Аннотация
программы государственной итоговой аттестации
направления подготовки
10.03.01 Информационная безопасность
образовательная программа
«Комплексная защита объектов информатизации»
Уровень образования
бакалавриат
Форма обучения
очная,очно- заочная

1. **Общие положения**	Программа государственной итоговой аттестации составлена в соответствии с: – Положением об итоговой аттестации обучающихся в АНО ВО «Межрегиональный открытый социальный институт» по программам бакалавриата, программам специалитета и программам магистратуры от 5 декабря 2016 г. – требованиями федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.03.01 Информационная безопасность (уровень бакалавриата), утвержденного приказом Министерства образования и науки Российской Федерации от «1» декабря 2016 г. №1515; – учебным планом и календарным учебным графиком по направлению подготовки 10.03.01 Информационная безопасность. Государственной итоговая аттестация в полном объеме относится к базовой части образовательной программы 10.03.01 Информационная безопасность и завершается присвоением квалификации «бакалавр». В государственную итоговую аттестацию выпускников по направлению подготовки 10.03.01 Информационная безопасность входит защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты.
2. Требования к выпускной квалификационной работе и порядок ее выполнения	Выпускная квалификационная работа рассматривается как самостоятельная заключительная работа обучающегося, в которой систематизируются, закрепляются и расширяются теоретические знания и практические умения и навыки, полученные при освоении дисциплин (модулей) и прохождении практик, предусмотренных образовательной программой 10.03.01 Информационная безопасность. Выпускная квалификационная работа демонстрирует уровень подготовленности выпускника к самостоятельной профессиональной деятельности. Выпускная квалификационная работа выполняется по следующим примерным темам: 1. Методика оценки рисков информационной безопасности хозяйствующего субъекта (на конкретном примере) на основе моделирования угроз и уязвимостей его информационной системы 2. Управление рисками информационной безопасности хозяйствующего субъекта (на конкретном примере) 3. Система обеспечения информационной безопасности

	(защиты информации) хозяйствующего субъекта, ее анализ и выработка рекомендаций (предложений) по дальнейшему совершенствованию 4. Разработка рекомендаций по организации системы защиты персональных данных хозяйствующего субъекта (на конкретном примере) 5. Системный анализ информационной инфраструктуры и разработка защищенной корпоративной информационной системы предприятия (на конкретном примере) 6. Информационная система предприятия энергетики (на конкретном примере) и ее анализ с позиций информационной безопасности 7. Разработка системы защиты информации финансового учреждения (банка) на основе типовых решений 8. Организация и управление службой информационной безопасности хозяйствующего субъекта (на конкретном примере) 9. Проектирование системы защиты компьютерной информации на объектах информационной инфраструктуры предприятия (фирмы) 10. Анализ системы противодействия преступлениям в области информационных технологий в Российской Федерации 11. Организация системы защиты электронного документооборота хозяйствующего субъекта (на конкретном примере) и ее анализ 12. Организация системы защиты электронного документооборота хозяйствующего субъекта (на конкретном примере) на основе применения электронной цифровой подписи 13. Организация системы защиты компьютерной информации предприятия, организации (на конкретном примере) на основе единого контрольно-пропускного пункта 14. Организация защиты корпоративной информационной системы хозяйствующего субъекта (на конкретном примере) на основе типовых решений (на конкретных примерах) 15. Комплексный анализ угроз и уязвимостей информационной системы хозяйствующего субъекта (на конкретном примере) на основе метода экспертного опроса 16. Разработка прототипа корпоративного стандарта информационной безопасности предприятия энергетики на основе требований международных и национальных стандартов 17. Организационно-правовое обеспечение защиты информации в интересах хозяйствующего субъекта 18. Организация режима защиты конфиденциальной информации хозяйствующего субъекта (на конкретном примере) 19. Разработка комплекта документации по результатам аттестации объекта информационной системы хозяйствующего субъекта (на конкретном примере) 20. Разработка концепции (политики) информационной безопасности хозяйствующего субъекта (на конкретном примере) 21. Разработка комплекса мероприятий по лицензированию объекта информационной системы хозяйствующего субъекта (на конкретном примере) в области защиты информации 22. Разработка комплекса мероприятий по сертификации объекта

	информационной системы хозяйствующего субъекта (на конкретном примере) в области защиты информации 23. Организация режима защиты конфиденциальной информации хозяйствующего субъекта (на конкретном примере) и его комплексный анализ 24. Разработка комплекса политик для системы информационной безопасности хозяйствующего субъекта (на конкретном примере) 25. Анализ требований лучших отечественных и зарубежных стандартов (на конкретных примерах) в области информационной безопасности и их применение при разработке политики информационной безопасности хозяйствующего субъекта (на конкретном примере) 26. Кадровое обеспечение защиты информации в интересах хозяйствующего субъекта 27. Администрирование информационной системы хозяйствующего субъекта (на конкретном примере) и его роль в системе управления персоналом 28. Обеспечение информационной безопасности хозяйствующего субъекта (на конкретном примере), на основе формирования корпоративной информационной культуры персонала 29. Организация профилактики нарушений режима и расследования инцидентов информационной безопасности хозяйствующего субъекта (на конкретном примере) 30. Организация и методика использования результатов специальных проверок персонала с применением современных программно-аппаратных комплексов для противодействия инсайдерам (на примере финансового учреждения) 31. Финансово-экономическое обеспечение защиты информации в интересах хозяйствующего субъекта 32. Обоснование затрат на обеспечение информационной безопасности хозяйствующего субъекта (на конкретном примере) на основе использования стандартных методик 33. Моделирование и анализ инвестиционного проекта создания (совершенствования) системы обеспечения информационной безопасности хозяйствующего субъекта (на конкретном примере) 34. Экономическая оценка рисков информационной безопасности в интересах хозяйствующего субъекта (на конкретном примере) 35. Экономическое обоснование управленческих решений, направленных на создание системы обеспечения информационной безопасности хозяйствующего субъекта (на конкретном примере) 36. Моделирование и анализ инвестиционного проекта создания и оборудования на предприятии (на конкретном примере) защищаемого помещения 37. Инженерно-техническое обеспечение защиты информации в интересах хозяйствующего субъекта 38. Разработка комплекса рекомендаций по технической защите конфиденциальной информации хозяйствующего субъекта (на конкретном примере) 39. Разработка комплекса рекомендаций по технической защите

	конфиденциальной информации на автоматизированных рабочих местах (на примере хозяйствующего субъекта) 40. Разработка комплекса мероприятий (рекомендаций) по защите информации, циркулирующей в защищаемых помещениях хозяйствующего субъекта (на конкретном примере) 41. Оценка защищенности помещения хозяйствующего субъекта (на конкретном примере) от утечки речевой конфиденциальной информации по акустическому и виброакустическому каналам 42. Оценка защищенности помещения хозяйствующего субъекта (на конкретном примере) от утечки речевой информации по каналам электроакустических преобразований 43. Оценка защищенности технических средств и систем хозяйствующего субъекта (на конкретном примере), предназначенных для обработки конфиденциальной информации от утечки по линиям связи 44. Оценка защищенности конфиденциальной информации хозяйствующего субъекта (на конкретном примере) от утечки за счет наводок на технические средства, системы и их коммуникации линиям связи 45. Комплексная оценка защищенности помещения хозяйствующего субъекта (на конкретном примере) от утечки конфиденциальной информации по техническим каналам 46. Оценка защищенности конфиденциальной информации хозяйствующего субъекта (на конкретном примере) от утечки за счет побочных электромагнитных излучений и наводок при использовании электронно-вычислительной техники 47. Разработка комплекса мероприятий по обнаружению и поиску устройств для несанкционированного съема информации по радио-каналу в защищаемом помещении хозяйствующего субъекта (на конкретном примере) 48. Разработка комплекса мероприятий по обнаружению и поиску временно отключенных устройств несанкционированного съема информации в защищаемом помещении хозяйствующего субъекта (на конкретном примере) 49. Разработка комплекса мероприятий по обнаружению и поиску устройств несанкционированного съема информации в защищаемом помещении хозяйствующего субъекта (на конкретном примере) 50. Организация и методика проведения радиомониторинга защищаемого помещения (на примере хозяйствующего субъекта) 51. Программно-аппаратная защита информации в интересах хозяйствующего субъекта 52. Организация защиты информации в локальной вычислительной сети хозяйствующего субъекта (на конкретном примере) 53. Защита информации в локальной вычислительной сети хозяйствующего субъекта (на конкретном примере) при использовании сервисов и ресурсов сетей общего пользования 54. Организация криптографической защиты информации в информационной системе хозяйствующего субъекта (на конкретном примере) на основе анализа современных предложений

	55. Организация программной защиты информационной системы хозяйствующего субъекта (на конкретном примере) на основе встроенных возможностей современных операционных систем (на конкретном примере) 56. Организация программной защиты информации хозяйствующего субъекта (на конкретном примере) на основе возможностей современных пользовательских приложений (на конкретном примере) 57. Организация использования цифровых сертификатов и электронной цифровой подписи при обеспечении безопасности электронного документооборота хозяйствующего субъекта 58. Организация системы мониторинга информационной безопасности хозяйствующего субъекта на основе использования сканеров безопасности 59. Организация программно-аппаратной защиты информационной системы хозяйствующего субъекта (на конкретном примере) на основе возможностей современных систем и средств маршрутизации (на конкретном примере) 60. Защита информации в локальной (корпоративной) вычислительной сети хозяйствующего субъекта (на конкретном примере) на основе использования возможностей провайдеров 61. Организация использования средств межсетевого экранирования в системе защиты информации хозяйствующего субъекта 62. Организация системы резервного копирования при обеспечении защиты информации хозяйствующего субъекта (на конкретном примере) 63. Организация системы антивирусной защиты информационной инфраструктуры хозяйствующего субъекта (на конкретном примере) на основе оценки отечественного и зарубежного рынка 64. Аудит информационной системы хозяйствующего субъекта с позиций безопасности 65. Организация и применение технологии активного аудита при проведении комплексного аудита информационной системы хозяйствующего субъекта (на конкретном примере) с позиций безопасности 66. Разработка программы проведения комплексного аудита информационной системы хозяйствующего субъекта (на конкретном примере) с позиций безопасности 67. Разработка методики проведения внутреннего аудита информационной системы хозяйствующего субъекта (на конкретном примере) с позиций безопасности 68. Методика использования тестирующего программного обеспечения (на конкретном примере) при проведении аудита информационной системы хозяйствующего субъекта с позиций безопасности 69. Разработка системы обязательной маркировки экспортируемых файлов на основе цифровых водяных знаков 70. Разработка биометрической системы верификации авторства деловой переписки. 71. Разработка системы защиты от подмены авторизованного

	оператора ключевой системы информационной инфраструктуры 72. Разработка системы автоматического сбора доказательной базы для последующего расследования утечек информации. 73. Разработка комплекса мероприятий по защите от утечек ценной информации в хозяйствующем субъекте (на конкретном примере) 74. Разработка системы проверки исходящей информации в хозяйствующем субъекте. 75. Разработка системы резервного копирования по протоколу P2P при обеспечении защиты информации хозяйствующего субъекта 76. Разработка программной системы противодействия использованию анонимайзеров при обеспечении защиты информации хозяйствующего субъекта 77. Разработка комплекса мероприятий по противодействия использованию анонимайзеров хозяйствующего субъекта (на конкретном примере) в области защиты информации 78. Разработка методики оценки финансового ущерба от инсайдерских действий в хозяйствующем субъекте (на конкретном примере) 79. Разработка программного комплекса мониторинга внутреннего и внешнего трафика, как средство защиты от инсайдеров 80. Защита конфиденциальной информации на мобильных устройствах как часть системы управления информационной безопасности предприятия 81. Система управления информационной безопасности, как средство обеспечения непрерывности бизнеса на примере конкретного хозяйствующего субъекта 82. Анализ существующего международного законодательства по защите персональных данных 83. Разработка регламента управления рисками в области информационной безопасности конкретного хозяйствующего субъекта 84. Разработка требований к средствам защиты информации в корпоративных системах с внешним информационным обменом на основе анализа рисков 85. Методология предупреждения угроз информационной безопасности техническими средствами в телекоммуникационной инфраструктуре интеллектуального здания 86. Защита учреждений и предприятий от несанкционированного доступа к информации в технических каналах связи 87. Методика защиты информации в беспроводных сетях на основе динамической маршрутизации трафика 88. Исследование электромагнитных полей в помещениях для целей электромагнитной и информационной безопасности 89. Управление защитой информации в сегменте корпоративной информационной системы на основе интеллектуальных технологий 90. Модели и алгоритмы повышения уровня информационной безопасности корпоративных информационно-телекоммуникационных сетей

	91. Обработка изображения радужной оболочки глаза в системе идентификации личности 92. Разработка и анализ высокоэффективных способов и алгоритмов автоматического сопряжения, синхронизации, юстировки изображений, управления поворотными камерами и обработки информации в приборах и системах видеонаблюдения 93. Автоматизация процессов обработки информации в системах видеонаблюдения на особо опасных производствах.
3. Критерии оценки выпускных квалификационных работ	Критерии оценки результатов защиты выпускных квалификационных работ отражены в программе государственной итоговой аттестации обучающихся по направлению подготовки 10.03.01 Информационная безопасность, ОП «Комплексная защита объектов информатизации».