ПРОЕКТ

ПРОФЕССИОНАЛЬНЫЕ КОМПЕТЕНЦИИ СПЕЦИАЛИСТОВ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (примеры)[1]

ДЛЯ ТЕХНОЛОГИЧЕСКИХ ПРОЦЕССОВ

- Эксплуатация (обеспечение эксплуатации) оборудования и систем информационной безопасности
- Разработка оборудования и систем информационной безопасности

СОДЕРЖАНИЕ

[1] Сформированы на основе профессиональных стандартов в области информационной безопасности, требований к квалификации работников в вакансиях и экспертных обсуждений.
Проводятся дополнительные обсуждения. Предложения просьба отправлять по адресу: yuv407@vcot.info.

Предложения просим отправлять по адресу: yuv407@vcot.info

1. ЭКСПЛУАТАЦИЯ (ОБЕСПЕЧЕНИЕ ЭКСПЛУАТАЦИИ) ОБОРУДОВАНИЯ И СИСТЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.1. Типовые формулировки общепрофессиональных и специальных профессиональных умений

Общепрофессиональные умения[2]	**Специальные профессиональные умения**[3]
Уровень квалификации 5[4]	
Аналитические (анализ, сопоставление, сравнение, мониторинг и др.)	*Аналитические (анализ, сопоставление, сравнение, мониторинг и др.)*
	Проводить мониторинг, анализ и сравнение эффективности программно-аппаратных средств защиты информации в операционных системах/ компьютерных сетях Формулировать предложения по применению программно-аппаратных средств защиты информации в компьютерных сетях
Коммуникационные/организационные/управленческие	*Коммуникационные/организационные/управленческие*
	Взаимодействовать с организациями, осуществляющими гарантийный и послегарантийный ремонт СССЭ, а также средств и подсистем защиты СССЭ от НСД, средств для поиска признаков компьютерных атак в сетях электросвязи
Работа с документами:	*Работа с документами:*
Оформлять документацию по регламентации мероприятий и оказанию услуг в области защиты информации Оформлять техническую документацию в соответствии с нормативными правовыми актами в области защиты информации Оформлять эксплуатационную документацию программно-аппаратных средств защиты информации	
Установка/настройка общего программного обеспечения:	*Установка/настройка специального программного обеспечения:*
Устанавливать обновления программного обеспечения, включая программное	Конфигурировать параметры системы защиты информации автоматизированной

[2] Знания и умения, которые используются специалистами для осуществления широкого круга профессиональных задач в рамках различных видов профессиональной деятельности.
[3] Знания и умения, которые используются специалистами для осуществления узкопрофессиональных задач в рамках конкретного вида профессиональной деятельности.
[4] Определяется в соответствии с приказом Министерства труда и социальной защиты Российской Федерации от 12 апреля 2013 г. № 148н «Об утверждении уровней квалификации в целях разработки проектов профессиональных стандартов».

Общепрофессиональные умения[2]	**Специальные профессиональные умения**[3]
обеспечение средств защиты информации Выполнять резервное копирование и аварийное восстановление работоспособности средств защиты информации Управлять учетными записями пользователей, в том числе генерацией, сменой и восстановлением паролей Контролировать корректность настройки межсетевых экранов в соответствии с заданными правилами Устанавливать программное обеспечение в соответствии с технической документацией Выполнять настройку параметров работы программного обеспечения, включая системы управления базами данных и средства электронного документооборота Устанавливать межсетевые экраны в компьютерных сетях Конфигурировать межсетевые экраны в соответствии с заданными правилами	системы в соответствии с ее эксплуатационной документацией Обнаруживать и устранять неисправности системы защиты информации автоматизированной системы согласно эксплуатационной документации Настраивать компоненты подсистем защиты информации операционных систем Контролировать целостность подсистем защиты информации операционных систем Устранять неисправности подсистем защиты информации операционных систем и программно-аппаратных средств защиты информации согласно технической документации Производить установку и настройку программных (программно-технических) средств защиты информации от несанкционированного доступа в соответствии с инструкциями по эксплуатации и эксплуатационно-техническими документами Проводить испытания программных (программно-технических) средств защиты информации от несанкционированного доступа в соответствии с инструкциями по эксплуатации и эксплуатационно-техническими документами Конфигурировать параметры системы защиты информации ИАС в соответствии с ее эксплуатационной документацией Обнаруживать и устранять неисправности системы защиты информации ИАС согласно эксплуатационной документации
Использование/применение общего программного обеспечения	*Использование/применение специального программного обеспечения*
Использовать типовые криптографические средства защиты информации, в том числе средства электронной подписи Использовать программные средства для архивирования информации Использовать программные и программно-аппаратные средства для уничтожения (стирания) информации и носителей информации Применять программно-аппаратные средства защиты информации в операционных системах/ компьютерных сетях	

Общепрофессиональные умения[2]	**Специальные профессиональные умения**[3]
Применять антивирусные средства защиты информации в операционных системах Работать в операционных системах/компьютерных сетях/ с программным обеспечением с соблюдением действующих требований по защите информации	
Монтаж/наладка/ремонт общих технических средств	*Монтаж/наладка/ремонт специальных технических средств*
Производить монтаж и диагностику компьютерных сетей Производить монтаж и диагностику компонентов ИАС	Проводить установку и монтаж технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок в соответствии с техническим проектом, инструкциями по эксплуатации и эксплуатационно-техническими документами Проводить настройку и испытание технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок в соответствии с инструкциями по эксплуатации и требованиями нормативно-методических
	Документов Проводить техническое обслуживание технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок в соответствии с инструкциями по эксплуатации и эксплуатационно-техническими документами Проводить устранение выявленных неисправностей технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок и при необходимости организовывать их ремонт Проводить проверку комплектности СССЭ, средств и систем защиты СССЭ от НСД Проводить монтаж (для программных средств – установку) СССЭ, средств и систем защиты СССЭ от НСД Проводить первичную настройку и проверку функционирования СССЭ, средств и систем защиты СССЭ от НСД Проводить текущий контроль показателей и процесса функционирования СССЭ, а

Общепрофессиональные умения[2]	**Специальные профессиональные умения**[3]
	также программных, программно-аппаратных (в том числе криптографических) и технических средств, и систем защиты СССЭ от НСД, средств для поиска признаков компьютерных атак в сетях электросвязи, предусмотренный регламентом их эксплуатации
Использование/применение общих технических средств	*Использование/применение специальных технических средств*
Уровень квалификации 6	
Аналитические (анализ, разработка, сопоставление, сравнение, мониторинг и др.)	*Аналитические (анализ, сопоставление, сравнение, мониторинг и др.)*
Применять общенаучные методики, характерные для теории распределенных систем, к решению конкретных задач обработки информации	Оценивать информационные риски в автоматизированных системах Классифицировать и оценивать угрозы безопасности информации
Анализировать и оценивать угрозы информационной безопасности Проверять гипотезы и границы их применения в задачах анализа информации в ИАС Разрабатывать и применять математические модели и методы решения задач анализа информации в ИАС, создавая соответствующее программное и математическое обеспечение Представлять результаты решения аналитических задач в стандартном виде Интерпретировать профессиональный смысл получаемых результатов анализа информации в ИАС Разрабатывать формализованные модели, методы и алгоритмы решения типовых задач автоматизированной информационно-аналитической поддержки процессов принятия решений Применять методы и средства мониторинга и ситуационного анализа обстановки на базе ситуационных центров и геоинформационных автоматизированных систем Оценивать эффективность и качество в задачах прогнозирования, планирования, принятия решений при различной априорной неопределенности имеющейся информации Применять аналитические и компьютерные	Разрабатывать предложения по совершенствованию системы управления защиты информации автоматизированных систем Определять источники и причины возникновения инцидентов Оценивать последствия выявленных инцидентов Проводить анализ структурных и функциональных схем защищенной автоматизированной системы Проводить анализ доступных информационных источников с целью выявления известных уязвимостей, используемых в системе защиты информации программных и программно-аппаратных средств Анализировать программные и программно-аппаратные решения при проектировании системы защиты информации с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах Проводить анализ и сравнение эффективности применения СКЗИ в автоматизированных системах Анализировать программные, архитектурно-технические и схемотехнические решения с целью выявления потенциальных

Общепрофессиональные умения[2]	**Специальные профессиональные умения**[3]
модели автоматизированных систем и систем защиты информации Использовать современные модели и методы измерения, прогнозирования, планирования, принятия решений в профессиональной области	Анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах Производить анализ эффективности программно-аппаратных средств защиты информации в операционных системах Производить анализ эффективности программно-аппаратных средств защиты информации в компьютерных сетях Оценивать оптимальность выбора программно-аппаратных средств защиты информации и их режимов функционирования в компьютерных сетях
Рассчитывать радиусы опасных зон побочных электромагнитных излучений и наводок Анализировать и оценивать технологический процесс обработки информации Оценивать помехоустойчивость и эффективность сетей электросвязи при передаче трафика, оптимизировать их параметры Строить алгоритмы решения типовых задач обработки информации в ИАС Разрабатывать программы реализации в ИАС алгоритмов решения типовых задач обработки информации	Оценивать оптимальность выбора программно-аппаратных средств защиты информации и их режимов функционирования в операционных системах Оценивать угрозы безопасности информации в компьютерных сетях Обосновывать выбор используемых программно-аппаратных средств защиты информации в компьютерных сетях Проводить мониторинг функционирования программно-аппаратных средств защиты информации в операционных системах Проводить мониторинг функционирования программно-аппаратных средств защиты информации в компьютерных сетях Разрабатывать методики контроля защищенности акустической речевой информации от утечки по техническим каналам Рассчитывать показатели защищенности акустической речевой информации Анализировать события, связанные с защитой информации в автоматизированных системах Определять подлежащие защите информационные ресурсы автоматизированных систем
Коммуникационные/организационные/управленческие	*Коммуникационные/организационные/управленческие*
Работать в коллективе, принимать управленческие решения и оценивать их	Контролировать сроки передачи, использования, условий хранения и

Общепрофессиональные умения[2]	**Специальные профессиональные умения**[3]
эффективность Организовывать работу информационно-аналитического подразделения Организовывать процессы создания и эксплуатации ИАС Организовывать процессы создания и эксплуатации средств защиты ИАС Контролировать эффективность принятых мер по защите	размещения СКЗИ в соответствии с распорядительной и технической документацией Контролировать эффективность принятых мер по криптографической защите информации в автоматизированных информационных и телекоммуникационных системах Консультирование персонала автоматизированной системы по комплексу мер (правила, процедуры, практические приемы,
информации в автоматизированных системах	руководящие принципы, методы, средства) обеспечения защиты информации Осуществлять планирование и организацию работы персонала автоматизированной системы с учетом требований по защите информации Планировать политику безопасности компонентов (операционных систем, баз данных, компьютерных сетей, программных систем) автоматизированных систем с использованием СКЗИ Взаимодействовать с организациями, осуществляющими гарантийный и послегарантийный ремонт СКЗИ Обучать персонал комплексу мер по защите информации в автоматизированных информационных и Организовывать хранение, списание и утилизацию СКЗИ, составлять акты об их уничтожении (утилизации) Формировать политику безопасности программных компонентов автоматизированных систем
Работа с документами	*Работа с документами*
Оформлять документацию по регламентации мероприятий и оказанию услуг в области защиты информации Использовать нормативно-правовые акты, нормативно-методические документы по защите информации ограниченного доступа, по противодействию технической разведке и разрешительной системе в сфере информационной безопасности Заполнять формуляры и оформлять документацию на вспомогательное электронное оборудование Применять нормативные документы по	Применять техническую документацию, инструкции производителей программных, программно-аппаратных и аппаратных СКЗИ Выполнять задачи по получению, хранению, учету, выдаче, приему и утилизации специальных документов, применяемых в процессе эксплуатации СКЗИ Вести учет, заполнять формуляры на СКЗИ и права доступа к ним Вносить изменения в рабочую и эксплуатационную документацию на

Общепрофессиональные умения[2]	**Специальные профессиональные умения**[3]
защите от несанкционированного доступа к информации и противодействию технической разведке	криптографические средства защиты информации Документировать действия по устранению неисправностей в работе системы защиты информации автоматизированной системы
Использовать установленные федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации формы документов, сопровождающих жизненный цикл объекта критической информационной инфраструктуры Применять на практике требования нормативно-распорядительных документов (приказы, указания, инструкции) по вопросам создания и эксплуатации ИАС Использовать в процессе работы нормативные документы, регламентирующие функционирование ИАС	Документировать процедуры и результаты контроля функционирования системы защиты информации автоматизированной системы Вести учет проведения технических осмотров и обслуживания СКЗИ Подготавливать отчеты об использовании документации на СКЗИ, содержащей сведения, составляющие государственную тайну Регистрировать события, связанные с защитой информации в автоматизированных системах
Установка/настройка общего программного обеспечения:	*Установка/настройка специального программного обеспечения:*
Устанавливать и настраивать операционные системы, системы управления базами данных, компьютерные сети и программные системы с учетом требований по обеспечению защиты информации Создавать, удалять и изменять учетные записи пользователей значимых объектов критической информационной инфраструктуры критической информационной инфраструктуры объектов топливно-энергетического комплекса Создавать, удалять и изменять учетные записи пользователей системы криптографической защиты информации автоматизированных систем Устанавливать и настраивать операционные системы, системы управления базами данных, компьютерные сети и программные системы с учетом требований по криптографической защите информации	Определять параметры настройки программного обеспечения системы защиты информации автоматизированной системы Конфигурировать аттестованную информационную систему и системы защиты информации информационной системы Конфигурировать параметры системы защиты информации автоматизированных систем Конфигурировать и контролировать корректность настройки программно-аппаратных средств защиты информации в компьютерных сетях Выбирать режимы работы программно-аппаратных средств защиты информации в компьютерных сетях
Создавать, удалять и изменять учетные	

Общепрофессиональные умения[2]	Специальные профессиональные умения[3]
записи пользователей автоматизированной системы Устанавливать и настраивать операционные системы, системы управления базами данных, компьютерные сети и программные системы с учетом требований по обеспечению защиты информации Конфигурировать параметры средств защиты информации и системы безопасности значимых объектов критической информационной инфраструктуры критической информационной инфраструктуры на предприятии (объекте) топливно-энергетического комплекса Устанавливать и настраивать параметры сетевых протоколов, реализованных в телекоммуникационном оборудовании Осуществлять наладку компонентов обеспечивающей части ИАС на всех этапах их жизненного цикла Производить обслуживание компонентов обеспечивающей части ИАС на всех этапах их жизненного цикла Восстанавливать работоспособность компонентов обеспечивающей части ИАС при внештатных ситуациях Осуществлять меры противодействия нарушениям сетевой безопасности с использованием программных и программно-аппаратных средств защиты информации Настраивать антивирусные средства защиты информации в операционных системах Устанавливать обновления программного обеспечения и средств антивирусной защиты Настраивать правила фильтрации пакетов в компьютерных	
сетях Устанавливать корреспондентские отношения с источниками информации	
Использование/применение общего программного обеспечения	*Использование/применение специального программного обеспечения*
Использовать программные средства для архивирования информации Использовать программные и программно-	Применять технические средства контроля эффективности мер защиты информации Администрировать программные средства

Общепрофессиональные умения[2]	**Специальные профессиональные умения**[3]
аппаратные средства для уничтожения информации и носителей информации Применять типовые программные средства резервирования и восстановления информации в значимых объектах критической информационной инфраструктуры на предприятиях топливно-энергетического комплекса Применять средства обеспечения отказоустойчивости значимых объектов критической информационной инфраструктуры объектов топливно-энергетического комплекса Применять защищенные протоколы, межсетевые экраны, средства обнаружения вторжений в компьютерные сети Использовать средства защиты, предоставляемые системами управления базами данных Использовать встроенные механизмы защиты от НСД и компьютерных атак в составе СССЭ Применять типовые программные средства резервирования и восстановления информации в автоматизированных системах Применять средства обеспечения отказоустойчивости автоматизированных систем	системы защиты информации автоматизированных систем Контролировать события безопасности и действия пользователей автоматизированных систем Использовать криптографические методы и средства защиты информации в автоматизированных системах
Применять программные средства обеспечения безопасности данных Реализовывать правила разграничения доступа персонала к объектам доступа Применять ИАС в информационно-аналитической деятельности Применять ИАС в процессах организационного управления Сопровождать ИАС, локальные сети Взаимодействовать с вычислительными системами и базами данных в телекоммуникационном режиме и работать в глобальных компьютерных сетях	
Монтаж/наладка/ремонт общих технических средств	*Монтаж/наладка/ремонт специальных технических средств*
	Проводить проверку комплектности, монтаж (для программных средств – установку), первичную настройку и проверку функционирования СКЗИ

Общепрофессиональные умения[2]	Специальные профессиональные умения[3]
	Проводить ремонтные работы и настройку СКЗИ, составлять заявки на приобретение запасных частей Выполнять предусмотренные в технической и нормативно-методической документации работы по изменению настроек СКЗИ Проводить текущий контроль показателей и процесса функционирования СКЗИ, предусмотренный регламентом их эксплуатации Проверять техническое состояние СКЗИ и носителей ключевой информации Устранять выявленные уязвимости автоматизированной системы, приводящие к возникновению угроз безопасности информации Производить проверку соответствия реальных характеристик
	программно-аппаратных средств защиты информации заявленным в их технической документации Производить установку и монтаж защищенных технических средств обработки информации Проводить настройку защищенных технических средств обработки информации в соответствии с инструкциями по эксплуатации и эксплуатационно-техническими документами Проводить испытания защищенных технических средств обработки информации в соответствии с инструкциями по эксплуатации и эксплуатационно-техническими документами Проводить техническое обслуживание защищенных технических средств обработки информации в соответствии с инструкциями по эксплуатации и эксплуатационно-технической документацией Проводить устранение выявленных неисправностей защищенных технических средств обработки информации и при необходимости организовывать их ремонт Проводить измерение электрической и магнитной составляющей побочных

Общепрофессиональные умения[2]	Специальные профессиональные умения[3]
	электромагнитных излучений технических средств обработки информации в различных режимах их работы с использованием контрольно-измерительной аппаратуры Проводить измерение наводок побочных электромагнитных излучений технических средств обработки информации в различных режимах их работы с использованием контрольно-измерительной аппаратуры
Использовать/применять общие технические средства	*Использовать/применять специальные технические средства*
	Применять инструментальные средства контроля защищенности информации в автоматизированных системах Использовать типовые средства диагностики технического состояния СКЗИ и элементов среды функционирования
	Проводить контроль защищенности акустической речевой информации от утечки по акустическим, вибрационным и акустооптическим каналам
Уровень квалификации 7	
Аналитические (анализ, сопоставление, сравнение, мониторинг и др.)	*Аналитические (анализ, сопоставление, сравнение, мониторинг и др.)*
Структурировать аналитическую информацию для включения в отчет Определять причину и условия изменения программного обеспечения в компьютерных системах и сетях Выделять свойства и признаки информации, поступающей (обрабатываемой) в компьютерных системах и сетях, позволяющие установить ее принадлежность к определенному источнику Формировать исходные данные и ограничения при проектировании сети электросвязи Применять методологию менеджмента рисков информационной безопасности в телекоммуникационных системах и сетях электросвязи Проводить анализ рынка программных, программно-аппаратных и технических средств и систем защиты СССЭ от НСД Проводить мониторинг и анализ нормативных правовых актов,	Разрабатывать методики оценки защищенности программно-аппаратных средств защиты информации Оценивать эффективность защиты информации Анализировать программно-аппаратные средства защиты с целью определения уровня обеспечиваемой ими защищенности и доверия Анализировать компьютерную систему с целью определения необходимого уровня защищенности и доверия Разрабатывать профили защиты компьютерных систем Формулировать задания по безопасности компьютерных систем Выполнять анализ безопасности компьютерных систем и разрабатывать рекомендации по эксплуатации системы защиты информации Формировать политики безопасности компьютерных систем и сетей Прогнозировать возможные пути развития

Общепрофессиональные умения[2]	**Специальные профессиональные умения**[3]
руководящих и методических документов уполномоченных федеральных органов исполнительной власти в сфере защиты СССЭ от НСД и обеспечения безопасности критической информационной инфраструктуры	действий нарушителя информационной безопасности Производить анализ политики безопасности на предмет адекватности Проводить мониторинг, анализ и сравнение эффективности программно-аппаратных средств защиты информации в операционных системах Разрабатывать предложения по устранению выявленных уязвимостей
	Делать выводы по оценке защищенности компьютерных систем и сетей на основании аналитического отчета Формализовывать задачу управления безопасностью компьютерных систем Применять методы анализа защищенности компьютерных систем и сетей Анализировать структуру механизма возникновения и обстоятельства события, имеющего признаки компьютерного преступления, правонарушения или инцидента в компьютерных системах и сетях Прогнозировать возможные пути возникновения новых видов компьютерных преступлений, правонарушений и инцидентов в компьютерных системах и сетях Разрабатывать программы и методики сертификационных испытаний технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок на соответствие требованиям по безопасности информации Проводить экспертизу технических и эксплуатационных документов на сертифицируемые технические средства защиты информации от утечки за счет побочных электромагнитных излучений и наводок и материалов сертификационных испытаний Разрабатывать программы и методики предварительных испытаний системы защиты информации
Коммуникационные/организационные/управленческие	*Коммуникационные/организационные/управленческие*
Организовать информирование потенциальных потребителей о	Организовывать проведение специальных исследований и специальных проверок

Общепрофессиональные умения[2]	**Специальные профессиональные умения**[3]
номенклатуре, характеристиках и условиях поставки средств и систем защиты СССЭ от НСД	технических средств обработки информации ограниченного доступа Организовывать установку и настройку технических, программных (программно-технических) средств защиты информации, входящих в состав системы защиты информации
	организации, в соответствии с техническим проектом и инструкциями по эксплуатации Разрабатывать организационно-распорядительные документы, определяющие мероприятия по защите информации в организации Разрабатывать и реализовывать организационные меры, обеспечивающие эффективность системы защиты информации Организовывать обучение персонала использованию технических, программных (программно-технических) средств защиты информации Организовывать опытную эксплуатацию и доработку системы защиты информации Организовывать приемочные испытания системы защиты информации Организовывать и сопровождать аттестацию объектов вычислительной техники и выделенных (защищаемых) помещений на соответствие требованиям по защите информации Организовывать ввод системы защиты информации в эксплуатацию
Работа с документами	*Работа с документами*
Составлять и оформлять аналитический отчет по результатам проведенного анализа Оформлять экспертное заключение органа по сертификации Применять действующую законодательную базу в области обеспечения защиты информации в компьютерных системах и сетях	Составлять и оформлять аналитический отчет по проведенным сертификационным испытаниям программно-аппаратных средств защиты информации Применять нормативные и правовые акты при проведении криминалистической экспертизы и криминалистического анализа при расследовании компьютерных преступлений, правонарушений и инцидентов в компьютерных системах и сетях Оформлять материалы аттестационных испытаний (протоколов аттестационных испытаний и заключения по результатам аттестации ОВТ/ выделенных (защищаемых) помещений на

Общепрофессиональные умения[2]	**Специальные профессиональные умения**[3]
	соответствие требованиям по защите информации) Оформлять аттестат соответствия ОВТ/ выделенных (защищаемых) помещений требованиям по защите информации Оформлять протоколы испытаний и технические заключения по результатам сертификационных испытаний технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок на соответствие требованиям по безопасности информации
Установка/настройка общего программного обеспечения:	*Установка/настройка специального программного обеспечения:*
Использовать профили защиты и задания по безопасности Выявлять несоответствия атрибутов и содержания имеющейся информации ее расположению в компьютерной системе Определять принципы деления программного обеспечения на группы, их специфические свойства и взаимосвязь с компьютерной системой Выявлять возможные траектории изменения состояний функционирования компьютерной системы	
Использование/применение общего программного обеспечения	*Использование/применение специального программного обеспечения*
Монтаж/наладка/ремонт общих технических средств	*Монтаж/наладка/ремонт специальных технических средств*
	Проводить сертификационные испытания технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок на соответствие требованиям по безопасности информации Подготавливать объекты вычислительной техники и выделенные
	(защищаемые) помещения к аттестации по требованиям безопасности информации
Использовать/применять общие технические средства	*Использовать/применять специальные технические средства*
	Применять инструментальные средства проведения сертификационных испытаний программно-аппаратных средств защиты информации

Общепрофессиональные умения[2]	Специальные профессиональные умения[3]
	Применять инструментальные средства проведения мониторинга защищенности компьютерных систем

1.2. Типовые формулировки общепрофессиональных и специальных профессиональных знаний

Общепрофессиональные знания	Специальные профессиональные знания
Уровень квалификации 5	
Общенаучные и общетехнические	*Специальные по техническим средствам*
Назначение и принципы работы основных узлов современных технических средств информатизации Номенклатура, функциональное назначение и основные характеристики СССЭ критической информационной инфраструктуры Типы, основные характеристики средств измерений и контроля процесса и параметров функционирования СССЭ	Технические средства контроля эффективности мер защиты информации Общие принципы функционирования средств криптографической защиты информации в компьютерных сетях Возможности средств акустической речевой разведки Основные характеристики электронных устройств перехвата информации
Нормативные, организационные, методические документы	*Нормативные, организационные, методические документы*
Нормативные правовые акты Российской Федерации в области защиты информации Нормативные правовые акты в области связи, информатизации и защиты информации, обеспечения безопасности Порядок обеспечения безопасности информации при эксплуатации компьютерных сетей Порядок обеспечения безопасности информации при эксплуатации операционных систем	Регламент информирования персонала автоматизированной системы о выявленных инцидентах Регламент учета выявленных инцидентов Регламент устранения последствий инцидентов Основные методические и руководящие документы федеральных органов исполнительной власти, уполномоченных в области обеспечения информационной безопасности, безопасности информации в ключевых системах информационной инфраструктуры, противодействия техническим разведкам и
Формы и методы инструктажа пользователей по порядку работы в компьютерных сетях Порядок настройки программного обеспечения, систем управления базами данных и средств электронного документооборота Порядок оформления эксплуатационной документации Формы и методы инструктажа пользователей по порядку работы в	технической защиты информации Правила ведения эксплуатационной документации СССЭ, а также программных, программно-аппаратных (в том числе криптографических) и технических средств, и систем защиты СССЭ от НСД, средств для поиска признаков компьютерных атак в сетях электросвязи Методики и приемы ремонта СССЭ, а также средств и систем защиты СССЭ от НСД, средств для поиска признаков компьютерных

операционных системах Порядок эксплуатации средств антивирусной защиты в операционных системах Содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем безопасности автоматизированных систем Основные методические и руководящие документы уполномоченных федеральных органов исполнительной власти по защите информации Национальные, межгосударственные и международные стандарты в области защиты информации Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации Организация технического обслуживания и ремонта компонентов автоматизированной системы	атак в сетях электросвязи Порядок устранения неисправностей программно-технических средств защиты информации от несанкционированного доступа и специальных воздействий, организации их ремонта Номенклатура, функциональное назначение и основные характеристики средств и систем защиты СССЭ от НСД Нормативные требования к составу и содержанию эксплуатационной документации СССЭ, а также средств и систем защиты СССЭ от НСД Последовательность действий в целях изменения настроек СССЭ, а также средств и систем защиты СССЭ от НСД, средств для поиска признаков компьютерных атак в сетях электросвязи без прерывания процесса их функционирования Последовательность действий в целях восстановления процесса и параметров функционирования СССЭ, а также средств и систем защиты СССЭ от НСД, средств для поиска признаков компьютерных атак в сетях электросвязи Организация и содержание диагностики и технического обслуживания СССЭ, а также средств и систем защиты СССЭ от НСД, средств для поиска признаков компьютерных атак в сетях электросвязи
	Порядок технического обслуживания технических средств защиты речевой информации от утечки по техническим каналам Порядок устранения неисправностей технических средств защиты акустической речевой информации от утечки по техническим каналам и организация их ремонта Нормативные правовые акты, методические документы, национальные стандарты в области защиты информации от несанкционированного доступа и аттестации автоматизированных систем на соответствие требованиям по защите информации Принципы организации и структура систем защиты программного обеспечения автоматизированных систем Методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем и

	систем защиты автоматизированных систем Основные методические и руководящие документы федеральных органов исполнительной власти, уполномоченных в области обеспечения информационной безопасности, безопасности информации в ключевых системах информационной инфраструктуры, противодействия техническим разведкам и технической защиты информации Нормативные правовые акты и национальные стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации Методики сертификационных испытаний технических средств защиты информации от несанкционированного доступа и утечки по техническим каналам на соответствие требованиям по безопасности информации Порядок устранения неисправностей и организации ремонта средств защиты информации от утечки за счет побочных
	электромагнитных излучений и наводок Нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и аттестации выделенных (защищаемых) помещений на соответствие требованиям по защите информации Основные руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации и обеспечению безопасности критической информационной инфраструктуры Нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и аттестации объектов информатизации на соответствие требованиям по защите информации
Общие по ИКТ	*Специальные по ИБ*
Основные методы организации и проведения технического обслуживания технических средств ИАС Процедуры по архивированию информации, обрабатываемой ИАС Типовые уязвимости программного обеспечения и методы их эксплуатации Особенности источников угроз информационной безопасности,	Основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения защиты информации в автоматизированных системах Методы контроля эффективности защиты информации от утечки по техническим каналам Критерии оценки эффективности и надежности средств защиты программного

связанных с эксплуатацией программного обеспечения Признаки наличия вредоносного программного обеспечения Общие принципы функционирования вредоносного программного обеспечения Принципы функционирования средств антивирусной защиты	обеспечения автоматизированных систем Средств и систем защиты СССЭ от НСД, средств для поиска признаков компьютерных атак в сетях электросвязи Особенности применения программных и программно-аппаратных средств защиты информации в ИАС Особенности применения программных и программно-аппаратных средств защиты информации в автоматизированных системах Основные методы управления защитой информации Основные угрозы безопасности информации и модели нарушителя
Общие принципы функционирования программно-аппаратных средств криптографической защиты информации Топологии и протоколы сетевого взаимодействия, применяемые в эксплуатируемых компьютерных сетях Состав и основные характеристики оборудования, применяемого при построении компьютерных сетей Типовые методы и протоколы идентификации, аутентификации и авторизации в компьютерных сетях Типовые сетевые атаки и способы защиты от них Основные источники угроз информационной безопасности и меры по их предотвращению Основные методы организации и проведения технического обслуживания коммутационного оборудования компьютерных сетей Принципы формирования политики информационной безопасности в автоматизированных системах Программно-аппаратные средства защиты информации автоматизированных систем Основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах Основные меры по защите информации в автоматизированных системах Методы и способы обеспечения отказоустойчивости автоматизированных систем	в автоматизированных системах Методы защиты информации от несанкционированного доступа и утечки по техническим каналам Способы контроля эффективности защиты информации от несанкционированного доступа и утечки по техническим каналам Способы и средства защиты акустической речевой информации от утечки по техническим каналам Средства и методики контроля эффективности защиты акустической речевой информации от утечки техническим каналам Способы реализации несанкционированного доступа к информации и специальных программных воздействий на информацию и ее носители в автоматизированных системах Методы и средства защиты информации от несанкционированного доступа и специальных программных воздействий на нее Средства и методики контроля защищенности информации от несанкционированного доступа и специальных программных воздействий Способы и средства защиты информации от утечки за счет побочных электромагнитных излучений и наводок Средства и методики контроля эффективности защиты информации от утечки за счет побочных электромагнитных излучений и наводок Техническое обслуживание технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок Технические каналы утечки акустической

Основные информационные технологии, используемые в автоматизированных системах Принципы построения средств защиты информации от	речевой информации (прямые акустические, вибрационные, акустооптические, акустоэлектрические, акустоэлектромагнитные)
утечки по техническим каналам Способы защиты информации от несанкционированного доступа и утечки по техническим каналам Основные методы и средства криптографической защиты информации Методы, способы и средства обеспечения отказоустойчивости автоматизированных информационных систем Архитектура и пользовательские интерфейсы операционных систем Источники угроз информационной безопасности и меры по их предотвращению Сущность и содержание понятия информационной безопасности, характеристики ее составляющих Типовые средства защиты информации в операционных системах Программно-аппаратные средства и методы защиты информации Типовые средства и методы защиты информации в локальных и глобальных вычислительных сетях Базовая конфигурация системы защиты информации автоматизированной системы Типовые средства, методы и протоколы идентификации, аутентификации и авторизации Организационные меры по защите информации Основные методы организации и проведения технического обслуживания технических средств информатизации Процедуры по архивированию информации, обрабатываемой автоматизированной системой	Техническое обслуживание программно-технических средств защиты информации от несанкционированного доступа и специальных воздействий
Процедуры уничтожения (стирания) информации на машинных носителях, а также контроля уничтожения (стирания) информации Принципы построения средств защиты информации от несанкционированного	

доступа и утечки по техническим каналам Критерии оценки защищенности автоматизированной системы	
Эксплуатационная и проектная документация общего характера	*Эксплуатационная и проектная документация в области ИБ*
Организация технического обслуживания и ремонта компонентов ИАС Эксплуатационная и проектная документация на ИАС Эксплуатационная и проектная документация на автоматизированную систему	Технические описания и инструкции по эксплуатации программных (программно-технических) средств защиты информации от несанкционированного доступа Технические описания и инструкции по эксплуатации технических средств защиты речевой информации от утечки по техническим каналам Проектная документация на систему защиты выделенного помещения (в части защиты акустической речевой информации от утечки по техническим каналам) Проектная документация на систему защиты выделенного помещения (в части защиты акустической речевой информации от утечки по техническим каналам) Технические описания и инструкции по эксплуатации технических средств защиты речевой информации от утечки по техническим каналам Проектная документация на систему защиты выделенного помещения (в части защиты акустической речевой информации от утечки по техническим каналам) Технические описания и инструкции (руководства) по
	эксплуатации технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок Проектная документация на систему защиты объекта информатизации (в части защиты объекта от утечки информации за счет побочных электромагнитных излучений и наводок)
Общенаучные и общетехнические	*Специальные по техническим средствам*
Уровень квалификации 6	
Стандарты Единой системы конструкторской документации, Единой системой технической документации, Единой системы программной документации (ЕСКД, ЕСТД и ЕСПД) Методологические основы теории принятия решений, теории измерений, теории прогнозирования и планирования	Возможности средств акустической речевой разведки Основные характеристики специальных электронных устройств перехвата информации Функциональное назначение и основные характеристики средств контроля функционирования СССЭ, их защищенности от НСД и компьютерных атак

Способы измерения свойств объектов предметной области Структура, принципы построения и функционирования ситуационных центров Основы построения и функционирования геоинформационных автоматизированных систем Методы оценки эффективности и качества в задачах прогнозирования, планирования, принятия решений при различной априорной неопределенности имеющейся информации Методы теории вероятностей, теории случайных процессов и математической статистики Роль и место информационно-аналитической деятельности в системах организационного управления Методологические основы информационно-аналитической деятельности Принципы организации информационно-аналитической	Номенклатура, функциональное назначение и основные характеристики средств связи сетей связи специального назначения, включая СКЗИ, средства для поиска признаков компьютерных атак в сетях электросвязи Назначение и принципы работы основных узлов средств связи сетей связи специального назначения, включая СКЗИ, средства для поиска признаков компьютерных атак в сетях электросвязи Типы, основные характеристики средств измерений и контроля процесса и параметров функционирования средств связи сетей связи специального назначения
деятельности Способы формирования описаний объектов и классов объектов предметной области Методологические основы, методы и средства построения распределенных ИАС Математические модели, методы и алгоритмы решения типовых задач анализа информации в ИАС Методические подходы к интерпретации профессионального смысла получаемых результатов анализа информации в ИАС Методологические основы организационного управления Назначение и классификация информационных и аналитических систем, систем управления Научные основы, цели, принципы, методы и технологии управленческой деятельности	
Нормативные, организационные, методические документы	*Нормативные, организационные, методические документы*
Содержание и порядок деятельности персонала по эксплуатации автоматизированных систем,	Нормативно-методические документы в области защиты информации ограниченного доступа, документы национальной системы

защищенных с помощью СКЗИ Нормативные правовые акты в области защиты информации Организационные меры по защите информации Нормативные правовые акты Российской Федерации в области связи и защиты информации Законодательство Российской Федерации в области обеспечения безопасности критической информационной инфраструктуры Нормативные правовые акты Президента Российской	стандартизации в области криптографической защиты информации, проектирования средств защиты информации, сертификации средств защиты информации на соответствие требованиям безопасности информации Порядок эксплуатации СКЗИ Методика (регламент, последовательность) и нормативные требования к действиям в целях изменения настроек средств криптографической защиты информации Порядок проведения периодического осмотра и проверки работоспособности средства криптографической защиты
Федерации, Правительства Российской Федерации, федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации Нормативные правовые акты Российской Федерации в области защиты информации ограниченного доступа Национальные, межгосударственные и международные стандарты в области защиты информации Нормативная база, регламентирующая создание и эксплуатацию специальных ИАС Принципы и методы организации работы специалистов по созданию и эксплуатации ИАС Принципы и методы организации работы специалистов по созданию и эксплуатации средств защиты в ИАС Основные методы организационного обеспечения процесса разработки документов, регламентирующих функционирование ИАС Принципы и методы организации работы в информационно-аналитическом подразделении	информации, включая средства изготовления ключевых документов Нормативные и методические документы по разрешительной системе и делопроизводству, связанные с обеспечением учета и защиты документации, содержащей сведения ограниченного доступа, в т. ч., составляющие государственную тайну Порядок ведения журналов, формуляров, протоколов и эксплуатационной документации на средства криптографической защиты информации ограниченного доступа, в т. ч. содержащей сведения, составляющие государственную тайну Правила обращения и учета средств криптографической защиты информации ограниченного доступа, в т. ч. содержащей сведения, составляющие государственную тайну Законодательные акты Российской Федерации, нормативно-правовые акты, нормативно-методические документы уполномоченных государственных органов, документы национальной системы стандартизации Российской Федерации в области криптографической защиты информации, государственные стандарты в области защиты информации ограниченного доступа, проектирования средств защиты информации, сертификации средств защиты информации на соответствие требованиям безопасности информации Руководящие, нормативные и методические документы ФСБ России по организации и обеспечению безопасности передачи информации по защищенным с

	использованием СКЗИ каналам связи Нормативные и методические документы по вопросам ведения закрытого документооборота (в т. ч. электронного) и делопроизводства
	Организация защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации и обеспечению безопасности критической информационной инфраструктуры Нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и эксплуатации защищенных технических средств обработки информации Нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и эксплуатации защищенных программных (программно-технических) средств обработки информации Порядок организации технического обслуживания защищенных технических средств обработки информации Порядок устранения неисправностей защищенных технических средств обработки информации и организации их ремонта Порядок аттестации объектов информатизации на соответствие требованиям безопасности информации Нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и аттестации объектов информатизации на соответствие требованиям по защите информации Отчетные документы, оформляемые по результатам специальных исследований на побочные электромагнитные излучения и наводки технических средств обработки информации Цели и задачи управления персоналом по обеспечению защиты сетей электросвязи от НСД и компьютерных атак в сетях
	электросвязи Критерии комплексной оценки квалификации персонала, обслуживающего сооружения и

	СССЭ, средства и системы их защиты от НСД, средства для поиска признаков компьютерных атак в сетях электросвязи Методика выработки и реализации управленческого решения по обеспечению защиты сетей электросвязи от НСД и компьютерных атак в сетях электросвязи Правила ведения специального делопроизводства и технических документов средств связи сетей связи специального назначения Локальные нормативные акты и другие документы, определяющие политику и правила обеспечения информационной безопасности на предприятии (объекте) топливно-энергетического комплекса Содержание и порядок деятельности персонала по эксплуатации защищенных значимых объектов критической информационной инфраструктуры критической информационной инфраструктуры объектов топливно-энергетического комплекса и систем защиты информации
Общие по ИКТ	*Специальные по ИБ*
Основные угрозы безопасности информации и модели нарушителя в автоматизированных информационных и телекоммуникационных системах Типовые средства, методы и протоколы идентификации и аутентификации Основные криптографические методы, алгоритмы, протоколы защиты информации Принципы формирования политики информационной безопасности в автоматизированных системах Программно-аппаратные средства обеспечения	Назначение, особенности и условия применения различных видов СКЗИ, включая средства шифрования, средства имитозащиты, средства цифровой подписи, средства кодирования и средства изготовления ключевых документов. Типовые схемы построения СКЗИ и особенности их аппаратной и программной реализации с учетом среды функционирования Требования по составу и характеристикам средств криптографической защиты информации для различных классов защищенных автоматизированных систем, методы их практической реализации
безопасности информации, предназначенные для использования в типовых операционных системах, системах управления базами данных, компьютерных сетях Основные принципы и способы защиты информации в современных телекоммуникационных системах Принципы построения и функционирования современных операционных систем, систем	Основные характеристики средств измерений и контроля процесса и параметров функционирования средств криптографической защиты информации Критерии оценки эффективности и надежности встроенных средств защиты современных операционных систем, систем управления базами данных и компьютерных сетей Способы определения соответствия методов и средств криптографической защиты

управления базами данных и компьютерных сетей Общие принципы организации криптографической защиты персональных данных Общие принципы организации и функционирования удостоверяющих центров Основные угрозы безопасности информации и модели нарушителя в защищенных с использованием криптографических средств автоматизированных систем Принципы построения защищенного документооборота с использованием средств электронной подписи и виртуальных частных сетей Архитектура и принципы построения операционных систем Основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации Программные интерфейсы операционных систем Виды политик управления доступом и информационными потоками применительно к операционным системам Архитектура подсистем защиты информации в операционных системах	информации политике безопасности Методы измерений, контроля и технических расчетов характеристик программно-аппаратных средств защиты информации Средства и методы обнаружения ранее неизвестного вредоносного программного обеспечения Технические каналы утечки информации, возникающие за счет побочных электромагнитных излучений от основных технических средств, за счет наводок информативных сигналов на цепи электропитания и заземления основных технических средств и систем, вспомогательные технические средства и системы, их кабельные коммуникации, а также создаваемые методом "высокочастотного облучения" основных технических средств и систем и за счет возможно внедренных электронных устройств перехвата информации в основных технических средствах и системах Средства и методики контроля эффективности защиты информации от утечки за счет побочных электромагнитных излучений и наводок Способы реализации несанкционированного доступа к информации и специальных программных воздействий на информацию и ее носители в автоматизированных системах
Принципы функционирования средств защиты информации в операционных системах, в том числе использующих криптографические алгоритмы Состав типовых конфигураций программно-аппаратных средств защиты информации Требования по составу и характеристикам подсистем защиты информации применительно к операционным системам Порядок реализации методов и средств антивирусной защиты в операционных системах Программно-аппаратные средства и методы защиты информации в операционных системах Принципы работы и правила эксплуатации программно-аппаратных	Методы и средства защиты автоматизированных систем от несанкционированного доступа к информации и специальных программных воздействий на нее Методы контроля защищенности информации от несанкционированного доступа и специальных программных воздействий Средства и методики контроля защищенности информации от несанкционированного доступа Технические каналы утечки информации, возникающие за счет побочных электромагнитных излучений от основных технических средств, за счет наводок информативных сигналов на цепи электропитания и заземления основных технических средств и систем, вспомогательные технические средства и

средств защиты информации Принципы построения компьютерных сетей Стек сетевых протоколов операционных систем Стек протоколов сетевого оборудования Порядок реализации методов и средств межсетевого экранирования Принципы функционирования сетевых протоколов, включающих криптографические алгоритмы Виды политик управления доступом и информационными потоками в компьютерных сетях Источники угроз информационной безопасности в компьютерных сетях и меры по их предотвращению Программно-аппаратные средства и методы защиты информации в компьютерных сетях Структуры функциональной и обеспечивающих частей специальных ИАС	системы, их кабельные коммуникации, а также создаваемые методом "высокочастотного облучения" основных технических средств и систем и за счет возможно внедренных электронных устройств перехвата информации в основных технических средствах и системах Средства контроля защищенности информации от утечки за счет побочных электромагнитных излучений и наводок Методики проведения специальных исследований на побочные электромагнитные излучения и наводки технических средств обработки информации Методики расчета радиусов опасных зон побочных электромагнитных излучений и наводок Программные (программно-технические) средства защиты автоматизированных систем от несанкционированного доступа к информации и специальных программных воздействий на нее
Принципы эксплуатации и сопровождения ИАС Методы настройки, обслуживания и восстановления средств защиты информации на всех этапах жизненного цикла ИАС Источники и классификация угроз информационной безопасности Принципы функционирования автоматизированных систем поддержки документооборота и их безопасности Основные методы организационного обеспечения информационной безопасности ИАС Основные виды угроз безопасности операционных систем Защитные механизмы и средства обеспечения безопасности операционных систем Программные и программно-аппаратные средства защиты информации Принципы построения систем управления базами данных Основные средства и методы анализа программных реализаций Принципы построения антивирусного программного обеспечения	

Виды политик управления доступом и информационными потоками применительно к прикладному программному обеспечению Источники угроз информационной безопасности программного обеспечения и меры по их предотвращению Уязвимости используемого программного обеспечения и методы их эксплуатации Виды и формы функционирования вредоносного программного обеспечения	
Характерные признаки наличия вредоносного программного обеспечения Принципы функционирования программных средств криптографической защиты информации Порядок обеспечения безопасности информации при эксплуатации программного обеспечения Способы и средства защиты информации от утечки за счет побочных электромагнитных излучений и наводок Методы и средства защиты информации от несанкционированного доступа и специальных программных воздействий на нее Принципы построения современных сетей электросвязи, математические модели каналов связи, виды модуляции сигналов Возможные источники и технические каналы утечки информации Возможные угрозы НСД и компьютерных атак к сооружениям и СССЭ Сетевые протоколы и их параметры настройки Методы комплексного обеспечения защиты сетей электросвязи Системы распределенной обработки данных, используемые в ИАС Программное обеспечение процесса решения задач анализа информации в ИАС	
Эксплуатационная и проектная документация	*Эксплуатационная и проектная документация*

Содержание эксплуатационной документации автоматизированных информационных телекоммуникационных систем	Эксплуатационная и техническая документация на проверяемые и ремонтируемые СКЗИ Технические описания и инструкции по эксплуатации технических
	средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок Проектная документация на систему защиты объекта информатизации (в части защиты объекта от утечки информации за счет побочных электромагнитных излучений и наводок) Технические описания и инструкции по эксплуатации защищенных технических средств обработки информации Эксплуатационная и проектная документация на информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, обеспечивающие функционирование предприятий (объектов) топливно-энергетического комплекса
Уровень квалификации 7	
Общенаучные и общетехнические	*Специальные по техническим средствам*
Принципы построения систем управления базами данных Стандарты ЕСКД, ЕСТД и ЕСПД	Основные характеристики специальных электронных устройств перехвата информации
Нормативные, организационные, методические документы	*Нормативные, организационные, методические документы*
Национальные, межгосударственные и международные стандарты в области защиты информации Нормативные правовые акты Российской Федерации в области защиты информации Организационные меры по защите информации Национальные стандарты на проведение научно-исследовательских и опытно-конструкторских работ, сертификационных испытаний и создание систем защиты информации Порядок создания и структура отчета, создаваемого по результатам проверок	Нормативные правовые акты в области связи, информатизации и защиты информации Национальные, межгосударственные и международные стандарты в области средств и систем защиты сетей электросвязи от НСД и обеспечения безопасности критической информационной инфраструктуры Нормативные правовые акты по организации производства товаров и услуг в сфере защиты СССЭ от НСД, включая лицензирование такой деятельности Порядок сертификации средств и систем защиты СССЭ от НСД и компьютерных атак
Порядок создания автоматизированных систем в защищенном исполнении Нормы уголовного и административного права в сфере компьютерной информации	Порядок аттестации ЗТКС на соответствие требованиям защиты информации Порядок заказа и поставки программных, программно-аппаратных и технических средств и систем защиты СССЭ от НСД

Характеристики правонарушений в области связи и информации Виды преступлений в сфере компьютерной информации	Требования потребителей к уровню защищенности СССЭ от НСД Организационно-технические мероприятия по защите сетей связи специального назначения от НСД и их эффективность Нормативные правовые акты, руководящие и методические документы уполномоченных федеральных органов исполнительной власти, устанавливающие требования к системам защиты сетей связи специального назначения и их средств связи от НСД Нормативные правовые акты по организации защиты государственной тайны и конфиденциальной информации, задачам органов защиты государственной тайны Отчетные документы, оформляемые по результатам сертификационных испытаний программных (программно-технических) средств контроля защищенности информации от несанкционированного доступа на соответствие требованиям по безопасности информации Методики сертификационных испытаний программных (программно-технических) средств контроля защищенности информации от несанкционированного доступа на соответствие требованиям по безопасности информации Порядок аттестации выделенных (защищаемых) помещений на соответствие требованиям по защите информации Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации и обеспечению безопасности критической
	информационной инфраструктуры Способы организации работ при проведении сертификации программно-аппаратных средств защиты Порядок фиксации и документирования следов компьютерных преступлений, правонарушений и инцидентов в компьютерных системах и сетях Порядок проведения экспертизы вычислительной техники и носителей компьютерной информации с учетом нормативных правовых актов при расследовании компьютерных преступлений, правонарушений и инцидентов Порядок подготовки научно-технических

	экспертных заключений по результатам выполненных работ по информационно-аналитической и технической экспертизе компьютерных систем Порядок аттестации объектов информатизации на соответствие требованиям по защите информации Отчетные документы, оформляемые по результатам аттестации объектов вычислительной техники на соответствие требованиям по защите информации Порядок аттестации объектов информатизации на соответствие требованиям по защите информации Порядок организации технического обслуживания и ремонта технических, программных (программно-технических) средств защиты информации Нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и аттестации объектов информатизации на соответствие требованиям по защите информации
Общие по ИКТ	*Специальные по ИБ*
Принципы построения компьютерных систем и сетей Модели безопасности компьютерных систем Виды политик безопасности компьютерных систем и сетей Принципы построения средств криптографической защиты информации Возможности используемых и планируемых к использованию средств защиты информации Уязвимости компьютерных систем и сетей Криптографические методы защиты информации Принципы построения систем обнаружения компьютерных атак Форматы хранения информации в анализируемой компьютерной системе Основные форматы файлов, используемые в компьютерных системах Особенности хранения конфигурационной и системной информации в компьютерных системах	Способы и средства защиты акустической речевой информации от утечки по техническим каналам Средства и методики контроля защищенности акустической речевой информации от утечки по акустическим, вибрационным и акустооптическим каналам Средства и методики контроля защищенности акустической речевой информации от утечки по акустоэлектрическим и акустоэлектромагнитным каналам Администрирование системы защиты информации от несанкционированного доступа Методы проведения расследования компьютерных преступлений, правонарушений и инцидентов Методы анализа остаточной информации и поиска следов для фиксации компьютерных инцидентов Криптографические алгоритмы и особенности их программной реализации в компьютерных системах и сетях Технические каналы утечки информации, возникающие за счет побочных электромагнитных излучений от основных

Средства анализа конфигураций Современные информационные технологии (операционные системы, базы данных, вычислительные сети) Способы реализации несанкционированного доступа к информации и специальных программных воздействий на информацию и ее носители в автоматизированных системах Программные (программно-технические) средства защиты автоматизированных систем от несанкционированного доступа к информации и специальных программных	технических средств, за счет наводок информативных сигналов на цепи электропитания и заземления основных технических средств и систем, вспомогательные технические средства и системы, их кабельные коммуникации, а также создаваемые методом "высокочастотного облучения" основных технических средств и систем и за счет возможно внедренных электронных устройств перехвата информации в основных технических средствах и системах Способы реализации несанкционированного доступа к информации и специальных программных воздействий на
воздействий на нее Языки программирования и технологии программирования	информацию и ее носители в автоматизированных системах Способы и средства защиты информатизации от утечки за счет побочных электромагнитных излучений и наводок Методы и технологии защиты информации от несанкционированного доступа и специальных программных воздействий на нее Программные (программно-технические) средства защиты автоматизированных систем от несанкционированного доступа к информации и специальных программных воздействий на нее Средства и методики контроля защищенности информации от утечки за счет побочных электромагнитных излучений и наводок Средства и методики контроля защищенности информации от несанкционированного доступа и специальных программных воздействий Технические каналы утечки акустической речевой информации (прямые акустические, вибрационные, акустооптические, акустоэлектрические, акустоэлектромагнитные) Возможности средств акустической речевой разведки Технические каналы утечки акустической речевой информации, создаваемые за счет возможно внедренных специальных электронных устройств перехвата информации в технические средства и (или) предметы интерьера помещения. Состояние и перспективы развития систем защиты сетей

	электросвязи от НСД Модели угроз НСД к сетям электросвязи Основы моделирования ЗТКС и угрозы их информационной безопасности Методология менеджмента рисков информационной безопасности в телекоммуникационных системах и сетях электросвязи Основные производители и поставщики программных,
	программно-аппаратных и технических средств и систем защиты СССЭ от НСД, технические характеристики соответствующего оборудования и программного обеспечения Способы и средства защиты информации от утечки по техническим каналам и методы контроля их эффективности Методики оценки уязвимостей сетей связи специального назначения с точки зрения возможности НСД Средства анализа и контроля защищенности сетей связи специального назначения Основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения защиты сетей связи специального назначения от НСД Программно-аппаратные средства обеспечения защиты сетей связи специального назначения от НСД Основные угрозы НСД и модели нарушителя политики информационной безопасности сетей связи специального назначения Модели угроз НСД к сооружениям и средствам связи сетей связи специального назначения Состав и назначение аппаратно-программных средств защиты сооружений и средств связи сетей связи специального назначения от НСД Методы комплексного обеспечения защиты сооружений и средств связи сетей связи специального назначения от НСД Показатели эффективности применяемых программно-аппаратных (в том числе криптографических) и технических средств защиты средств связи сетей связи специального назначения от НСД Способы реализации несанкционированного доступа к информации и специальных программных воздействий на
	информацию и ее носители в

	автоматизированных системах Основные классы и виды уязвимостей программного обеспечения Методы и технологии защиты информации от несанкционированного доступа и специальных программных воздействий на нее Программные (программно-технические) средства защиты автоматизированных систем от несанкционированного доступа к информации и специальных программных воздействий на нее Средства и методики контроля защищенности информации от несанкционированного доступа Методики контроля защищенности информации от несанкционированного доступа Способы и средства защиты информации от утечки за счет побочных электромагнитных излучений и наводок Средства и методики контроля защищенности информации от утечки за счет побочных электромагнитных излучений и наводок Методики сертификационных испытаний технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок на соответствие требованиям по безопасности информации Отчетные документы, оформляемые по результатам сертификационных испытаний технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок на соответствие требованиям по безопасности информации Технические каналы утечки акустической речевой информации Методы и методики оценки безопасности программно-аппаратных средств защиты информации Принципы построения программно-аппаратных средств защиты информации Принципы построения подсистем защиты информации в компьютерных системах Методы оценки эффективности политики безопасности, реализованной в программно-аппаратных средствах защиты информации Методы и средства оценки корректности и эффективности программных реализаций алгоритмов защиты информации Методы анализа программного кода с целью

	поиска потенциальных уязвимостей и недокументированных возможностей Способы анализа применяемых методов и средств защиты информации на предмет соответствия политике безопасности Методы обработки данных мониторинга безопасности компьютерных систем и сетей Способы обнаружения и нейтрализации последствий вторжений в компьютерные системы Криптографические протоколы, применяемые в компьютерных сетях Технологии поиска и анализа следов компьютерных преступлений, правонарушений и инцидентов Методы анализа систем обеспечения информационной безопасности объектов информатизации на базе компьютерных систем в защищенном исполнении Основные классы и виды уязвимостей программного обеспечения

2. РАЗРАБОТКА ОБОРУДОВАНИЯ И СИСТЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

2.1. Типовые формулировки общепрофессиональных и специальных профессиональных умений

Общепрофессиональные умения	Специальные профессиональные умения
Уровень квалификации 7	
Аналитические (анализ, сопоставление, сравнение, мониторинг и др.)	*Аналитические (анализ, сопоставление, сравнение, мониторинг и др.)*
Анализировать основные характеристики и возможности телекоммуникационных систем по передаче информации Анализировать основные узлы и устройства современных автоматизированных систем Анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей систем защиты информации автоматизированных систем Оценивать информационные риски в автоматизированных системах и определять информационную инфраструктуру и информационные ресурсы, подлежащие защите Оценивать сложность алгоритмов и вычислений Анализировать цели создания автоматизированных систем и задачи, решаемые автоматизированными системами Выявлять уязвимости информационно-технологических ресурсов автоматизированных систем Систематизировать результаты проведенных исследований Определять эффективность применения средств	Строить и обосновывать математические модели процессов защиты информации, реализуемых в СКЗИ Проводить исследования математических моделей процессов защиты информации, реализуемых в СКЗИ Применять математические методы (методы алгебры, аналитической геометрии, математического анализа, теории функций комплексного переменного, теории вероятностей, математической статистики, теории информации и кодирования, теории чисел, теории графов, математической логики, теории алгоритмов, теории дискретных функций) для исследования математических моделей процессов защиты информации, реализуемых в СКЗИ Оценивать угрозы безопасности информации Анализировать возможные уязвимости информационных систем Выявлять известные уязвимости информационных систем Классифицировать и оценивать угрозы безопасности информации для автоматизированной системы
Информатизации Выполнять сбор, обработку, анализ и систематизацию научно-технической информации в области защиты информации Разрабатывать и исследовать математические модели конкретных явлений и процессов для решения	Проводить сбор и анализ исходных данных для проектирования средств и систем защиты СССЭ от НСД, средств для поиска признаков компьютерных атак в сетях электросвязи, ЗТКС Проводить сравнительный анализ сетей и систем передачи информации по показателям защиты информации

Общепрофессиональные умения	Специальные профессиональные умения
расчетных и исследовательских задач Выявлять информационные потребности автоматизируемых подразделений Производить формализацию предметной области с целью создания ИАС Строить инфологическую модель предметной области Описывать функциональную часть ИАС Выбирать эффективную технологию функционирования ИАС на базе моделирования Производить сравнительный анализ вариантов конфигураций и состава обеспечивающей части ИАС Разрабатывать проекты информационно-лингвистического обеспечения Работать с интегрированной средой разработки программного обеспечения Формализовывать предметную область с целью создания баз данных и экспертных систем Проводить анализ доступных информационных источников с целью выявления известных уязвимостей, используемых в системе защиты информации программных и программно-аппаратных средств	Классифицировать и оценивать угрозы безопасности информации для значимых объектов критической информационной инфраструктуры на предприятии (объекте) топливно-энергетического комплекса Исследовать эффективность проектных решений программно-аппаратных средств обеспечения защиты информации в значимых объектах критической информационной инфраструктуры объектов топливно-энергетического комплекса с целью обеспечения требуемого уровня защищенности Исследовать модели значимых объектов критической информационной инфраструктуры объектов топливно-энергетического комплекса и систем безопасности значимых объектов критической информационной инфраструктуры объектов топливно-энергетического комплекса
Коммуникационные/организационные/управленческие	*Коммуникационные/организационные/управленческие*
Производить изучение служебной деятельности	Организовывать работы по созданию, внедрению,
автоматизируемых подразделений	проектированию, разработке и сопровождению защищенных автоматизированных систем
Работа с документами:	*Работа с документами:*
Применять действующую нормативную базу в области обеспечения безопасности информации Готовить проекты технических заданий на проектирование ИАС Готовить проекты нормативно-распорядительных документов (приказов, указаний, инструкций) по вопросам создания и эксплуатации ИАС	Применение документов национальной системы стандартизации Российской Федерации в области криптографической защиты информации, государственных стандартов в области защиты информации ограниченного доступа, проектирования средств защиты информации, сертификации средств защиты информации на соответствие требованиям безопасности информации Применять нормативные документы по противодействию технической разведке
Разработка/проектирование общего ПО и технических средств:	*Разработка/проектирование специального ПО и технических средств:*

Общепрофессиональные умения	Специальные профессиональные умения
Проводить предпроектное обследование ОВТ (объект вычислительной техники) Проводить предпроектное обследование выделенного (защищаемого) помещения Проектировать и реализовывать политику безопасности вычислительных сетей Использовать стандартные методы и средства проектирования цифровых узлов и устройств, методы анализа электрических цепей Решать типовые задачи помехоустойчивого кодирования и декодирования сообщений Составлять техническое задание на разработку ИАС Готовить проектную документацию на создаваемые ИАС Разрабатывать проекты программного обеспечения ИАС Разрабатывать проекты математического обеспечения ИАС	Применять методы криптографического анализа для оценки стойкости алгоритмов криптографического преобразования, используемых в СКЗИ Применять методы анализа криптографических протоколов, применяемых в СКЗИ Оценивать качество криптографической защиты информации, осуществляемой СКЗИ, на основе проверки выполнения требований по безопасности информации, предъявляемых к СКЗИ Выполнение инженерно-криптографических исследований СКЗИ Проводить выбор, исследовать эффективность и проводить технико-экономическое обоснование проектных решений по применению СКЗИ с учётом заданных требований Оценивание технических каналов утечки информации при
Разрабатывать проекты технического обеспечения ИАС	функционировании СКЗИ Классифицировать и оценивать угрозы безопасности информации защищенных с использованием СКЗИ автоматизированных систем Проводить проверку работоспособности и эффективности применяемых СКЗИ Применять методики оценки защищенности программных, программно-аппаратных, аппаратных СКЗИ Разрабатывать предложения по совершенствованию системы управления информационной безопасностью защищенных с использованием СКЗИ автоматизированных систем Определять правила и процедуры управления системой криптографической защиты информации с использованием СКЗИ Разрабатывать предложения по устранению выявленных уязвимостей и совершенствованию системы управления криптографической защитой информации Оценка стойкости использованного криптографического алгоритма Оценка корректности встраивания криптографического средства Оценка невлияния среды на криптографические средства

Общепрофессиональные умения	Специальные профессиональные умения
	Разрабатывать технические задания на создание подсистем информационной безопасности автоматизированных систем Проектировать подсистемы безопасности информации с учетом действующих нормативных и методических документов Проводить технико-экономическое обоснование проектных решений программно-аппаратных средств обеспечения
	защиты информации в автоматизированной системе с целью обеспечения требуемого уровня защищенности Исследовать эффективность проектных решений программно-аппаратных средств обеспечения защиты информации в автоматизированной системе с целью обеспечения требуемого уровня защищенности Проводить комплексное тестирование и отладку аппаратных и программных систем защиты информации Разрабатывать технические задания на создание подсистем безопасности информации автоматизированных систем, проектировать такие подсистемы с учетом требований нормативных документов, ЕСКД и ЕСПД Разрабатывать модели автоматизированных систем и систем защиты информации автоматизированных систем Исследовать модели автоматизированных систем и систем защиты безопасности автоматизированных систем Применять математические модели при проектировании систем защиты информации автоматизированных систем Разрабатывать техническое задание на создание технического средства защиты информации от утечки за счет побочных электромагнитных излучений и наводок Разрабатывать проектно-сметную документацию на создание технического средства защиты информации от утечки за счет побочных электромагнитных излучений и наводок Проектировать технические средства защиты информации от утечки за счет побочных электромагнитных излучений и

Общепрофессиональные умения	Специальные профессиональные умения
	наводок с использованием современных программных средств проектирования электронных схем Разрабатывать конструкторскую, технологическую и
	эксплуатационную документацию по правилам, установленным стандартами ЕСКД, ЕСТД и ЕСПД Изготавливать опытный образец технического средства защиты информации от утечки за счет побочных электромагнитных излучений и наводок Разрабатывать программы и методики испытаний технического средства защиты информации от утечки за счет побочных электромагнитных излучений и наводок Проводить испытания технического средства защиты информации от утечки за счет побочных электромагнитных излучений и наводок Определять типы субъектов доступа и объектов доступа, являющихся объектами защиты Определять методы управления доступом, типы доступа и правила разграничения доступа к объектам доступа, подлежащим реализации в автоматизированной системе Выбирать меры защиты информации, подлежащие реализации в системе защиты информации автоматизированной системы Определять виды и типы средств защиты информации, обеспечивающих реализацию технических мер защиты информации Использовать рисковую методологию управления защитой информации в автоматизированной системе Определять класс защищенности автоматизированных систем и ее составных частей Производить выбор программно-аппаратных средств защиты информации для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности информации в автоматизированной
	системе Выявлять известные уязвимости информационных систем Разрабатывать техническое задание на

Общепрофессиональные умения	Специальные профессиональные умения
	создание технического средства защиты акустической речевой информации от утечки по техническим каналам Разрабатывать проектно-сметную документацию на создание технического средства защиты акустической речевой информации от утечки по техническим каналам Проектировать техническое средство защиты акустической речевой информации от утечки по техническим каналам с использованием современных программных средств проектирования электронных схем Проектировать с использованием современных программных средств проектирования программного (программно-технического) средство защиты информации от несанкционированного доступа и специальных воздействий на нее Разрабатывать конструкторскую, технологическую и эксплуатационную документацию по правилам, установленным стандартами ЕСКД, ЕСТД и ЕСПД Проектировать программное (программно-техническое) средство контроля защищенности информации от несанкционированного доступа Разрабатывать эскизный проект ОВТ в защищенном исполнении, Разрабатывать технический проект ОВТ в защищенном исполнении, Разрабатывать рабочую документацию на ОВТ в защищенном исполнении
	Проектировать средства и системы защиты СССЭ от НСД, средства для поиска признаков компьютерных атак в сетях электросвязи, ЗТКС с учетом нормативных правовых актов и методических документов Разрабатывать проекты, технические задания, планы и графики проведения работ по защите СССЭ от НСД, компьютерных атак в сетях электросвязи и необходимую техническую документацию Обеспечивать рациональный выбор элементной базы при проектировании устройств и систем защиты СССЭ от НСД,

Общепрофессиональные умения	Специальные профессиональные умения
	компьютерных атак в сетях электросвязи , ЗТКС Разрабатывать политику безопасности, выбирать методы и средства обеспечения информационной безопасности сетей электросвязи
	Разработка организационных, методических документов по ИБ
	Определять структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области защиты информации автоматизированных систем Определять меры (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для защиты информации в автоматизированных системах Формировать перечень мероприятий по предотвращению угроз безопасности информации автоматизированной системы Разрабатывать проекты нормативных документов, регламентирующих работу по защите информации в автоматизированных системах Разрабатывать предложения по совершенствованию системы
	управления защиты информации автоматизированных систем Разрабатывать предложения по совершенствованию системы управления защитой информации значимых объектов критической информационной инфраструктуры на предприятиях топливно-энергетического комплекса. Определять комплекс мер для обеспечения безопасности информационной в автоматизированных системах Определять информационную инфраструктуру и информационные ресурсы автоматизированной системы, подлежащие защите Разрабатывать эксплуатационную документацию на ОВТ в защищенном исполнении, а также организационно-распорядительную документацию по защите информации на объекте СВТ Составлять эксплуатационную и проектную документацию на систему

Общепрофессиональные умения	Специальные профессиональные умения
	защиты информации
Монтаж/наладка/ремонт технических средств	
Проводить комплексное тестирование аппаратных и программных средств	
Использование/применение общих технических средств	*Использование/применение специальных технических средств*
Применение средств современной микроэлектроники и цифровой схемотехники, чтение электрических принципиальных схем цифровых электронных устройств	Проводить технические работы и готовить заключения при аттестации защищенных с использованием СКЗИ автоматизированных систем на соответствие требованиям безопасности информации Проводить инструментальный мониторинг защищенности автоматизированных информационных и телекоммуникационных систем Контролировать безотказное функционирование технических средств защиты информации
	Восстанавливать (заменять) отказавшие технические средства защиты информации Проводить проверку работоспособности и эффективности применяемых программно-аппаратных (в том числе криптографических) и технических средств защиты сетей электросвязи от НСД Проводить инструментальный мониторинг защищенности СССЭ Проводить технические работы при аттестации СССЭ с учетом требований по защите информации
Уровень квалификации 8	
Аналитические (анализ, сопоставление, сравнение, мониторинг и др.)	*Аналитические (анализ, сопоставление, сравнение, мониторинг и др.)*
Обобщать научно-техническую литературу, нормативные и методические материалы в области защиты информации Подбирать и обобщать научно-техническую литературу, методические материалы по программным и аппаратным средствам и способам защиты информации, в том числе на английском языке	Формировать модели угроз и модели нарушителя безопасности компьютерных систем Выявлять наиболее целесообразные подходы к обеспечению защиты информации компьютерной системы Проводить исследования с целью нахождения наиболее целесообразных практических решений по обеспечению защиты информации Анализировать программные, архитектурно-технические и схемотехнические решения СССЭ с целью выявления потенциальных уязвимостей их защиты от НСД и компьютерных атак

Общепрофессиональные умения	Специальные профессиональные умения
	Проводить анализ выполнения требований защищенности СССЭ от НСД и компьютерных атак Проводить анализ и выбор состава, характеристик технологических процессов производства программных, программно-аппаратных (в том числе криптографических) и технических средств, и систем защиты СССЭ от НСД, средств
	для поиска признаков компьютерных атак в сетях электросвязи Выполнять анализ и обоснование системы мониторинга технологических процессов производства программных, программно-аппаратных (в том числе криптографических) и технических средств, и систем защиты СССЭ от НСД, средств для поиска признаков компьютерных атак в сетях электросвязи
Коммуникационные/организационные/управленческие	*Коммуникационные/организационные/управленческие*
	Осуществлять принятие решений о необходимости использования программно-аппаратных средств защиты информации
Работа с документами	*Работа с документами*
Применять действующую законодательную базу в области обеспечения компьютерной безопасности Применять действующую законодательную базу в области обеспечения защиты информации Применять национальные, межгосударственные и международные стандарты в области защиты информации Читать и понимать нормативные и методические документы по информационной безопасности на английском языке	
Разработка/проектирование общего ПО и технических средств:	*Разработка/проектирование специального ПО и технических средств:*
Использовать приемы защитного программирования Использовать приемы защиты от типовых атак компьютерных систем Применять методы и приемы отладки Применять методы и средства тестирования	Разрабатывать архитектуру и интерфейсы средств защиты информации, процедуры восстановления работоспособности средств и систем защиты после сбоев Обеспечивать подготовку исходных данных при разработке, исследовании сетей электросвязи, а также технических и программно-аппаратных средств их

Общепрофессиональные умения	Специальные профессиональные умения
	защиты от НСД, средств для поиска признаков компьютерных атак в сетях электросвязи Оценивать эффективность сетей электросвязи, а также
	технических и программно-аппаратных средств их защиты от НСД, средств для поиска признаков компьютерных атак в сетях электросвязи Разрабатывать и исследовать аналитические и компьютерные модели средств и систем защиты СССЭ от НСД, средств для поиска признаков компьютерных атак в сетях электросвязи Формировать технологическую документацию на производство программных, программно-аппаратных (в том числе криптографических) и технических средств, и систем защиты СССЭ от НСД, средств для поиска признаков компьютерных атак в сетях электросвязи Оценивать информационные риски в сетях электросвязи и определять информационную инфраструктуру и информационные ресурсы, подлежащие защите
Использовать/применять общее ПО	*Разработка организационных, методических документов по ИБ*
	Разрабатывать частные политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками
Монтаж/наладка/ремонт технических средств	
Использование/применение общих технических средств	*Использование/применение специальных технических средств*
Выбирать номенклатуру и характеристики технологического оборудования	Использовать технические, программно-аппаратные средства обеспечения защиты СССЭ от НСД, средства для поиска признаков компьютерных атак в сетях электросвязи

2.2. Типовые формулировки общепрофессиональных и специальных профессиональных знаний

Общепрофессиональные знания	Специальные профессиональные знания
Уровень квалификации 7	
Общенаучные и общетехнические	*Специальные технические*

Общепрофессиональные знания	Специальные профессиональные знания
Понятия и результаты, и методы аналитической геометрии, математического анализа, теории функций комплексного	Средства контроля защищенности информации от НСД, от утечки информации от утечки за счет побочных
переменного, теории меры Основные алгебраические структуры и их свойства Результаты и методы в области линейной алгебры, теории групп подстановок, теории матриц, теории полей, теории колец, линейных рекуррентных последовательностей над полем Понятия, результаты и методы теории чисел и её специальных разделов, связанных с применением эллиптических кривых и целочисленных решеток Понятия, результаты и методы комбинаторного анализа, теории графов, математической логики и теории алгоритмов, теории дискретных функций Понятия, результаты и методы теории вероятностей, математической статистики, теории информации и кодирования Стандарты ЕСКД, ЕСТД и ЕСПД Методы статистического анализа данных Эталонная модель взаимодействия открытых систем Основные понятия теории автоматов, математической логики, теории алгоритмов и теории графов Принципы работы элементов и функциональных узлов электронной аппаратуры, типовые схемотехнические решения основных узлов и блоков электронной аппаратуры Принципы организации документирования разработки и процесса сопровождения программного и аппаратного обеспечения Основы теории электрических цепей, методы анализа и синтеза электронных схем	электромагнитных излучений и наводок (ПЭМИН). Порядок создания автоматизированных систем в защищенном исполнении
Средства проектирования электронных схем	

Общепрофессиональные знания	Специальные профессиональные знания
Технологии производства электронной аппаратуры Технические каналы утечки акустической речевой информации Современные информационные технологии (операционные системы, базы данных, вычислительные сети) Основные классы и виды уязвимостей программного обеспечения Уязвимости информационных систем Назначение и классификация информационных и аналитических систем, систем управления Основные модели данных, модели представления знаний и программные средства работы с ними Логико-лингвистические основы обработки данных и знаний в ИАС Принципы проектирования реляционных баз данных Основные функциональные возможности современных систем управления базами данных	
Нормативные, организационные, методические документы	*Нормативные, организационные, методические документы*
Нормативные правовые акты Российской Федерации в области защиты информации Нормативные правовые акты Российской Федерации в области связи, информатизации Национальные, межгосударственные и международные стандарты в области информационной безопасности Нормативная база, регламентирующая создание и эксплуатацию ИАС Методики сертификационных испытаний технических средств защиты информации от несанкционированного доступа и	Законодательные акты Российской Федерации, нормативно-правовые акты, нормативно-методические документы уполномоченных государственных органов в области защиты информации ограниченного доступа, документы национальной системы стандартизации Российской Федерации в области криптографической защиты информации, Государственные стандарты проектирования средств защиты информации, сертификации средств защиты информации на соответствие требованиям безопасности информации и
утечки по техническим каналам на соответствие требованиям по безопасности информации Содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем защиты информации Специфические особенности функционирования подразделений, подлежащих автоматизации	аттестации автоматизированных и телекоммуникационных систем, объектов информатизации на соответствие требованиям безопасности информации, Нормативно-правовые акты Российской Федерации, нормативно-методические документы в области разработки, производства, реализации и эксплуатации СКЗИ Регламент проведения расследований

Общепрофессиональные знания	Специальные профессиональные знания
Инструкции по организации обследования автоматизируемых подразделений	нарушений условий эксплуатации СКЗИ Нормативно-правовые основания для проведения, методические материалы по проведению, порядок оформления заявок на проведение, порядок организации, порядок анализа и реализации результатов контрольно-технических мероприятий по оценке защищенности и аттестации защищенных с использованием СКЗИ автоматизированных систем Организационно-технические мероприятия по защите защищенных с использованием СКЗИ автоматизированных систем Отчетные документы, оформляемые по результатам аттестации защищенных с использованием СКЗИ автоматизированных систем на соответствие требованиям безопасности информации Законодательные акты Российской Федерации, нормативно-правовые акты, нормативно-методические документы уполномоченных государственных органов, документы национальной системы стандартизации Российской Федерации в области криптографической защиты информации, государственные стандарты в области защиты информации ограниченного доступа, сертификации средств
	защиты информации и аттестации автоматизированных и телекоммуникационных систем, объектов информатизации на соответствие требованиям безопасности информации Методики оценки уязвимостей защищенных с использованием криптографических средств автоматизированных систем Методики контроля защищенности информации от НСД, от утечки по каналам ПЭМИН Организационно-технические мероприятия по обеспечению защиты автоматизированных систем от НСД и их эффективность Организационные основы защиты информации от несанкционированного доступа и утечки по техническим каналам на объектах информатизации Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации

Общепрофессиональные знания	Специальные профессиональные знания
	Нормативные правовые акты и национальные стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации Национальные, межгосударственные и международные стандарты в области защиты информации Порядок аттестации объектов информатизации на соответствие требованиям безопасности информации Организационно-распорядительная документация по защите информации на выделенное (защищаемое) помещение Законодательство Российской Федерации в области обеспечения безопасности критической информационной инфраструктуры, нормативные правовые акты Президента
	Российской Федерации, Правительства Российской Федерации, федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, федерального органа исполнительной власти, уполномоченного в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, министерства энергетики Российской Федерации. Основные методические и руководящие документы уполномоченных федеральных органов исполнительной власти по защите информации в областях, относящихся к областям функционирования значимых объектов критической информационной инфраструктуры (информационной безопасности) Локальные нормативные акты и другие документы, определяющие политику и правила обеспечения информационной безопасности на предприятии (объекте) топливно-энергетического комплекса
Общие по ИКТ	*Специальные по информационной безопасности;*
Модели нарушителя и угрозы безопасности информации Основные угрозы безопасности	Методы криптографического анализа для оценки стойкости алгоритмов криптографического преобразования,

Общепрофессиональные знания	Специальные профессиональные знания
информации и модели нарушителя в автоматизированных и телекоммуникационных системах Принципы формирования и реализации политики безопасности информации Принципы построения защищенных с использованием криптографических средств автоматизированных систем	используемых в СКЗИ Криптографические методы и средства защиты информации Принципы построения защищенных с использованием криптографических средств автоматизированных информационных и телекоммуникационных систем Методы анализа криптографических протоколов,
Технические каналы утечки информации. Методы, способы и средства защиты информации от несанкционированного доступа, от утечки по техническим каналам и контроля эффективности защиты информации Общие принципы построения системы криптографической защиты информации Принципы построения и функционирования систем и сетей передачи информации Основные меры по защите информации в автоматизированных системах Принципы построения средств защиты информации от несанкционированного доступа и утечки по техническим каналам Организационные меры по защите информации Принципы построения и функционирования, примеры реализаций современных локальных и глобальных компьютерных сетей и их компонентов Основные информационные технологии, используемые в автоматизированных системах Средства и способы обеспечения безопасности информации, принципы построения систем защиты информации Языки и современные технологии программирования Особенности защиты информации в автоматизированных системах управления технологическими процессами Методы тестирования и отладки программного и аппаратного обеспечения	применяемых в СКЗИ Элементная база для аппаратной реализации СКЗИ (современная микроэлектронная компонентная база, схемотехническая реализация типовых операций криптографических алгоритмов, архитектура и характеристики основных серий программируемых логических интегральных схем, методы и этапы проектирования цифровых узлов электронных устройств) Методы инженерно-криптографических исследований СКЗИ, математические модели функционирования СКЗИ с учётом возможных неисправностей Принципы разработки технико-экономического обоснования проектируемой системы криптографической защиты информации Характеристики технических каналов утечки информации при функционировании СКЗИ Основные угрозы и модели нарушителя политики информационной безопасности защищенных с использованием СКЗИ автоматизированных систем Основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности информации в автоматизированных системах Модели угроз НСД к защищенным с использованием криптографических средств автоматизированных информационных и телекоммуникационным системам Методы, средства анализа и контроля защищенности СКЗИ Способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации

Общепрофессиональные знания	Специальные профессиональные знания
Архитектура, основные модели, последовательность и содержание этапов проектирования, физическая организация баз данных	
Общие сведения о методах проектирования, документирования, разработки, тестирования и отладки компонентов обеспечивающей части ИАС Принципы эксплуатации и сопровождения ИАС Структуры функциональной и обеспечивающих частей ИАС Методы проведения предпроектного обследования при разработке ИАС Средства и методы хранения и передачи информации Принципы построения защищенных телекоммуникационных систем Методы проектирования ИАС Основы моделирования функционирования ЗТКС Методы, способы и средства обеспечения отказоустойчивости автоматизированных систем Последствия от нарушения свойств безопасности информации Основные средства и способы обеспечения безопасности информации, принципы построения систем защиты информации Принципы построения средств защиты информации от несанкционированного доступа и утечки по техническим каналам Методы тестирования и отладки, принципы организации документирования разработки, процесса сопровождения программного обеспечения Основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации Источники и классификация угроз информационной безопасности	Особенности защиты информации в автоматизированных системах управления технологическими процессами Технические средства контроля эффективности мер защиты информации Критерии оценки эффективности и надежности средств защиты информации программного обеспечения автоматизированных систем Принципы организации и структура систем защиты информации программного обеспечения автоматизированных систем Основные характеристики технических средств защиты информации от несанкционированного доступа и утечек по техническим каналам Принципы формирования политики информационной безопасности в автоматизированных системах Основные методы управления информационной безопасностью Угрозы безопасности, информационные воздействия, критерии оценки защищенности и методы защиты информации в автоматизированных системах Методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем и систем защиты информации автоматизированных системах Программно-аппаратные средства обеспечения защиты информации в программном обеспечении автоматизированных систем Основные средства, способы и принципы построения систем защиты информации автоматизированных систем Профессиональная и криптографическая терминология в
	области безопасности информации Виды информационных воздействий и критерии оценки защищенности информации в автоматизированных системах

Общепрофессиональные знания	Специальные профессиональные знания
	Методы защиты информации от несанкционированного доступа и утечки по техническим каналам Программно-аппаратные средства обеспечения защиты информации в программном обеспечении автоматизированных систем Основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности в вычислительных сетях Способы реализации угроз безопасности в автоматизированных системах Способы и средства защиты информации от несанкционированного доступа и утечки по техническим каналам и контроля эффективности защиты информации Методы и технологии проектирования, моделирования, исследования систем защиты информации автоматизированных систем Технические каналы утечки информации, возникающие за счет побочных электромагнитных излучений от основных технических средств, за счет наводок информативных сигналов на цепи электропитания и заземления основных технических средств и систем, вспомогательные технические средства и системы, их кабельные коммуникации, а также создаваемые методом "высокочастотного облучения" основных технических средств и систем и за счет возможно внедренных электронных устройств перехвата информации в основных технических средствах и системах
	Программно-аппаратные средства обеспечения защиты информации автоматизированных систем Программные (программно-технические) средства защиты автоматизированных систем от несанкционированного доступа к информации и специальных программных воздействий на нее Модели угроз НСД к сетям электросвязи Методики оценки уязвимостей сетей электросвязи с точки зрения возможности НСД к ним Средства анализа и контроля защищенности СССЭ Технологии, методы, языки и средства

Общепрофессиональные знания	Специальные профессиональные знания
	программирования, применяемые для создания программного обеспечения в составе СССЭ, а также средств и систем защиты СССЭ от НСД, средств для поиска признаков компьютерных атак в сетях электросвязи , ЗТКС Модель угроз информационной безопасности, модель нарушителя информационной безопасности на предприятии (объекте) топливно-энергетического комплекса Основные угрозы безопасности информации и модели нарушителя в значимых объектах критической информационной инфраструктуры объектов топливно-энергетического комплекса Основные меры по защите информации в значимых объектах критической информационной инфраструктуры объектов топливно-энергетического комплекса Особенности защиты информации в значимых объектах критической информационной инфраструктуры объектов топливно-энергетического комплекса управления технологическими процессами
	Основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в значимых объектах критической информационной инфраструктуры объектов топливно-энергетического комплекса Технические средства контроля эффективности мер защиты информации
	Эксплуатационная и проектная документация
	Содержание эксплуатационной документации на средства и системы криптографической защиты информации Эксплуатационная документация на систему защиты информации выделенного (защищаемого) помещения
Уровень квалификации 8	
Общенаучные и общетехнические	*Специальные технические*
Теоретико-числовые методы и алгоритмы, применяемые в средствах защиты информации	
Нормативные, организационные, методические документы	*Нормативные, организационные, методические документы*
Нормативные правовые акты в области связи, информатизации и защиты	Национальные, межгосударственные и международные стандарты в области защиты

Общепрофессиональные знания	Специальные профессиональные знания
информации Организационные меры по защите информации	информации Национальные, межгосударственные и международные стандарты в области средств и систем защиты сетей электросвязи от НСД, средств для поиска признаков компьютерных атак в сетях электросвязи Нормативные правовые акты по организации производства товаров и услуг в сфере защиты СССЭ от НСД, средств для поиска признаков компьютерных атак в сетях электросвязи Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации и безопасности критической информационной
	инфраструктуры Порядок организации работ по защите информации в компьютерных системах и сетях Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации и обеспечению безопасности критической информационной инфраструктуры Принципы и методы управления проектами в области информационной безопасности Порядок организации работ по защите информации
Общие по ИКТ	*Специальные по информационной безопасности;*
Методы и средства получения, обработки и передачи информации в операционных системах, системах управления базами данных и компьютерных сетях Принципы построения средств защиты информации компьютерных систем Формальные модели управления доступом в компьютерных системах и сетях Принципы и методы проектирования программно-аппаратного обеспечения Методологии и технологии разработки программного обеспечения Принципы проектирования антивирусного программного обеспечения Модели угроз информационной безопасности сетей электросвязи	Методы анализа безопасности компьютерных систем Виды атак и механизмы их реализации в компьютерных системах Методы выявления каналов утечки информации в компьютерных системах и сетях Методы и средства защиты информации в компьютерных сетях, операционных системах и системах управления базами данных Криптографические алгоритмы и особенности их программной реализации в компьютерных системах и сетях Криптографические алгоритмы и особенности их программной реализации Методы планирования и организации проведения работ по защите информации и обеспечению государственной тайны Методы проведения специальных

Общепрофессиональные знания	Специальные профессиональные знания
Основные информационные технологии, используемые в сетях электросвязи Принципы построения ЗТКС	исследований и проверок, работ по защите информации Основные характеристики способов, средств и систем защиты СССЭ от НСД и компьютерных атак
	Основы моделирования ЗТКС Элементная база производства программных, программно-аппаратных (в том числе криптографических) и технических средств, и систем защиты СССЭ от НСД, средств для поиска признаков компьютерных атак в сетях электросвязи Методология испытаний программных, программно-аппаратных (в том числе криптографических) и технических средств, и систем защиты СССЭ от НСД, средств для поиска признаков компьютерных атак в сетях электросвязи Принципы построения системы мониторинга технологических процессов производства программных, программно-аппаратных (в том числе криптографических) и технических средств, и систем защиты СССЭ от НСД, средств для поиска признаков компьютерных атак в сетях электросвязи Требования к показателям качества программных, программно-аппаратных (в том числе криптографических) и технических средств, и систем защиты СССЭ от НСД, средств для поиска признаков компьютерных атак в сетях электросвязи