Функциональные квалификационные требования
к категориям и группам должностей государственной гражданской службы

Направление профессиональной служебной деятельности:
Управление в сфере информации и информационных технологий

Специализация по направлению профессиональной служебной деятельности:
Осуществление технической защита информации от утечки по техническим каналам, несанкционированного доступа и обеспечение безопасности информации в ключевых системах информационной инфраструктуры

Наименование федерального государственного органа
Федеральная служба по техническому и экспортному контролю

<table>
<tr><th colspan="3">Категория «руководители» высшей и главной групп должностей</th></tr>
<tr><td colspan="2">I. Требования к направлению подготовки (специальности) профессионального образования</td><td>К магистрам:
направление подготовки «Информационная безопасность».
К специалистам:
направления подготовки (специальности) «Безопасность информационных технологий в правоохранительной сфере», «Информационная безопасность автоматизированных систем», «Информационная безопасность телекоммуникационных систем».
Иное направление подготовки (специальность), для которого законодательством об образовании Российской Федерации установлено соответствие направлению подготовки (специальности), указанному в предыдущих перечнях профессий, специальностей и направлений подготовки.</td></tr>
<tr><td rowspan="2">II. Требования к профессиональным знаниям</td><td>1. Профессиональные знания в области законодательства Российской Федерации</td><td>Знать основные законодательные и правовые акты в области защиты информации, в том числе в области обеспечения безопасности персональных данных, и обеспечения безопасности информации в ключевых системах информационной инфраструктуры и перспективы их дальнейшей разработки (0.1, 0.2, 0.3, 0.4, 0.5, 0.6, 0.7, 0.8, 0.9, 0.10, 0.11);
основные нормативные правовые акты в области сертификации средств защиты информации по требованиям безопасности информации
государственную систему противодействия иностранным техническим разведкам и технической защиты информации;
нормативные правовые акты и организационные основы защиты информации в Российской Федерации;
функции и задачи ФСТЭК России и управлений ФСТЭК России по федеральным округам по технической защите информации.</td></tr>
<tr><td>2. Иные профессиональные знания</td><td>Знание основных понятий в области технической защиты информации и обеспечения безопасности информации в ключевых системах информационной инфраструктуры;
технических каналов утечки информации ограниченного доступа, возникающих при ее</td></tr>
</table>

		обработке, физических явлений, лежащих в основе появления различных каналов утечки информации, в части касающейся побочных электромагнитных излучений и наводок, акустических и виброакустических каналов; каналов утечки информации при эксплуатации электронных вычислительных машин, автоматизированных систем управления, волоконно-оптических систем передачи информации и беспроводных устройств передачи данных; системы организации комплексной защиты информации, действующей в органе государственной власти, организации; перспективных направлений развития технических методов и средств защиты информации ограниченного доступа, программно-аппаратных средств защиты информации от утечки по техническим каналам, методов и средств защиты информации (носителей информации) от специальных воздействий; основ методологии и методики проведения технической защиты информации в органе государственной власти, организации; характера взаимодействия подразделений и служб организаций в процессе проведения исследований и разработок с использованием информации ограниченного доступа; методов и средств контроля за состоянием технической защиты информации; отечественного и зарубежного опыта в области технической защиты информации; методов и средств получения, обработки и передачи информации; методов и процедур выявления угроз безопасности информации на объектах информатизации организации; средств защиты информации от различных видов угроз безопасности информации; средств контроля эффективности технической защиты информации по различным физическим полям; порядка оформления технической документации по защите информации; классификации факторов, воздействующих на защищаемую информацию, физические основы образования технических каналов утечки информации и их свойства; системы защиты информации в автоматизированной системе в защищенном исполнении, классы защищенности автоматизированных систем; методов и порядка организации и проведения специальных исследований , специальных проверок, экспертиз, тестовых испытаний и контрольных проверок, процедур сертификации, аттестации и лицензирования; типовые проектные решения по применению средств и систем технической защиты информации. целей, задач, основных принципов организации, методов и средств ведения контроля состояния защищенности информации ограниченного доступа в органе государственной власти, организации;

		порядка оформления технической документации по защите информации; методов и порядка обработки результатов контроля, анализа и оценки защищенности объектов информатизации, порядка подготовки актов по результатам специальных исследований, специальных проверок, протоколов измерений, предписаний на право эксплуатации объектов, систем и средств в защищенном исполнении и других документов по результатам контроля (оценки); признаков, критериев и порядка отнесения информационно-телекоммуникационных систем, функционирующих в составе критически важных объектов, к числу защищаемых от деструктивных информационных воздействий; порядка, методов и средств выявления угроз безопасности информации в ключевых системах информационной инфраструктуры; основных направлений деятельности и особенностей организации работ по обеспечению безопасности информации в ключевых системах информационной инфраструктуры при их создании и эксплуатации; форм осуществления оценки соответствия ключевых систем информационной инфраструктуры требованиям по безопасности информации. методических основ и методики оценки опасности угроз утечки информации ограниченного доступа по различным каналам; целей, задач, основных принципов организации, методов и средств ведения контроля состояния защищенности информации ограниченного доступа в органах государственной власти, организациях; основ методологии и методики проведения аттестации объектов информатизации в органах государственной власти, организациях; методов и средств контроля за состоянием объектов информатизации; отечественного и зарубежного опыта в области сертификации средств защиты информации; перечня сертифицированных средств защиты информации, их характеристик по основному назначению; средств контроля эффективности средств защиты информации; порядка оформления технической документации по аттестации объектов информатизации; построение и функции системы защиты информации в автоматизированной системе в защищенном исполнении, классы защищенности автоматизированных систем; методов и порядка организации и проведения специальных исследований, экспертиз, тестовых испытаний и контрольных проверок, процедур сертификации, аттестации, оформления и выдачи аттестатов соответствия; методов и порядка обработки результатов контроля, анализа и оценки защищенности объектов информатизации с проведением расчетов, порядка подготовки актов по результатам специальных исследований, протоколов измерений, предписаний на право эксплуатации

		объектов, систем и средств в защищенном исполнении и других документов по результатам контроля (оценки).
III. Требования к профессиональным навыкам		Навыки работы с нормативными правовыми актами в области защиты информации и обеспечения безопасности информации в ключевых системах информационной инфраструктуры; работы с правовыми базами данных, базами данных, содержащих информацию ограниченного доступа, в том числе по угрозам безопасности информации в органе государственной власти, организации, в ключевой системе информационной инфраструктуры; разработка необходимых документов в интересах организации работ по защите информации и обеспечению безопасности информации в ключевых системах информационной инфраструктуры в масштабах организации; разработка необходимых документов в интересах организации работ по сертификации средств защиты информации и аттестации объектов информатизации; проведения работ, связанных с защитой информации и контролем ее эффективности; проектирования, построения и эксплуатации комплексной системы защиты информации; определения уровня защищенности персональных данных; выявления угроз безопасности информации, в том числе персональных данных, в информационных системах; работы с нормативными и методическими документами по обеспечению безопасности информации в ключевых системах информационной инфраструктуры и контроля; составления и корректировки перечней ключевых систем информационной инфраструктуры различных уровней принадлежности и важности; проведения сравнительного анализа характеристик (показателей) разных классов средств обеспечению безопасности информации и технико-экономического обоснования выбора предпочтительных. планирования и организации работ проведения работ в области технической защиты информации на уровне объекта информатизации; проведения аттестации объектов информатизации, программ, алгоритмов на предмет соответствия требованиям технической защиты информации по соответствующим классам безопасности; оценки возможностей технических разведок, выявления угроз безопасности, технических каналов утечки информации, выявления нарушений в использовании основных и вспомогательных технических систем и средств при обработке информации ограниченного доступа; использования и обслуживания технических средств контроля, составления планирующих, отчетных документов и рекомендаций по результатам оценки, подготовки проектов договоров; планирования, организации и контроля выполнения мероприятий по проектированию и эксплуатации защищенных объектов информатизации;

	разработки методик анализа проектной и эксплуатационной документации, методик оценки эффективности мероприятий по технической защите информации ограниченного доступа на уровне отрасли, организации; проведения специальных экспертиз и (или) аттестации объектов информатизации; подготовка заключений и итоговой отчетной документации. проведения экспертизы материалов сертификационных испытаний средств защиты информации; проведения специальных экспертиз по вопросам оценки возможности аккредитации организаций в качестве органов по сертификации средств защиты информации и испытательных лабораторий; умения разрабатывать документы по результатам сертификационных испытаний средств защиты информации и работ по аттестации объектов информатизации.

Направление профессиональной служебной деятельности:
Управление в сфере информации и информационных технологий

Специализация по направлению профессиональной служебной деятельности:
Осуществление технической защиты информации от несанкционированного доступа и обеспечение безопасности информации в ключевых системах информационной инфраструктуры

Наименование федерального государственного органа:
Федеральная служба по техническому и экспортному контролю

Категория «специалисты» главной и ведущей групп должностей государственной гражданской службы		
I. Требования к направлению подготовки (специальности) профессионального образования		**К магистрам:** направление подготовки «Информационная безопасность». **К специалистам:** направления подготовки (специальности) «Безопасность информационных технологий в правоохранительной сфере», «Информационная безопасность автоматизированных систем», «Информационная безопасность телекоммуникационных систем». Иное направление подготовки (специальность), для которого законодательством об образовании Российской Федерации установлено соответствие направлению подготовки (специальности), указанному в предыдущих перечнях профессий, специальностей и направлений подготовки.
II. Требования к профессиональным знаниям	1. Профессиональные знания в области законодательства Российской Федерации	Знать основные законодательные и правовые акты в области защиты информации, в том числе в области обеспечения безопасности персональных данных, и обеспечения безопасности информации в ключевых системах информационной инфраструктуры и перспективы их дальнейшей разработки (0.1, 0.2, 0.3, 0.4, 0.5, 0.6, 0.7, 0.8, 0.9); государственную систему противодействия иностранным техническим разведкам и технической защиты информации. функции и задачи ФСТЭК России и управлений ФСТЭК России по федеральным округам по технической защите информации.
	2. Иные профессиональные знания	Знание основных понятий в области технической защиты информации и обеспечения безопасности информации в ключевых системах информационной инфраструктуры; системы организации комплексной защиты информации, действующей в органе государственной власти, организации; основ методологии и методики проведения технической защиты информации в органе государственной власти, организации; методов и средств получения, обработки и передачи информации;

		методов и процедур выявления угроз безопасности информации на объектах информатизации организации; средств защиты информации от различных видов угроз безопасности информации; целей, задач, основных принципов организации, методов и средств ведения контроля состояния защищенности информации ограниченного доступа в органе государственной власти, организации; порядка оформления технической документации по защите информации; методов и порядка обработки результатов контроля, анализа и оценки защищенности объектов информатизации, порядка подготовки актов по результатам специальных исследований, специальных проверок, протоколов измерений, предписаний на право эксплуатации объектов, систем и средств в защищенном исполнении и других документов по результатам контроля (оценки); признаков, критериев и порядка отнесения информационно-телекоммуникационных систем, функционирующих в составе критически важных объектов, к числу защищаемых от деструктивных информационных воздействий; порядка, методов и средств выявления угроз безопасности информации в ключевых системах информационной инфраструктуры; основных направлений деятельности и особенностей организации работ по обеспечению безопасности информации в ключевых системах информационной инфраструктуры при их создании и эксплуатации; форм осуществления оценки соответствия ключевых систем информационной инфраструктуры требованиям по безопасности информации.
III. Требования к профессиональным навыкам		Навыки работы с нормативными правовыми актами в области защиты информации и обеспечения безопасности информации в ключевых системах информационной инфраструктуры; работы с правовыми базами данных, базами данных, содержащих информацию ограниченного доступа, в том числе по угрозам безопасности информации в органе государственной власти, организации, в ключевой системе информационной инфраструктуры; разработка необходимых документов в интересах организации работ по защите информации и обеспечению безопасности информации в ключевых системах информационной инфраструктуры в масштабах организации; проведения работ, связанных с защитой информации и контролем ее эффективности; проектирования, построения и эксплуатации комплексной системы защиты информации; определения уровня защищенности персональных данных; выявления угроз безопасности информации, в том числе персональных данных, в информационных системах; работы с нормативными и методическими документами по обеспечению безопасности информации в ключевых системах информационной инфраструктуры и контроля;

	составления и корректировки перечней ключевых систем информационной инфраструктуры различных уровней принадлежности и важности; проведения сравнительного анализа характеристик (показателей) разных классов средств обеспечению безопасности информации и технико-экономического обоснования выбора предпочтительных.

Направление профессиональной служебной деятельности:
Управление в сфере информации и информационных технологий

Специализация по направлению профессиональной служебной деятельности:
Осуществление технической защиты информации от несанкционированного доступа и обеспечение безопасности информации в ключевых системах информационной инфраструктуры

Наименование федерального государственного органа:
Федеральная служба по техническому и экспортному контролю

Категория «специалисты старшей группы должностей государственной гражданской службы		
I. Требования к направлению подготовки (специальности) профессионального образования		**К специалистам:** направления подготовки (специальности) «Безопасность информационных технологий в правоохранительной сфере», «Информационная безопасность автоматизированных систем», «Информационная безопасность телекоммуникационных систем». **К бакалаврам:** Направление подготовки «Информационная безопасность». Иное направление подготовки (специальность), для которого законодательством об образовании Российской Федерации установлено соответствие направлению подготовки (специальности), указанному в предыдущих перечнях профессий, специальностей и направлений подготовки.
II. Требования к профессиональным знаниям	1. Профессиональные знания в области законодательства Российской Федерации	Знать основные законодательные и правовые акты в области защиты информации, в том числе в области обеспечения безопасности персональных данных, и обеспечения безопасности информации в ключевых системах информационной инфраструктуры и перспективы их дальнейшей разработки (0.1, 0.2, 0.3, 0.4, 0.5, 0.6, 0.7, 0.8, 0.9); государственную систему противодействия иностранным техническим разведкам и технической защиты информации. функции и задачи ФСТЭК России и управлений ФСТЭК России по федеральным округам по технической защите информации.
	2. Иные профессиональные знания	Знание основных понятий в области технической защиты информации и обеспечения безопасности информации в ключевых системах информационной инфраструктуры; системы организации комплексной защиты информации, действующей в органе государственной власти, организации; основ методологии и методики проведения технической защиты информации в органе государственной власти, организации; методов и средств получения, обработки и передачи информации;

		методов и процедур выявления угроз безопасности информации на объектах информатизации организации; средств защиты информации от различных видов угроз безопасности информации; целей, задач, основных принципов организации, методов и средств ведения контроля состояния защищенности информации ограниченного доступа в органе государственной власти, организации; порядка оформления технической документации по защите информации; методов и порядка обработки результатов контроля, анализа и оценки защищенности объектов информатизации, порядка подготовки актов по результатам специальных исследований, специальных проверок, протоколов измерений, предписаний на право эксплуатации объектов, систем и средств в защищенном исполнении и других документов по результатам контроля (оценки); признаков, критериев и порядка отнесения информационно-телекоммуникационных систем, функционирующих в составе критически важных объектов, к числу защищаемых от деструктивных информационных воздействий; порядка, методов и средств выявления угроз безопасности информации в ключевых системах информационной инфраструктуры; основных направлений деятельности и особенностей организации работ по обеспечению безопасности информации в ключевых системах информационной инфраструктуры при их создании и эксплуатации; форм осуществления оценки соответствия ключевых систем информационной инфраструктуры требованиям по безопасности информации.
III. Требования к профессиональным навыкам		Навыки работы с нормативными правовыми актами в области защиты информации и обеспечения безопасности информации в ключевых системах информационной инфраструктуры; работы с правовыми базами данных, базами данных, содержащих информацию ограниченного доступа, в том числе по угрозам безопасности информации в органе государственной власти, организации, в ключевой системе информационной инфраструктуры; разработка необходимых документов в интересах организации работ по защите информации и обеспечению безопасности информации в ключевых системах информационной инфраструктуры в масштабах организации; проведения работ, связанных с защитой информации и контролем ее эффективности; проектирования, построения и эксплуатации комплексной системы защиты информации; определения уровня защищенности персональных данных; выявления угроз безопасности информации, в том числе персональных данных, в информационных системах; работы с нормативными и методическими документами по обеспечению безопасности информации в ключевых системах информационной инфраструктуры и контроля;

	составления и корректировки перечней ключевых систем информационной инфраструктуры различных уровней принадлежности и важности; проведения сравнительного анализа характеристик (показателей) разных классов средств обеспечению безопасности информации и технико-экономического обоснования выбора предпочтительных.

Направление профессиональной служебной деятельности:
Управление в сфере информации и информационных технологий

Специализация по направлению профессиональной служебной деятельности:
Осуществление технической защита информации от утечки по техническим каналам

Наименование федерального государственного органа
Федеральная служба по техническому и экспортному контролю

Категория «специалисты» главной и ведущей групп должностей государственной гражданской службы		
I. Требования к направлению подготовки (специальности) профессионального образования		**К магистрам:** направление подготовки «Информационная безопасность». **К специалистам:** направления подготовки (специальности) «Безопасность информационных технологий в правоохранительной сфере», «Информационная безопасность автоматизированных систем», «Информационная безопасность телекоммуникационных систем». Иное направление подготовки (специальность), для которого законодательством об образовании Российской Федерации установлено соответствие направлению подготовки (специальности), указанному в предыдущих перечнях профессий, специальностей и направлений подготовки.
II. Требования к профессиональным знаниям	1. Профессиональные знания в области законодательства Российской Федерации	Знание основных законодательных и правовых актов в области технической защиты информации и перспективы их дальнейшей разработки (0.1, 0.2, 0.3, 0.5, 0.6, 0.7, 0.9). Знание государственной системы противодействия иностранным техническим разведкам и технической защиты информации. Знание нормативных правовых актов и организационных основ защиты информации в Российской Федерации. Знание функций и задач ФСТЭК России и управлений ФСТЭК России по федеральным округам по технической защите информации.
	2. Иные профессиональные знания	Знание: технических каналов утечки информации ограниченного доступа, возникающих при ее обработке, физических явлений, лежащих в основе появления различных каналов утечки информации, в части касающейся побочных электромагнитных излучений и наводок, акустических и виброакустических каналов; каналов утечки информации при эксплуатации электронных вычислительных машин, автоматизированных систем управления, волоконно-оптических систем передачи информации и беспроводных устройств передачи данных; характеристик различных типов информационных сигналов, содержащих информацию

		ограниченного доступа (акустических, виброакустических, электрических, электромагнитных); системы организации комплексной защиты информации, действующей в органе государственной власти, организации; перспективных направлений развития технических методов и средств защиты информации ограниченного доступа, программно-аппаратных средств защиты информации от утечки по техническим каналам, методов и средств защиты информации (носителей информации) от специальных воздействий; основ методологии и методики проведения технической защиты информации в органе государственной власти, организации; характера взаимодействия подразделений и служб организаций в процессе проведения исследований и разработок с использованием информации ограниченного доступа; методов и средств контроля за состоянием технической защиты информации; отечественного и зарубежного опыта в области технической защиты информации; методов и средств получения, обработки и передачи информации; методов и процедур выявления угроз безопасности информации на объектах информатизации организации; средств защиты информации от различных видов угроз безопасности информации; средств контроля эффективности технической защиты информации по различным физическим полям; порядка оформления технической документации по защите информации; классификации факторов, воздействующих на защищаемую информацию, физические основы образования технических каналов утечки информации и их свойства; системы защиты информации в автоматизированной системе в защищенном исполнении, классы защищенности автоматизированных систем; методов и порядка организации и проведения специальных исследований , специальных проверок, экспертиз, тестовых испытаний и контрольных проверок, процедур сертификации, аттестации и лицензирования; типовые проектные решения по применению средств и систем технической защиты информации.
III. Требования к профессиональным навыкам		Навыки: работы с нормативными правовыми актами в области технической защиты информации ограниченного доступа; работы с правовыми базами данных, базами данных, содержащих информацию ограниченного доступа, угрозам безопасности информации в органах государственной власти, организации; разработка необходимых документов в интересах организации работ по технической защите информации ограниченного доступа в масштабах организации; проведения работ, связанных с защитой информации и контролем ее эффективности;

	планирования и организации работ проведения работ в области технической защиты информации на уровне объекта информатизации; проектирования, построения и эксплуатации комплексной системы защиты информации; проведения аттестации объектов информатизации на предмет соответствия требованиям технической защиты информации по соответствующим классам безопасности; оценки возможностей технических разведок, выявления угроз безопасности, технических каналов утечки информации, выявления нарушений в использовании основных и вспомогательных технических систем и средств при обработке информации ограниченного доступа; использования и обслуживания технических средств контроля, составления планирующих, отчетных документов и рекомендаций по результатам оценки, подготовки проектов договоров; планирования, организации и контроля выполнения мероприятий по проектированию и эксплуатации защищенных объектов информатизации; разработки методик анализа проектной и эксплуатационной документации, методик оценки эффективности мероприятий по технической защите информации ограниченного доступа на уровне отрасли, организации; проведения специальных экспертиз и (или) аттестации объектов информатизации; подготовка заключений и итоговой отчетной документации.

Направление профессиональной служебной деятельности:
Управление в сфере информации и информационных технологий

Специализация по направлению профессиональной служебной деятельности:
Осуществление технической защита информации от утечки по техническим каналам

Наименование федерального государственного органа
Федеральная служба по техническому и экспортному контролю

Категория «специалисты» старшей группы должностей государственной гражданской службы		
I. Требования к направлению подготовки (специальности) профессионального образования		**К специалистам:** направления подготовки (специальности) «Безопасность информационных технологий в правоохранительной сфере», «Информационная безопасность автоматизированных систем», «Информационная безопасность телекоммуникационных систем». **К бакалаврам:** Направление подготовки «Информационная безопасность». Иное направление подготовки (специальность), для которого законодательством об образовании Российской Федерации установлено соответствие направлению подготовки (специальности), указанному в предыдущих перечнях профессий, специальностей и направлений подготовки.
II. Требования к профессиональным знаниям	1. Профессиональные знания в области законодательства Российской Федерации	Знание основных законодательных и правовых актов в области технической защиты информации и перспективы их дальнейшей разработки (0.1, 0.2, 0.3, 0.5, 0.6, 0.7, 0.9). Знание государственной системы противодействия иностранным техническим разведкам и технической защиты информации. Знание нормативных правовых актов и организационных основ защиты информации в Российской Федерации. Знание функций и задач ФСТЭК России и управлений ФСТЭК России по федеральным округам по технической защите информации.
	2. Иные профессиональные знания	Знание: технических каналов утечки информации ограниченного доступа, возникающих при ее обработке, физических явлений, лежащих в основе появления различных каналов утечки информации, в части касающейся побочных электромагнитных излучений и наводок, акустических и виброакустических каналов; каналов утечки информации при эксплуатации электронных вычислительных машин, автоматизированных систем управления, волоконно-оптических систем передачи информации и беспроводных устройств передачи данных; характеристик различных типов информационных сигналов, содержащих информацию

		ограниченного доступа (акустических, виброакустических, электрических, электромагнитных); системы организации комплексной защиты информации, действующей в органе государственной власти, организации; перспективных направлений развития технических методов и средств защиты информации ограниченного доступа, программно-аппаратных средств защиты информации от утечки по техническим каналам, методов и средств защиты информации (носителей информации) от специальных воздействий; основ методологии и методики проведения технической защиты информации в органе государственной власти, организации; характера взаимодействия подразделений и служб организаций в процессе проведения исследований и разработок с использованием информации ограниченного доступа; методов и средств контроля за состоянием технической защиты информации; отечественного и зарубежного опыта в области технической защиты информации; методов и средств получения, обработки и передачи информации; методов и процедур выявления угроз безопасности информации на объектах информатизации организации; средств защиты информации от различных видов угроз безопасности информации; средств контроля эффективности технической защиты информации по различным физическим полям; порядка оформления технической документации по защите информации; классификации факторов, воздействующих на защищаемую информацию, физические основы образования технических каналов утечки информации и их свойства; системы защиты информации в автоматизированной системе в защищенном исполнении, классы защищенности автоматизированных систем; методов и порядка организации и проведения специальных исследований , специальных проверок, экспертиз, тестовых испытаний и контрольных проверок, процедур сертификации, аттестации и лицензирования; типовые проектные решения по применению средств и систем технической защиты информации.
III. Требования к профессиональным навыкам		Навыки: работы с нормативными правовыми актами в области технической защиты информации ограниченного доступа; работы с правовыми базами данных, базами данных, содержащих информацию ограниченного доступа, угрозам безопасности информации в органах государственной власти, организации; разработка необходимых документов в интересах организации работ по технической защите информации ограниченного доступа в масштабах организации; проведения работ, связанных с защитой информации и контролем ее эффективности;

	планирования и организации работ проведения работ в области технической защиты информации на уровне объекта информатизации; проектирования, построения и эксплуатации комплексной системы защиты информации; проведения аттестации объектов информатизации на предмет соответствия требованиям технической защиты информации по соответствующим классам безопасности; оценки возможностей технических разведок, выявления угроз безопасности, технических каналов утечки информации, выявления нарушений в использовании основных и вспомогательных технических систем и средств при обработке информации ограниченного доступа; использования и обслуживания технических средств контроля, составления планирующих, отчетных документов и рекомендаций по результатам оценки, подготовки проектов договоров; планирования, организации и контроля выполнения мероприятий по проектированию и эксплуатации защищенных объектов информатизации; разработки методик анализа проектной и эксплуатационной документации, методик оценки эффективности мероприятий по технической защите информации ограниченного доступа на уровне отрасли, организации; проведения специальных экспертиз и (или) аттестации объектов информатизации; подготовка заключений и итоговой отчетной документации.

Направление профессиональной служебной деятельности:
Управление в сфере информации и информационных технологий
Специализация по направлению профессиональной служебной деятельности:
Сертификация средств защиты информации и аттестация объектов информатизации
Наименование федерального государственного органа:
Федеральная служба по техническому и экспортному контролю

Категория «специалисты» главной и ведущей групп должностей государственной гражданской службы		
I. Требования к направлению подготовки (специальности) профессионального образования		**К магистрам:** направление подготовки «Информационная безопасность». **К специалистам:** направления подготовки (специальности) «Безопасность информационных технологий в правоохранительной сфере», «Информационная безопасность автоматизированных систем», «Информационная безопасность телекоммуникационных систем». Иное направление подготовки (специальность), для которого законодательством об образовании Российской Федерации установлено соответствие направлению подготовки (специальности), указанному в предыдущих перечнях профессий, специальностей и направлений подготовки.
II. Требования к профессиональным знаниям	1. Профессиональные знания в области законодательства Российской Федерации	Знать государственную систему противодействия иностранным техническим разведкам и технической защиты информации (0.1, 0.2, 0.3, 0.4, 0.5, 0.6, 0.7, 0.8, 0.9, 0.10, 0.11, 0.12). Знать основные нормативные правовые акты в области технической защиты информации ограниченного доступа и сертификации средств защиты информации по требованиям безопасности информации. Знать функции и задачи ФСТЭК России и управлений ФСТЭК России по федеральным округам по технической защите информации. Знание требований национальных стандартов, нормативных правовых актов и методических документов в области сертификации средств защиты информации и аттестации объектов информатизации.
	2. Иные профессиональные знания	Знание каналов утечки информации ограниченного доступа, возникающих при ее обработке; методических основ и методики оценки опасности угроз утечки информации ограниченного доступа по различным каналам; целей, задач, основных принципов организации, методов и средств ведения контроля состояния защищенности информации ограниченного доступа в органах государственной власти, организациях; основ методологии и методики проведения аттестации объектов информатизации в органах

		государственной власти, организациях; методов и средств контроля за состоянием объектов информатизации; отечественного и зарубежного опыта в области сертификации средств защиты информации; перечня сертифицированных средств защиты информации, их характеристик по основному назначению; средств контроля эффективности средств защиты информации; порядка оформления технической документации по аттестации объектов информатизации; построение и функции системы защиты информации в автоматизированной системе в защищенном исполнении, классы защищенности автоматизированных систем; методов и порядка организации и проведения специальных исследований, экспертиз, тестовых испытаний и контрольных проверок, процедур сертификации, аттестации, оформления и выдачи аттестатов соответствия; методов и порядка обработки результатов контроля, анализа и оценки защищенности объектов информатизации с проведением расчетов, порядка подготовки актов по результатам специальных исследований, протоколов измерений, предписаний на право эксплуатации объектов, систем и средств в защищенном исполнении и других документов по результатам контроля (оценки).
III. Требования к профессиональным навыкам		Навыки: работы с нормативными правовыми актами в области технической защиты информации ограниченного доступа; работы с правовыми базами данных, базами данных, содержащих информацию ограниченного доступа, угрозам безопасности информации в органах государственной власти, организации; разработка необходимых документов в интересах организации работ по сертификации средств защиты информации и аттестации объектов информатизации; проведения работ, связанных с защитой информации и контролем ее эффективности; проведения аттестации объектов информатизации, программ, алгоритмов на предмет соответствия требованиям технической защиты информации по соответствующим классам безопасности; работы с нормативными документами и методическими материалами по сертификации средств защиты информации и аттестации объектов информатизации; проведения экспертизы материалов сертификационных испытаний средств защиты информации; проведения специальных экспертиз по вопросам оценки возможности аккредитации организаций в качестве органов по сертификации средств защиты информации и испытательных лабораторий; умения разрабатывать документы по результатам сертификационных испытаний средств защиты информации и работ по аттестации объектов информатизации.

Направление профессиональной служебной деятельности:
Управление в сфере информации и информационных технологий
Специализация по направлению профессиональной служебной деятельности:
Сертификация средств защиты информации и аттестация объектов информатизации
Наименование федерального государственного органа:
Федеральная служба по техническому и экспортному контролю

<table>
<tr><th colspan="3">Категория «специалисты» старшей группы должностей государственной гражданской службы</th></tr>
<tr><td colspan="2">I. Требования к направлению подготовки (специальности) профессионального образования</td><td>К специалистам:
направления подготовки (специальности) «Безопасность информационных технологий в правоохранительной сфере», «Информационная безопасность автоматизированных систем», «Информационная безопасность телекоммуникационных систем».
К бакалаврам:
Направление подготовки «Информационная безопасность».
Иное направление подготовки (специальность), для которого законодательством об образовании Российской Федерации установлено соответствие направлению подготовки (специальности), указанному в предыдущих перечнях профессий, специальностей и направлений подготовки.</td></tr>
<tr><td rowspan="2">II. Требования к профессиональным знаниям</td><td>1. Профессиональные знания в области законодательства Российской Федерации</td><td>Знать государственную систему противодействия иностранным техническим разведкам и технической защиты информации (0.1, 0.2, 0.3, 0.4, 0.5, 0.6, 0.7, 0.8, 0.9, 0.10, 0.11, 0.12).
Знать основные нормативные правовые акты в области технической защиты информации ограниченного доступа и сертификации средств защиты информации по требованиям безопасности информации.
Знать функции и задачи ФСТЭК России и управлений ФСТЭК России по федеральным округам по технической защите информации.
Знание требований национальных стандартов, нормативных правовых актов и методических документов в области сертификации средств защиты информации и аттестации объектов информатизации.</td></tr>
<tr><td>2. Иные профессиональные знания</td><td>Знание каналов утечки информации ограниченного доступа, возникающих при ее обработке;
методических основ и методики оценки опасности угроз утечки информации ограниченного доступа по различным каналам;
целей, задач, основных принципов организации, методов и средств ведения контроля состояния защищенности информации ограниченного доступа в органах государственной власти, организациях;
основ методологии и методики проведения аттестации объектов информатизации в органах</td></tr>
</table>

		государственной власти, организациях; методов и средств контроля за состоянием объектов информатизации; отечественного и зарубежного опыта в области сертификации средств защиты информации; перечня сертифицированных средств защиты информации, их характеристик по основному назначению; средств контроля эффективности средств защиты информации; порядка оформления технической документации по аттестации объектов информатизации; построение и функции системы защиты информации в автоматизированной системе в защищенном исполнении, классы защищенности автоматизированных систем; методов и порядка организации и проведения специальных исследований, экспертиз, тестовых испытаний и контрольных проверок, процедур сертификации, аттестации, оформления и выдачи аттестатов соответствия; методов и порядка обработки результатов контроля, анализа и оценки защищенности объектов информатизации с проведением расчетов, порядка подготовки актов по результатам специальных исследований, протоколов измерений, предписаний на право эксплуатации объектов, систем и средств в защищенном исполнении и других документов по результатам контроля (оценки).
III. Требования к профессиональным навыкам		Навыки: работы с нормативными правовыми актами в области технической защиты информации ограниченного доступа; работы с правовыми базами данных, базами данных, содержащих информацию ограниченного доступа, угрозам безопасности информации в органах государственной власти, организации; разработка необходимых документов в интересах организации работ по сертификации средств защиты информации и аттестации объектов информатизации; проведения работ, связанных с защитой информации и контролем ее эффективности; проведения аттестации объектов информатизации, программ, алгоритмов на предмет соответствия требованиям технической защиты информации по соответствующим классам безопасности; работы с нормативными документами и методическими материалами по сертификации средств защиты информации и аттестации объектов информатизации; проведения экспертизы материалов сертификационных испытаний средств защиты информации; проведения специальных экспертиз по вопросам оценки возможности аккредитации организаций в качестве органов по сертификации средств защиты информации и испытательных лабораторий; умения разрабатывать документы по результатам сертификационных испытаний средств защиты информации и работ по аттестации объектов информатизации.

Перечень
ключевых нормативных правовых актов, знание которых необходимо для исполнения должностных обязанностей по специализации профессиональной служебной деятельности «Осуществление технической защиты информации от утечки по техническим каналам, несанкционированного доступа и обеспечение безопасности информации в ключевых системах информационной инфраструктуры» по направлению профессиональной служебной деятельности «Управление в сфере информации и информационных технологий»

№ п/п	Наименование и реквизиты документа
0.1	Закон Российской Федерации от 21 июля 1993 г. № 5485-1 «О государственной тайне»
0.2	Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»
0.3	Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании»
0.4	Федеральный Закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»
0.5	Указ Президента Российской Федерации от 30 ноября 1995 г. № 1203 «Об утверждении перечня сведений, отнесенных к государственной тайне»
0.6	Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»
0.7	Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю»
0.9	Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»
0.10	Постановление Правительства Российской Федерации от 18 мая 2009 г. № 424 «Об особенностях подключения федеральных государственных информационных систем к информационно-телекоммуникационным сетям»
0.11	Постановление Правительства Российской Федерации от 26 июня 1995 г. № 608 «О сертификации средств защиты информации»
0.12	Постановление Правительства Российской Федерации от 15 мая 2010 г. № 330 «Об особенностях оценки соответствия продукции (работ, услуг), используемой в целях защиты сведений, относимых к охраняемой в соответствии с законодательством Российской Федерации информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, а также процессов ее проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации, утилизации и захоронения, об особенностях аккредитации органов по сертификации и испытательных лабораторий (центров), выполняющих работы по подтверждению соответствия указанной продукции (работ, услуг)»