчейн
25. Инвентаризация и классификация информационных активов организации при оценке рисков
26. Оценка и анализ рисков с использованием программного обеспечения CORAS
27. Организация режима защиты конфиденциальной информации на предприятии государственного сектора экономики
28. Разработка комплекта документации по результатам аттестации объекта информатизации (автоматизированной системы)
29. Разработка политики информационной безопасности организации
30. Разработка комплекса мероприятий по лицензированию деятельности предприятия по технической защите конфиденциальной информации
31. Разработка комплекса мероприятий по сертификации средства обработки конфиденциальной информации
32. Разработка комплекса мероприятий по сертификации средства защиты информации
33. Организация режима коммерческой тайны на предприятии
34. Разработка частных политик информационной безопасности для организации
35. Моделирование угроз персональным данным в организации
36. Обеспечение безопасности информации на объектах критической информационной инфраструктуры
37. Документальное обеспечение режима коммерческой тайны предприятия
38. Формирование требований к сотруднику службы информационной безопасности при внедрении профессиональных стандартов
39. Разработка и реализация программы повышения осведомленности сотрудников предприятия (организации) в области информационной безопасности
40. Организация проверки и оценки уровня подготовки персонала предприятия, участвующего в обработке конфиденциальной информации
41. Управление поведением персонала при организации безопасной работы в информационной системе организации
42. Инструментальные проверки персонала организации, использующего в работе конфиденциальную информацию
43. Подготовка персонала организации, использующего в работе конфиденциальную информацию с использованием дистанционных образовательных технологий
44. Организация расследования инцидентов информационной безопасности на предприятии
45. Обеспечение режима конфиденциальности в организации при увольнении сотрудников
46. Организация специальных инструментальных проверок персонала для противодействия инсайдерству в финансовом учреждении (на предприятии энергетики)
47. Разработка проекта технической защиты конфиденциальной информации на предприятии от ее утечки по (конкретный вид) каналу
48. Разработка проекта технической защиты информации на автоматизированном рабочем месте от ее утечки по (конкретный вид) каналу
49. Проектирование системы охранного видеонаблюдения организации с использованием профессиональных графических инструментов
50. Разработка программы специального обследования по выявлению электронных устройств негласного получения информации в защищаемом помещении предприятия

51. Разработка программы специального обследования по выявлению временно отключенных электронных устройств негласного получения информации в защищаемом помещении предприятия
52. Разработка программы специального обследования защищаемого помещения (кабинета, переговорной комнаты, конференц-зала и т.д.) предприятия (организации)
53. Внедрение методов и способов организации автоматизированного пропускного режима на предприятии
54. Разработка технического проекта создания защищаемого помещения в организации
55. Разработка технического проекта системы защиты информации организации от утечки по постоянно действующим каналам связи
56. Разработка программы проведения специального обследования помещения организации по выявлению акустопараметрического канала утечки информации
57. Оценка защищенности планшетных компьютеров от утечки конфиденциальной информации по каналу ПЭМИ
58. Разработка проекта системы защиты конфиденциальной информации в организации
59. Разработка предложений по повышению защищенности вычислительной техники по каналу ПЭМИ пассивными методами
60. Разработка рекомендаций по защите конфиденциальной информации от утечки по акустическому каналу из защищаемого помещения пассивными методами
61. Разработка алгоритма поиска сигналов со сложными структурами в процессе радиомониторинга
62. Разработка технического задания на проведение поисковых работ по обнаружению скрытых неизлучающих устройств утечки информации
63. Автоматизация процесса подготовки отчетных документов по результатам проведения инструментального контроля уровня защищенности автоматизированного рабочего места
64. Администрирование систем безопасности сетевого взаимодействия на основе технологии VPN
65. Разработка комплекса правил, процедур и практических приемов защиты информации в мобильных устройствах
66. Программная защита информационной системы организации на основе возможностей операционной системы
67. Организация программной защиты сервера с использованием возможностей ОС Microsoft Windows
68. Разработка и внедрение электронной подписи в документооборот организации
69. Анализ уязвимостей систем удаленного видеонаблюдения на предприятии
70. Обеспечение безопасности сетевого взаимодействия с использованием технологии OpenVPN
71. Администрирование средств межсетевого экранирования в системе защиты информации организации
72. Применение межсетевых экранов экспертного уровня для защиты ресурсов локальной вычислительной сети в организации
73. Администрирование системы резервного копирования для защиты информационных активов организации
74. Внедрение в организации системы резервного копирования
75. Обеспечение безопасности сетевого взаимодействия с использованием технологии IPSec
76. Защита сетевого хранилища средствами QNAP NAS от несанкционированного доступа и нарушения целостности данных

77. Защита сетевого хранилища средствами Synology NAS от несанкционированного доступа и нарушения целостности данных
78. Организация программной защиты файлового сервера с использованием возможностей операционной системы AstraLinux
79. Организация программной защиты веб-сервера с использованием возможностей операционной системы AstraLinux
80. Организация программной защиты файлового сервера с использованием возможностей операционной системы ALT Linux
81. Организация программной защиты веб-сервера с использованием возможностей операционной системы ALT Linux
82. Администрирование программно-аппаратного комплекса «Соболь» на рабочих станциях в организации
83. Защита локальной вычислительной сети организации с использованием IDS/IPS систем
84. Диагностика стеганографических возможностей и противодействие им при реализации информационных процессов в организации
85. Разработка средств автоматизации для настройки средств защиты информации от несанкционированного доступа
86. Разработка средств автоматизации для контроля защищенности автоматизированных систем по требованиям безопасности информации
87. Разработка средств автоматизации для исследования программного обеспечения по требованиям безопасности информации
88. Разработка системы диагностики наличия вредоносного программного обеспечения («в локальной сети организации» или «на сетях IoT-устройств» или «в промышленной сети организации»)
89. Обеспечение безопасного подключения рабочих станций (название организации), обрабатывающих конфиденциальную информацию, к сети Интернет
90. 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)
91. Защита от несанкционированных проводных подключений к локальной сети (название организации)
- 92.
93. Организация аудита информационной безопасности организации с использованием специального программного обеспечения
94. Применение технологии активного аудита информационной безопасности в организации
95. Разработка программы проведения аудита информационной безопасности в организации
96. Разработка программы проведения внутреннего аудита информационной безопасности организации
97. Внедрение системы менеджмента инцидентов информационной безопасности в коммерческом банке
98. Организация мониторинга действий персонала организации с целью выявления инцидентов информационной безопасности
99. Внедрение технологий предотвращения утечки информации (DLP-системы) в организации
100. Внедрение технологии управления информацией и событиями безопасности (SIEM-системы) в организации
101. Автоматизация процессов менеджмента информационной безопасности в организации

102. Внедрение системы предотвращения утечки информации в финансово-кредитном учреждении
103. Внедрение системы сбора и корреляции событий информационной безопасности в финансово-кредитном учреждении
104. Организация центра управления информационной безопасностью в финансово-кредитном учреждении
105. Внедрение системы мониторинга информационной безопасности в финансово-кредитном учреждении
106. Расследование инцидентов информационной безопасности в организации
107. Проведение аудита информационной безопасности организации с использованием сканера безопасности
108. Аудит безопасности локальной вычислительной сети организации с использованием сканера безопасности
109. Защита информации с использованием методов и технологий упрощенной криптографии в организации
110. Криптографические способы контроля целостности и их практическая реализация
111. Асимметричные криптосистемы и методы обеспечения конфиденциальности при их использовании
112. Моделирование уязвимостей протоколов защиты TLS
113. Моделирование уязвимостей протоколов защиты SSL
114. Моделирование уязвимостей протоколов защиты информации в сетях Kerberos
115. Технология защиты авторских прав мультимедийных файлов с использованием цифровых водяных знаков
116. Обеспечение информационной безопасности Интернета вещей в цифровой экономике
117. Исследование механизмов целостности и доступности информации на платформе блокчейн.
118. Анализ технологий разработки смарт-контрактов и выявление их уязвимостей
119. Методика инвентаризации, классификации и анализа информационных активов организации.
120. Методика генерации сценариев целевых атак на информационные системы
121. Методика обоснования структуры службы информационной безопасности, функционального разделения обязанностей персонала и степени их дублирования.