Приказ Минздравсоцразвития России от 22.04.2009 № 205 "Об утверждении Единого квалификационного справочника должностей руководителей, специалистов и служащих, раздел "Квалификационные характеристики должностей руководителей и специалистов по обеспечению безопасности информации в ключевых системах информационной инфраструктуры, противодействию техническим разведкам и технической защите информации"

В соответствии с пунктом 5.2.52 Положения о Министерстве здравоохранения и социального развития Российской Федерации, утвержденного Постановлением Правительства Российской Федерации от 30 июня 2004 г. № 321 (Собрание законодательства Российской Федерации, 2004, № 28, ст. 2898; 2005, № 2, ст. 162; 2006, № 19, ст. 2080; 2008, № 11 (ч. I), ст. 1036; № 15, ст. 1555; № 23, ст. 2713; № 42, ст. 4825; № 46, ст. 5337; № 48, ст. 5618; 2009, № 2, ст. 244; № 3, ст. 378; № 6, ст. 738; № 12, ст. 1427), приказываю:

Утвердить Единый квалификационный справочник должностей руководителей, специалистов и служащих, раздел «Квалификационные характеристики должностей руководителей и специалистов по обеспечению безопасности информации в ключевых системах информационной инфраструктуры, противодействию техническим разведкам и технической защите информации» согласно приложению.

Министр
Т.Голикова

Единый квалификационный справочник должностей руководителей, специалистов и служащих

Раздел "Квалификационные характеристики должностей руководителей и специалистов по обеспечению безопасности информации в ключевых системах информационной инфраструктуры, противодействию техническим разведкам и технической защите информации"

Приложение
к Приказу
Министерства здравоохранения
и социального развития
Российской Федерации
от 22 апреля 2009 г. № 205

I. Общие положения

1. Раздел «Квалификационные характеристики должностей руководителей и специалистов по обеспечению безопасности информации в ключевых системах информационной инфраструктуры, противодействию техническим разведкам и технической защите информации» Единого квалификационного справочника разработан в соответствии с Законом Российской Федерации от 21 июля 1993 г. № 5485-1 "О государственной тайне" (Собрание законодательства Российской Федерации, 1997, № 41, ст. 4673), Законом Российской Федерации от 5 марта 1992 г. № 2446-1 «О безопасности» (Ведомости Съезда народных депутатов Российской Федерации и Верховного Совета Российской Федерации, 1992, № 15, ст. 769), Федеральным законом от 27 июля 2006 г. № 149-ФЗ "Об информации, информационных технологиях и о защите информации" (Собрание законодательства Российской Федерации, 2006, № 31 (ч. I), ст. 3448), Федеральным законом от 27 декабря 2002 г. № 184-ФЗ "О техническом регулировании" (Собрание законодательства Российской Федерации, 2002, № 52 (ч. I), ст. 5140), Федеральным законом от 8 августа 2001 г. № 128-ФЗ «О лицензировании отдельных видов деятельности» (Собрание законодательства Российской Федерации, 2001, № 33 (ч. I), ст. 3430), Указом Президента Российской Федерации от 16 августа 2004 г. № 1085 "Вопросы Федеральной службы по техническому и экспортному контролю" (Собрание законодательства Российской Федерации, 2004, № 34, ст. 3541) и иными нормативными правовыми актами Российской Федерации и состоит из трех разделов: I - «Общие положения»; II - «Должности руководителей»; III - «Должности специалистов».

2. Квалификационные характеристики должностей руководителей и специалистов по обеспечению безопасности информации в ключевых системах информационной инфраструктуры, противодействию технической разведке и технической защите информации (далее - квалификационные характеристики) предназначены для решения вопросов, связанных с регулированием трудовых отношений, управления персоналом организаций в сфере компетенции Федеральной службы по техническому и экспортному контролю (ФСТЭК России) независимо от форм собственности и организационно-правовых форм.

Квалификационные характеристики призваны способствовать правильному подбору и расстановке кадров, повышению их деловой квалификации, рациональному разделению труда, созданию действенного механизма разграничения функций, полномочий и ответственности между указанными категориями работников, а также установлению единых подходов в определении их должностных обязанностей и предъявляемых к ним квалификационных требований.

3. Квалификационные характеристики могут применяться в качестве нормативных документов или служить основой для разработки должностных инструкций, содержащих конкретный перечень должностных обязанностей работников с учетом особенностей организации производства, труда и управления, а также их прав и ответственности. При необходимости должностные обязанности, включенные в квалификационную характеристику определенной должности, могут быть распределены между несколькими исполнителями.

При разработке должностных инструкций допускается уточнение перечня работ, которые свойственны соответствующей должности в конкретных организационно-технических условиях, и установление требований к необходимой специальной подготовке работников.

4. Квалификационная характеристика каждой должности имеет три раздела: «Должностные обязанности», «Должен знать», «Требования к квалификации».

В разделе «Должностные обязанности» установлены основные трудовые функции, которые могут быть поручены полностью или частично работнику, занимающему данную должность, с учетом технологической однородности и взаимосвязанности работ, позволяющих обеспечить оптимальную специализацию служащих.

В разделе «Должен знать» содержатся основные требования, предъявляемые к работнику в отношении специальных знаний, а также знаний законодательных и иных нормативных правовых актов, положений, инструкций и других документов, методов и средств, которые работник должен применять при выполнении должностных обязанностей.

В разделе «Требования к квалификации» определены уровень профессиональной подготовки работника, необходимый для выполнения должностных обязанностей, требования к прохождению повышения квалификации и квалификационной аттестации, а также требования к стажу работы. Уровни требуемой профессиональной подготовки, указанные в разделе «Требования к квалификации», приведены в соответствии с Законом Российской Федерации «Об образовании» от 10 июня 1992 г. № 3266-1 (Собрание законодательства Российской Федерации, 1996, № 3, ст. 150).

Квалификационные характеристики предусматривают сертификацию соответствия руководителей и специалистов по видам их деятельности требованиям законодательных и иных нормативных правовых актов.

5. В квалификационных характеристиках должностей специалистов предусматривается в пределах одной и той же должности без изменения ее наименования внутридолжностное квалификационное категорирование по оплате труда.

6. Применение должностного наименования «старший» возможно при условии, если работник наряду с выполнением обязанностей, предусмотренных по занимаемой должности, осуществляет руководство подчиненными ему исполнителями. Должность «старшего» может устанавливаться в виде исключения и при отсутствии исполнителей в непосредственном подчинении работника, если на него возлагаются функции руководства самостоятельным участком работы. Для должностей специалистов, по которым предусматриваются квалификационные категории, должностное наименование «старший» не применяется. В этих случаях функции руководства подчиненными исполнителями возлагаются на специалиста I квалификационной категории.

Должностные обязанности «ведущих» устанавливаются на основе квалификационных характеристик соответствующих должностей специалистов. Кроме того, на них возлагаются функции руководителя и ответственного исполнителя работ по одному из направлений деятельности организации или ее структурных подразделений либо обязанности по координации и методическому руководству группами исполнителей, создаваемыми в отделах (бюро), с учетом рационального разделения труда в конкретных организационно-технических условиях. Требования к стажу работы повышаются на 1 - 2 года по сравнению со стажем, предусмотренным для специалистов I квалификационной категории.

Должностные обязанности, требования к знаниям и квалификации заместителей руководителей структурных подразделений определяются на основе характеристик соответствующих должностей руководителей.

II. Должности руководителей

Главный специалист по технической защите информации

Должностные обязанности. Руководит выполнением работ по технической защите информации в организациях. Организует проведение категорирования объектов информатизации, выявление угроз безопасности информации и технических каналов утечки информации, работы по специальным проверкам, специальным исследованиям, аттестации объектов информатизации, лицензированию деятельности организаций, применению сертифицированных средств технической защиты информации. Организует разработку организационно-распорядительных документов в области технической защиты информации. Участвует в рассмотрении технических заданий на научно-исследовательские и опытно-конструкторские работы по разработке изделий, подлежащих защите от технических разведок. Разрабатывает предложения для включения в планы и программы работ по технической защите информации. Участвует в работах по внедрению новых средств технической защиты информации. Содействует распространению в организации передового опыта и внедрению современных организационно-технических мер,

средств и способов технической защиты информации. Организует мероприятия по предотвращению утечки информации ограниченного доступа должностными лицами организаций, выполняющих работы, связанные со сведениями, составляющими государственную тайну и (или) содержащими иную информацию ограниченного доступа, при использовании открытых каналов радиосвязи. Осуществляет контроль выполнения требований нормативных правовых актов и иных документов по технической защите информации. Организует работы по определению потребности в средствах технической защиты информации, их заказу, получению и распределению. Участвует в подборе и расстановке специалистов. Организует работу по аттестации, обучению, профессиональной переподготовке и повышению квалификации специалистов в области технической защиты информации.

Должен знать: законы и иные нормативные правовые акты Российской Федерации, регулирующие отношения, связанные с защитой государственной тайны и иной информации ограниченного доступа; нормативные и методические документы по вопросам, связанным с обеспечением технической защиты информации, планированием мероприятий и контролем выполнения работ по технической защите информации; методы и средства контроля эффективности технической защиты информации; организационную структуру объектов защиты; организацию деятельности объектов защиты и функционирования на них систем управления, связи и автоматизации; правила организации аттестации, лицензирования и сертификации в области технической защиты информации; мероприятия по технической защите и контролю информации, в том числе при использовании открытых каналов радиосвязи; способы выявления угроз безопасности информации и методы технической защиты информации от них; порядок заключения договоров на проведение специальных исследований и специальных проверок; технические возможности специальной техники подразделений по защите информации, основы ее эксплуатации, организации обслуживания и ремонта; методики оценки возможностей технических разведок; порядок проведения категорирования объектов; требования по оформлению актов проверки, протоколов испытаний, предписаний на право эксплуатации основных и вспомогательных технических средств и систем; методы оценки профессионального уровня специалистов по технической защите информации, аттестации специалистов; основы экономики, организации производства и управления персоналом; основы трудового законодательства; правила по охране труда и пожарной безопасности.

Требования к квалификации. Высшее профессиональное образование по специальности «Информационная безопасность» и стаж работы по технической защите информации не менее 5 лет, в том числе на руководящих должностях не менее 3 лет.

Начальник отдела (лаборатории, сектора) по противодействию техническим разведкам

Должностные обязанности. Выполняет работы по противодействию техническим разведкам в организациях оборонно-промышленного комплекса. Руководит работами по выявлению каналов утечки информации и проведению мероприятий по использованию существующих методов и средств противодействия техническим разведкам, разработкой предложений по совершенствованию методов противодействия и оценки их эффективности. Определяет цели и задачи работ, осуществляет проверку выполнения требований нормативных документов по противодействию техническим разведкам. Возглавляет разработку проектов перспективных и текущих планов работ, составление отчетов по их выполнению. Принимает участие в разработке технических заданий и проведении научных исследований, выполняемых в организации, готовит отзывы и заключения на проекты вновь строящихся зданий и сооружений, а также обеспечивает взаимодействие соисполнителей по научно-исследовательским и опытно-конструкторским работам в части обеспечения мер противодействия техническим разведкам. Участвует в организации и осуществлении мероприятий по предотвращению утечки информации ограниченного доступа должностными лицами организаций, выполняющих работы, связанные со сведениями, составляющими государственную тайну и (или) содержащими иную информацию ограниченного доступа. Руководит работами по составлению актов, протоколов испытаний, предписаний на право эксплуатации и другой документации по обеспечению мероприятий противодействия техническим разведкам, участвует в разработке (доработке, модернизации) средств и систем, оценке технико-экономического уровня и эффективности предлагаемых и реализуемых решений в области противодействия техническим разведкам. Определяет нарушения в применении способов и средств по противодействию техническим разведкам, разрабатывает меры по их устранению и предотвращению. Участвует в экспертизе материалов, предназначенных для открытого опубликования. Оценивает потребность и организует обеспечение (снабжение) отдела (лаборатории, сектора) техникой и оборудованием, а также материальными, финансовыми и другими ресурсами, обеспечивая их рациональное расходование. Организует учет, использование по назначению, техническое обслуживание, ремонт, хранение и списание техники отдела (лаборатории, сектора) и другого оборудования. Участвует в подборе, расстановке и аттестации специалистов. Руководит работниками отдела (лаборатории, сектора), принимает меры по их профессиональной переподготовке и повышению квалификации.

Должен знать: законы и иные нормативные правовые акты Российской Федерации, регулирующие отношения, связанные с защитой государственной тайны и иной информации ограниченного доступа; нормативные и методические документы по вопросам, связанным с обеспечением противодействия техническим разведкам; перспективы развития, специализацию, направления деятельности организации и ее подразделений; документы, определяющие основные направления экономического и социального развития организации; действующие системы сертификации, лицензирования, каналы утечки информации, способы их выявления, методы и средства контроля охраняемых сведений; показатели оценки эффективности мер по противодействию техническим разведкам, методы их расчета и анализа, отыскания оптимальных решений по повышению эффективности противодействия техническим разведкам; достижения науки и техники в стране и за рубежом в области технических разведок и противодействия им; порядок заключения договоров на проведение специальных исследований, работ по защите основных и вспомогательных технических средств и систем; организацию взаимодействия подразделений при решении вопросов обеспечения по противодействию техническим разведкам и комплексного контроля; порядок финансирования, методы планирования и организации работ по противодействию техническим разведкам; порядок составления организационно-распорядительных документов, перспективных планов и программ проведения научных исследований, разработок, испытаний, внедрения новых технических средств по противодействию техническим разведкам; структуру, назначение, задачи, полномочия и техническую оснащенность отдела (лаборатории, сектора); основы эксплуатации специальной техники, организации ее обслуживания и ремонта; основы организации производства, труда и управления персоналом отдела (лаборатории, сектора); основы трудового

законодательства; правила по охране труда и пожарной безопасности.

Требования к квалификации. Высшее профессиональное образование по специальности «Информационная безопасность» и стаж работы по противодействию техническим разведкам не менее 5 лет, в том числе на руководящих должностях не менее 2 лет.

Начальник отдела (лаборатории, сектора) по технической защите информации

Должностные обязанности. Выполняет работы по технической защите информации в организациях. Руководит работами по выявлению угроз безопасности информации, определению возможностей технической разведки и проведению мероприятий технической защиты информации. Участвует в категорировании объектов информатизации, выявлении угроз безопасности информации и технических каналов утечки информации, работах по проведению специальных проверок и специальных исследований объектов информатизации. Формулирует цели и задачи работ по созданию безопасных информационных технологий, отвечающих требованиям технической защиты информации, определяет перспективы их развития для конкретных объектов защиты. Возглавляет разработку проектов перспективных и текущих планов работ, составление отчетов по их выполнению. Принимает участие в разработке технических заданий и проведении научных исследований, выполняемых в организации, а также обеспечивает взаимодействие соисполнителей по научно-исследовательским и опытно-конструкторским работам в части обеспечения технической защиты информации. Участвует в организации и осуществлении мероприятий по предотвращению утечки информации ограниченного доступа должностными лицами организаций, выполняющих работы, связанные со сведениями, составляющими государственную тайну и (или) содержащими иную информацию ограниченного доступа, при использовании открытых каналов радиосвязи. Руководит работами по составлению актов, протоколов испытаний, предписаний на право эксплуатации и другой документации по технической защите информации и обеспечению безопасности информации на объектах информатизации, доработке (модернизации) средств и систем технической защиты информации, их внедрению, информированию заинтересованных организаций о сущности и эффективности доработок, принимает меры по обеспечению финансирования этих работ, в том числе выполняемых по договорам. Определяет направления работы отдела (лаборатории, сектора) по разработке безопасных информационных технологий, согласовывает проектную и другую техническую документацию на вновь создаваемые и модернизируемые объекты в части выполнения требований по технической защите информации, обеспечивает высокий научно-технический уровень работ, эффективность и качество исследований и разработок. Оценивает потребность и организует обеспечение (снабжение) отдела (лаборатории, сектора) техникой и оборудованием, а также материальными, финансовыми и другими ресурсами, обеспечивая их рациональное расходование. Организует учет, использование по назначению, техническое обслуживание, ремонт, хранение и списание техники отдела и другого оборудования. Участвует в подборе, расстановке и аттестации специалистов. Руководит работниками отдела (лаборатории, сектора), принимает меры по их профессиональной переподготовке и повышению квалификации.

Должен знать: законы и иные нормативные правовые акты Российской Федерации, регулирующие отношения, связанные с защитой государственной тайны и иной информации ограниченного доступа; нормативные и методические документы по вопросам, связанным с обеспечением защиты информации; категорию объекта информатизации, перспективы развития, специализацию и направления деятельности организации и ее подразделений; документы, определяющие основные направления экономического и социального развития организации; системы сертификации, лицензирования и организацию технической защиты информации, действующую в организации; виды угроз безопасности информации, методы и средства контроля охраняемых сведений, способы выявления технических каналов утечки информации; показатели оценки эффективности мер по обеспечению безопасности информации, методы их расчета и анализа, отыскания оптимальных решений по повышению эффективности технической защиты информации; порядок заключения договоров на проведение специальных исследований и специальных проверок, работ по защите основных и вспомогательных технических средств и систем; организацию взаимодействия подразделений организации при решении вопросов обеспечения безопасности информации и комплексного контроля; порядок финансирования, методы планирования и организации выполнения работ по защите информации; порядок составления организационно-распорядительных документов, перспективных планов и программ проведения научных исследований, разработок, испытаний, внедрения новых технических и программно-аппаратных средств защиты информации; структуру, назначение, задачи, полномочия и техническую оснащенность отдела (лаборатории, сектора); основы эксплуатации специальной техники, организации ее обслуживания и ремонта; основы организации производства, труда и управления персоналом отдела (лаборатории, сектора); основы трудового законодательства; правила по охране труда и пожарной безопасности.

Требования к квалификации. Высшее профессиональное образование по специальности «Информационная безопасность» и стаж работы по технической защите информации не менее 5 лет, в том числе на руководящих должностях не менее 2 лет.

III. Должности специалистов

Специалист по обеспечению безопасности информации в ключевых системах информационной инфраструктуры

Должностные обязанности. Выполняет мероприятия по обеспечению безопасности информации в ключевых системах информационной инфраструктуры. Определяет возможные угрозы безопасности информации, уязвимость программного и аппаратного обеспечения, разрабатывает технологии обнаружения вторжения, оценивает и переоценивает риски, связанные с угрозами деструктивных информационных воздействий, способных нанести ущерб системам и сетям вследствие

несанкционированного доступа, использования раскрытия, модификации или уничтожения информации и ресурсов информационно-управляющих систем. Определяет ограничения по вводу информации, процедуры управления инцидентами нарушения безопасности и предотвращает их развитие, порядок подключения к открытым информационным системам с учетом обеспечения безопасности, связанной с соглашениями о доступе и приоритезации ресурсов, требования к местам резервного хранения, обработки и копирования информации, приоритеты обслуживания по использованию основных и резервных телекоммуникационных сервисов (услуг). Разрабатывает процедуры защиты носителей информации, коммуникаций и восстановления информационно-управляющих систем после сбоя или отказа. Осуществляет контроль деятельности по обеспечению безопасности информации в ключевых системах информационной инфраструктуры; информационное, материально-техническое и научно-техническое обеспечение безопасности информации; контроль состояния работ по обеспечению безопасности информации в ключевых системах информационной инфраструктуры и их соответствие нормативным правовым актам Российской Федерации. Дает отзывы и заключения на проекты вновь создаваемых и модернизируемых объектов и других разработок по вопросам обеспечения безопасности информации в ключевых системах информационной инфраструктуры. Участвует в рассмотрении технических заданий на научно-исследовательские и опытно-конструкторские работы по обеспечению безопасности информации в ключевых системах информационной инфраструктуры, оценивает их соответствие действующим нормативным и методическим документам. Участвует в работах по внедрению новых средств технической защиты информации. Содействует распространению в организации передового опыта и внедрению современных организационно-технических мер, средств и способов обеспечения безопасности информации в ключевых системах информационной инфраструктуры. Проводит оценки технико-экономического уровня и эффективности предлагаемых и реализуемых организационно-технических решений по обеспечению безопасности информации в ключевых системах информационной инфраструктуры. Разрабатывает списки доступа персонала на объекты защиты, порядок и правила поведения работников, в том числе при их перемещении, увольнении и взаимодействии с персоналом сторонних организаций. Осуществляет руководство и обучение персонала действиям в кризисных ситуациях, включая порядок действий руководящих и других ответственных лиц ключевых систем информационной инфраструктуры.

Должен знать: законы и иные нормативные правовые акты Российской Федерации, регулирующие отношения, связанные с защитой государственной тайны и иной информации ограниченного доступа; нормативные и методические документы по вопросам, связанным с обеспечением безопасности информации; структуру управления, связи и автоматизации и основные элементы ключевой системы информационной инфраструктуры организации; подсистемы разграничения доступа, подсистемы обнаружения атак, подсистемы защиты от преднамеренных воздействий, контроля целостности информации; порядок создания защищенного канала между взаимодействующими объектами через систему общего пользования с использованием выделенных каналов связи; порядок осуществления аутентификации взаимодействующих объектов и проверки подлинности отправителя и целостности, передаваемых через систему общего пользования данных; оснащенность организации основными и вспомогательными техническими средствами и системами, перспективы их развития и модернизации; перспективы и направления развития методов и средств технических и программно-аппаратных средств защиты информации от деструктивных информационных воздействий; порядок проектирования и аттестации объектов информатизации; контроль эффективности защиты информации на объектах информатизации; порядок осуществления контроля использования открытых каналов радиосвязи; методы и средства выявления угроз безопасности информации, методики выявления каналов утечки информации; методы проведения научных исследований, разработок по технической защите информации; порядок обследования ключевых систем информационной инфраструктуры, составления актов проверки, протоколов испытаний, предписаний на право эксплуатации специальных средств обеспечения безопасности информации, а также положений, инструкций и других организационно-распорядительных документов; полномочия по вопросам обеспечения безопасности информации, возможности и порядок применения штатных технических средств обеспечения безопасности информации и контроля их эффективности; методы анализа результатов проверок, учета нарушений требований по обеспечению безопасности информации; методику подготовки предложений, методы и средства выполнения вычислительных работ в интересах планирования, организации и проведения работ по обеспечению безопасности информации и обеспечению государственной тайны; достижения науки и техники в стране и за рубежом в области технической разведки и защиты информации; методы оценки профессионального уровня специалистов по обеспечению безопасности информации, аттестации специалистов; основы трудового законодательства; правила по охране труда и пожарной безопасности.

Требования к квалификации.

Специалист по обеспечению безопасности информации в ключевых системах информационной инфраструктуры I категории: высшее профессиональное образование по специальности «Информационная безопасность» и стаж работы в должности специалиста по обеспечению безопасности информации в ключевых системах информационной инфраструктуры II категории не менее 3 лет.

Специалист по обеспечению безопасности информации в ключевых системах информационной инфраструктуры II категории: высшее профессиональное образование по специальности «Информационная безопасность» и стаж работы в должности специалиста по обеспечению безопасности информации в ключевых системах информационной инфраструктуры или на других должностях, замещаемых специалистами с высшим профессиональным образованием, не менее 3 лет.

Специалист по обеспечению безопасности информации в ключевых системах информационной инфраструктуры: высшее профессиональное образование по специальности «Информационная безопасность» без предъявления требований к стажу работы.

Специалист по противодействию техническим разведкам

Должностные обязанности. Проводит сбор и анализ информации, необходимой для оценки возможностей средств, систем и аппаратуры технических разведок, обоснования организационных и технических мероприятий по противодействию техническим

разведкам и использованию техники противодействия техническим разведкам. Выполняет расчеты, необходимые для оценки возможностей технических разведок и применения подразделений и средств противодействия техническим разведкам, участвует в оценке состояния противодействия техническим разведкам. Проводит работы по контролю эффективности противодействия техническим разведкам с использованием существующих методов и средств противодействия техническим разведкам, разрабатывает предложения по их совершенствованию. Осуществляет проверку выполнения требований нормативных документов по противодействию техническим разведкам. Разрабатывает и готовит к утверждению проекты документов, регламентирующих работу по противодействию техническим разведкам. Разрабатывает предложения для включения в соответствующие разделы перспективных и текущих планов работ и программ по противодействию техническим разведкам, готовит отзывы и заключения на проекты вновь строящихся и реконструируемых зданий и сооружений по вопросам противодействия техническим разведкам. Участвует в рассмотрении технических заданий на научно-исследовательские и опытно-конструкторские работы в области противодействия техническим разведкам, в обосновании организационных и технических мер по противодействию техническим разведкам. Участвует в разработке (доработке, модернизации) средств и систем противодействия техническим разведкам, в работах по оценке технико-экономического уровня и эффективности предлагаемых и реализуемых решений в области противодействия техническим разведкам. Определяет потребность в технических средствах противодействия техническим разведкам, составляет заявки на их приобретение с необходимыми обоснованиями и расчетами к ним, контролирует их поставку и использование. Участвует в экспертизе материалов, предназначенных для открытого опубликования.

Должен знать: законы и иные нормативные правовые акты Российской Федерации, регулирующие отношения, связанные с защитой государственной тайны и иной информации ограниченного доступа; нормативные и методические документы по вопросам, связанным с обеспечением противодействия техническим разведкам; специализацию и особенности деятельности организации; методики оценки возможностей технических разведок; порядок и содержание работ по противодействию техническим разведкам; достижения науки и техники в стране и за рубежом в области технических разведок и противодействия техническим разведкам; методы противодействия техническим разведкам, перспективы и направления развития организационных и технических мероприятий противодействия техническим разведкам; средства противодействия техническим разведкам и способы их применения; методы планирования, организации и выполнения работ по противодействию техническим разведкам; основные требования и мероприятия по обеспечению режима секретности; порядок пользования реферативными и справочно-информационными изданиями, а также другими источниками научно-технической информации; методики оценки профессионального уровня персонала; основы трудового законодательства; правила по охране труда и пожарной безопасности.

Требования к квалификации.

Специалист по противодействию техническим разведкам I категории: высшее профессиональное образование по специальности «Информационная безопасность» и стаж работы в должности специалиста по противодействию техническим разведкам II категории не менее 3 лет.

Специалист по противодействию техническим разведкам II категории: высшее профессиональное образование по специальности «Информационная безопасность» и стаж работы в должности специалиста по противодействию техническим разведкам или на других должностях, замещаемых специалистами с высшим профессиональным образованием, не менее 3 лет.

Специалист по противодействию техническим разведкам: высшее профессиональное образование по специальности «Информационная безопасность» без предъявления требований к стажу работы.

Специалист по технической защите информации

Должностные обязанности. Выполняет работы по технической защите информации в организациях. Проводит работы по выявлению угроз безопасности информации, определению возможности технической разведки и проведению мероприятий технической защиты информации. Участвует в категорировании объектов информатизации, выявлении угроз безопасности информации и технических каналов утечки информации, работах по проведению специальных проверок и специальных исследований объектов информатизации. Разрабатывает предложения по размещению основных и вспомогательных технических средств и систем с соблюдением установленных норм технической защиты информации. Организует и проводит (при необходимости) мероприятия по технической защите информации при размещении сторонних организаций в пределах контролируемой зоны. Участвует в обследовании объектов информатизации, их категорировании и аттестации. Разрабатывает и готовит к утверждению проекты нормативных и методических документов, регламентирующих работу по технической защите информации, акты проверки, протоколы испытаний, предписания на право эксплуатации, а также положения, инструкции и другие организационно-распорядительные документы. Участвует в определении потребности в средствах технической защиты информации, составляет заявки на их приобретение с необходимыми обоснованиями и расчетами к ним, контролирует их поставку и использование. Осуществляет проверку выполнения требований нормативных документов по технической защите информации.

Должен знать: законы и иные нормативные правовые акты Российской Федерации, регулирующие отношения, связанные с защитой государственной тайны и иной информации ограниченного доступа; нормативные и методические документы по вопросам, связанным с обеспечением защиты информации; методы и средства выявления угроз безопасности информации, способы выявления каналов утечки информации; специализацию, основы технологических процессов производства организации и последствия их нарушения; структуру управления, связи и автоматизации, оснащенность объектов информатизации организации основными и вспомогательными техническими средствами и системами, перспективы их развития и модернизации; достижения науки и техники в стране и за рубежом в области технических разведок и технической защиты информации; перспективы и направления развития технических и программно-аппаратных средств защиты информации; порядок и содержание специальных исследований и контрольных проверок, работ по категорированию, аттестации объектов информатизации и других работ по технической защите информации; методы планирования работ по технической защите информации; методы проведения научных

исследований, разработок по технической защите информации; документацию, разрабатываемую на объектах информатизации по технической защите информации; правила разработки и подготовки к утверждению проектов нормативных и методических документов, регламентирующих работу по технической защите информации, составления актов проверки, протоколов испытаний, предписаний на право эксплуатации средств технической защиты информации, а также положений, инструкций и других документов в области технической защиты информации; структуру, назначение, задачи, полномочия отдела по вопросам технической защиты информации; порядок применения штатных средств технической защиты информации и контроля ее эффективности; подсистемы разграничения доступа, подсистемы обнаружения атак, методы анализа результатов проверок, учета нарушений требований по технической защите информации; порядок подготовки предложений, методы и средства выполнения вычислительных работ в интересах планирования, организации и проведения работ по технической защите информации; порядок создания защищенных каналов между взаимодействующими объектами через систему общего пользования с использованием выделенных каналов связи; порядок осуществления аутентификации взаимодействующих объектов, проверки подлинности отправителя и целостности передаваемых через систему общего пользования данных; порядок пользования реферативными и справочно-информационными изданиями, а также другими источниками научно-технической информации; достижения науки и техники в стране и за рубежом в области технической разведки и технической защиты информации; основы трудового законодательства; правила по охране труда и пожарной безопасности.

Требования к квалификации.

Специалист по технической защите информации I категории: высшее профессиональное образование по специальности «Информационная безопасность» и стаж работы в должности специалиста по технической защите информации II категории не менее 3 лет.

Специалист по технической защите информации II категории: высшее профессиональное образование по специальности «Информационная безопасность» и стаж работы в должности специалиста по технической защите информации или на других должностях, замещаемых специалистами с высшим профессиональным образованием, не менее 3 лет.

Специалист по технической защите информации: высшее профессиональное образование по специальности «Информационная безопасность» без предъявления требования к стажу работы.

Администратор по обеспечению безопасности информации

Должностные обязанности. Устанавливает разграничение полномочий пользователей и порядок доступа к информационным ресурсам, порядок использования основных и вспомогательных технических средств и систем. Проводит контроль выполнения работниками организации работ согласно перечню мероприятий по обеспечению безопасности информации, ведет учет нештатных ситуаций; информирует руководство и уполномоченных работников службы безопасности об инцидентах и попытках несанкционированного доступа к информации, элементам автоматизированных систем управления по результатам функционирования и контроля систем технической защиты информации. Осуществляет администрирование сервисами и механизмами безопасности автоматизированных систем управления, комплексами и средствами технической защиты информации и контроля; прекращает работы при несоблюдении установленной технологии обработки информации и невыполнении требований информационной безопасности; готовит предложения по совершенствованию технологических мер защиты информации. Контролирует работы по установке, модернизации и профилактике аппаратных и программных средств; созданию, учету, хранению и использованию резервных и архивных копий массивов данных и электронных документов. Принимает участие в работах по внесению изменений в программно-аппаратную конфигурацию автоматизированных систем управления и контролирует ее соответствие требованиям обеспечения безопасности информации. Ведет учет носителей информации, осуществляет их хранение, прием, выдачу ответственным исполнителям, контролирует правильность их использования.

Должен знать: законы и иные нормативные правовые акты Российской Федерации, регулирующие отношения, связанные с защитой государственной тайны и иной информации ограниченного доступа; нормативные и методические документы по вопросам, связанным с обеспечением технической защиты информации; объекты информатизации, подлежащие защите; специализацию и направления деятельности организации и ее подразделений, применяемые информационные технологии и системы, структуру управления, связи, автоматизации; средства технической разведки и методы оценки их возможностей, угрозы безопасности информации и классификацию (категории) нарушений; оснащенность объектов информатизации основными и вспомогательными техническими средствами и системами, комплексами и средствами технической защиты информации, сервисами и механизмами безопасности автоматизированных систем управления; подсистемы разграничения доступа, подсистемы обнаружения атак, подсистемы защиты от преднамеренного воздействия, контроля целостности информации, перспективы их развития и модернизации; методы оценки результатов состояния систем безопасности, выявления каналов утечки информации, контроля процесса резервирования и дублирования критичных вычислительных и информационных ресурсов; порядок работы с техническими, программными, программно-аппаратными средствами защиты информации и контроля, сервисами и механизмами безопасности автоматизированных систем управления и аудита их состояния; основы трудового законодательства; правила по охране труда и пожарной безопасности.

Требования к квалификации. Высшее профессиональное образование по специальности «Информационная безопасность» и стаж работы в должности специалиста по защите информации не менее 3 лет.

Инженер по технической защите информации

Должностные обязанности. Выполняет работы по внедрению специальных технических и программно-математических средств защиты информации, обеспечению организационных и инженерно-технических мер защиты информационных систем. Разрабатывает планы и графики работ по техническому обслуживанию и ремонту электронного оборудования технических средств защиты информации и повышению эффективности его использования. Участвует в проверке, приемке и освоении вновь вводимого в эксплуатацию оборудования. Ведет учет неисправностей, поломок и аварий оборудования, анализирует причины и определяет направления их устранения; изучает режимы работы оборудования и условия его эксплуатации. Выполняет работы по эксплуатации, обслуживанию и ремонту средств технической защиты информации, разрабатывает предложения по доработке (модернизации) оборудования, повышающие его надежность, долговечность и эффективность применения. Составляет заявки на приобретение оборудования, запасного имущества, принадлежностей и материалов к нему, ремонт неисправных устройств. Организует хранение и списание оборудования и средств защиты информации, не подлежащих дальнейшему использованию по назначению.

Должен знать: законы и иные нормативные правовые акты Российской Федерации, регулирующие отношения, связанные с защитой государственной тайны и иной информации ограниченного доступа; нормативные и методические документы по защите информации в области технического регулирования производства и эксплуатации средств технической защиты информации; системы управления, связи и автоматизации, их технико-эксплуатационные характеристики, конструктивные особенности; систему материально-технического обеспечения организации; спецификацию изделий технической защиты информации, комплектующих, запасного имущества и ремонтных материалов; передовые технологии автоматизированной обработки информации и средства их защиты; принципы построения локальных и распределенных автоматизированных систем управления; правила применения электронного и испытательного оборудования, контрольно-измерительных приборов, комплексов и средств технической защиты информации, сетевого оборудования, стандартного программного обеспечения используемого электронного оборудования; методы и средства диагностики и поиска неисправностей оборудования; организацию эксплуатации, технического обслуживания и ремонта электронного и испытательного оборудования, контрольно-измерительных приборов, комплексов и средств технической защиты информации; основы трудового законодательства; правила по охране труда и пожарной безопасности.

Требования к квалификации. Высшее профессиональное образование по специальности «Информационная безопасность» без предъявления требований к стажу работы или среднее профессиональное образование по специальности «Информационная безопасность» и стаж работы в должности техника по защите информации I категории не менее 3 лет либо в других должностях, замещаемых специалистами со средним профессиональным образованием, не менее 5 лет.

Инженер-программист по технической защите информации

Должностные обязанности. Разрабатывает и внедряет программно-математические методы и средства обеспечения безопасности информации и контроля эффективности мероприятий по технической защите информации. Участвует в автоматизации информационно-аналитических процессов автоматизированных систем управления организации. Определяет виды и категории данных, подлежащих обработке средствами вычислительной техники комплексов, их объемы, структуру, макеты и схемы ввода, обработки, хранения и вывода информации, методы верификации и контроля целостности. Осуществляет сопровождение программ и программных средств, разрабатывает и внедряет системы автоматизированного тестирования программного обеспечения. Разрабатывает программные средства, позволяющие расширить область применения разрабатываемых комплексов, средств технической защиты информации и информационных технологий защиты информации, инструкции пользователей. Оформляет необходимую техническую документацию; определяет возможность и ограничения по использованию программных продуктов, устанавливает программные и программно-аппаратные антивирусные средства. Разрабатывает мероприятия по защите от программно-математического воздействия на информационные управляющие системы и сохранению целостности программного обеспечения и информации. Определяет объем и содержание данных тестовых примеров, обеспечивающих наиболее полную проверку работоспособности программ и соответствия их функциональному назначению. Выполняет работу по унификации и типизации вычислительных процессов, используемых при создании комплексов, средств технической защиты информации и информационных технологий защиты информации, созданию каталогов и картотек стандартных программ.

Должен знать: законы и иные нормативные правовые акты Российской Федерации, регулирующие отношения, связанные с защитой государственной тайны и иной информации ограниченного доступа; нормативные и методические документы, регламентирующие методы разработки алгоритмов и программного обеспечения средств вычислительной техники, используемых при обработке информации ограниченного доступа и в комплексах технической защиты информации; методы и средства разработки программного обеспечения, предназначенные для защиты информации; современные методы и формализованные языки программирования; основные принципы структурного программирования; технико-эксплуатационные характеристики, конструктивные особенности, назначение и режимы работы современных ЭВМ, правила их технической эксплуатации в комплексах технической защиты информации; методы проведения испытаний и отладки программных средств, используемых в комплексах технической защиты информации, угрозы безопасности автоматизированных систем управления и телекоммуникационных систем; подсистемы разграничения доступа, подсистемы обнаружения атак, подсистемы защиты от преднамеренного воздействия, контроля целостности критически важной информации; критерии оценки безопасности информационных технологий; сертифицированное программное обеспечение, технологию автоматизированной обработки информации и средств ее защиты, математические модели и алгоритмы решения задач по технической защите информации ограниченного доступа; порядок выполнения работ в ходе проведения научных исследований в области разработки программных и программно-аппаратных средств защиты информации; основы трудового законодательства; правила по охране труда и пожарной безопасности.

Требования к квалификации.

Инженер-программист по технической защите информации I категории: высшее профессиональное (техническое) образование и стаж работы в должности инженера-программиста по технической защите информации II категории не менее 3 лет.

Инженер-программист по технической защите информации II категории: высшее профессиональное (техническое) образование и стаж работы в должности инженера-программиста по технической защите информации или должностях, замещаемых специалистами с высшим профессиональным образованием, не менее 3 лет.

Инженер-программист по технической защите информации: высшее профессиональное (техническое) образование без предъявления требования к стажу работы или среднее профессиональное (техническое) образование и стаж работы в должности техника по защите информации I категории не менее 3 лет либо других должностях, замещаемых специалистами со средним профессиональным образованием, не менее 5 лет.

Техник по технической защите информации

Должностные обязанности. Выполняет работы по эксплуатации средств технической защиты и контроля информации, по оформлению протоколов специальных измерений и другой технической документации, связанной с эксплуатацией средств технической защиты и контроля информации в телекоммуникационных сетях и системах критически важных объектов. Осуществляет проверку технического состояния, установку и регулировку аппаратуры и приборов, проводит их профилактические осмотры, техническое обслуживание и текущий ремонт, определяет причины отказов в работе технических средств, готовит предложения по их устранению и предупреждению. Участвует во внедрении разработанных технических решений и проектов во взаимодействии с другими специалистами, оказывает техническую помощь исполнителям при изготовлении, монтаже, настройке, испытаниях и эксплуатации технических средств. Готовит технические средства к проведению всех видов плановых и внеплановых контрольных проверок, аттестации оборудования. Ведет формуляры основных, вспомогательных технических средств и систем, а также средств контроля. Обеспечивает своевременное списание и пополнение запасного имущества, приборов и принадлежностей.

Должен знать: законы и иные нормативные правовые акты Российской Федерации, регулирующие отношения, связанные с защитой государственной тайны и иной информации ограниченного доступа; нормативные и методические документы по вопросам, связанным с обеспечением защиты информации ограниченного доступа, а также учета, эксплуатации, хранения и списания техники и материальных средств; специализацию организации и особенности ее деятельности; методы и технические средства, используемые в целях обеспечения защиты информации; назначение, принципы работы и правила эксплуатации технических средств и систем, аппаратуры контроля, защиты и другого оборудования, используемого при проведении работ по защите информации; виды и порядок выполнения технического обслуживания и текущего ремонта, монтажных и наладочных работ; требования по оформлению и ведению технической документации; периодичность поверок контрольно-измерительной аппаратуры, порядок представления (сдачи, приема) ее по соответствующим актам в поверочную лабораторию, а в ремонтные органы - неисправных блоков (узлов) аппаратуры, не подлежащих восстановлению собственными силами; порядок выполнения технических расчетов, ведения протоколов и документации по технической защите информации; инструкции по соблюдению режима проведения специальных работ; спецификацию изделий, комплектующих, запасного имущества и ремонтных материалов, порядок их учета и хранения; основы трудового законодательства; правила по охране труда и пожарной безопасности.

Требования к квалификации.

Техник по защите информации I категории: среднее профессиональное образование по специальности «Информационная безопасность» и стаж работы в должности техника по защите информации II категории не менее 2 лет.

Техник по защите информации II категории: среднее профессиональное образование по специальности «Информационная безопасность» и стаж работы в должности техника по защите информации или других должностях, замещаемых специалистами со средним профессиональным образованием, не менее 2 лет.

Техник по защите информации: среднее профессиональное образование по специальности «Информационная безопасность» без предъявления требований к стажу работы.

безопасность критической информационной инфраструктуры

From:
http://www.sps-ib.ru/ - **Справочно-правовая система по информационной безопасности**

Permanent link:
http://www.sps-ib.ru/npa:mzsr205_22.04.2009

Last update: **2016/09/09 09:16**