**Об утверждении профессионального стандарта**

«**Специалист по информационной безопасности ИКТ систем**»

В соответствии с пунктом 16 Правил разработки, утверждения и применения профессиональных стандартов, утвержденных постановлением Правительства Российской Федерации от 22 января 2013 г. № 23 (Собрание законодательства Российской Федерации, 2013, № 4, ст. 293; 2014, № 39, ст. 5266), п р и к а з ы в а ю:

Утвердить прилагаемый профессиональный стандарт «Специалист по информационной безопасности ИКТ систем».

Министр М.А. Топилин

УТВЕРЖДЕН

приказом Министерства

труда и социальной защиты Российской Федерации

от «\_\_» \_\_\_\_\_\_2014 г. №\_\_\_

ПРОФЕССИОНАЛЬНЫЙ  
 СТАНДАРТ

**Специалист по информационной безопасности ИКТ систем**

|  |
| --- |
|  |
| Регистрационный номер |

**I. Общие сведения**

|  |  |  |
| --- | --- | --- |
| Защита инфокоммуникационной инфраструктуры предприятия и оконечных устройств сотрудников |  |  |
| (наименование вида профессиональной деятельности) | | Код |

Основная цель вида профессиональной деятельности:

|  |
| --- |
| Противодействие вредоносному влиянию программно-технического воздействия на подсистемы, устройства, элементы и каналы инфокоммуникационных систем |

Группа занятий:

|  |  |  |  |
| --- | --- | --- | --- |
| 2139 | Специалисты по компьютерам не вошедшие в другие группы | 2144 | Инженеры-электроники, инженеры по связи и приборостроению |
| (код ОКЗ[[1]](#endnote-1)) | (наименование) | (код ОКЗ) | (наименование) |

Отнесение к видам экономической деятельности:

|  |  |
| --- | --- |
| 75.24 | Деятельность по обеспечению общественного порядка и безопасности. Обеспечение безопасности средств связи и информации |
| (код ОКВЭД[[2]](#endnote-2)) | (наименование вида экономической деятельности) |

**II. Описание трудовых функций, входящих в профессиональный стандарт   
(функциональная карта вида трудовой деятельности)**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Обобщенные трудовые функции | | | Трудовые функции | | |
| код | наименование | уровень квалификации | наименование | код | уровень (подуровень) квалификации |
| A | Эксплуатация защищенных инфокоммуникационных систем и применение методов и средств обеспечения их безопасности | 6 | Применение про­граммно-аппаратных средств обеспечения информационной безопасности в инфокоммуникационных системах | A/01.6 | 6 |
| Применение инженерно-технических средств обеспече­ния информацион­ной безопасности защищенных инфокоммуникационных систем | A/02.6 |
| Эксплуатация ком­плексных систем обеспечения информационной безопасности в инфокоммуникационных системах | A/03.6 |
| B | Администрирование и поддержка программно-аппаратных средств защиты информации в инфокоммуникационных системах | 6 | Настройка программно-аппаратных средств защиты инфокоммуникационных систем | B/01.6 | 6 |
| Проведение регламентов технического обслуживания и текущего ремонта систем безопасности инфокоммуникационных систем | B/02.6 |
| Внедрение программно-аппаратных средств защиты информации | B/03.6 |
| C | Разработка и применение методов оценки безопасности инфокоммуникационных систем, аттестация объектов информатизации | 7 | Проведение контрольных проверок работоспособности и эффективности применяемых программно-аппаратных средств защиты информации | C/01.7 | 7 |
| Применение методов и методик оценки безопасности инфокоммуникационных систем при проведении контрольного анализа системы защиты | C/02.7 |
| Разработка требований по защите, составление политик безопасности инфокоммуникационных систем | C/03.7 |
| Проведение экспериментально-исследовательских работ при аттестации объектов с учетом требований к обеспечению защищенности инфокоммуникационной системы | C/04.7 |
| Проведение инструментального мониторинга защищенности инфокоммуникационных систем | C/05.7 |
| Проведение экспертизы при расследовании инфокоммуникационных преступлений, правонарушений и инцидентов | C/06.7 |
| D | Создание  распределенных защищенных инфокоммуникационных систем | 7 | Разработка требований к распределенным защищенным инфокоммуникационным системам и средствам защиты для них с учетом действующих нормативных и методических документов | D/01.7 | 7 |
| Проектирование распределенных защищенных инфокоммуникационных систем | D/02.7 |
| Ввод в эксплуатацию и сопровождение распределенных инфокоммуникационных систем с использованием комплексов  средств защиты информации и организационно-технических мероприятий по информационной безопасности | D/03.7 |

**III. Характеристика обобщенных трудовых функций**

**3.1. Обобщенная трудовая функция**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Эксплуатация защищенных инфокоммуникационных систем и применение методов и средств обеспечения их безопасности | Код | A | Уровень квалификации | 6 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Происхождение обобщенной трудовой функции | Оригинал | X | Заимствовано из оригинала |  |  |  |
|  |  |  |  |  | Код оригинала | Регистрационный номер профессионального стандарта |

|  |  |
| --- | --- |
| Возможные наименования должностей | Техник по защите инфокоммуникационных систем  Старший техник по защите инфокоммуникационных систем |

|  |  |
| --- | --- |
| Требования к образованию и обучению | Среднее профессиональное образование - программы подготовки специалистов среднего звена или высшее образование - бакалавриат Дополнительное профессиональное образование – программы повышения квалификации, программы профессиональной переподготовки в области информационной безопасности инфокоммуникационных систем и/или их составляющих |
| Требования к опыту практической работы | - |
| Особые условия допуска к работе | - |

Дополнительные характеристики

|  |  |  |
| --- | --- | --- |
| Наименование документа | Код | Наименование базовой группы, должности (профессии) или специальности |
| ОКЗ | 2139 | Специалисты по компьютерам не вошедшие в другие группы |
| ОКЗ | 2144 | Инженеры-электроники, инженеры по связи и приборостроению |
| ОКСО | 220600 | Организация и технология защиты информации |
| ОКСО | 210400 | Телекоммуникации |
| ОКСО | 230101 | Вычислительные машины, комплексы, системы и сети |

**3.1.1. Трудовая функция**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Применение программно-аппаратных средств обеспечения информационной безопасности в инфокоммуникационных системах | Код | A/01.6 | Уровень (подуровень) квалификации | 6 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Происхождение обобщенной трудовой функции | Оригинал | X | Заимствовано из оригинала |  |  |  |
|  |  |  |  |  | Код оригинала | Регистрационный номер профессионального стандарта |

|  |  |
| --- | --- |
| Трудовые действия | Установка программно-аппаратных средств обеспечения информационной безопасности в инфокоммуникационных системах |
| Настройка программно-аппаратных средств обеспечения информационной безопасности в инфокоммуникационных системах |
| Поддержка программно-аппаратных средств обеспечения информационной безопасности в инфокоммуникационных системах |
| Необходимые умения | Применять программно-аппаратные средства обеспече­ния информационной безопасности в системах |
| Осуществлять техническое обслуживание программно-аппаратных средств обеспечения информационной безопасности |
| Осуществлять текущий ремонт программно-аппаратных средств обеспечения информационной безопасности |
| Проводить мониторинг эффективности программно-аппаратных средств обеспечения информационной безопасности |
| Обеспечивать учет, хранение и передачу носителей с конфиденциальной информацией не составляющей государственную тайну и средств защиты |
| Необходимые знания | Сущность и понятие информационной безопасности, основные характеристики ее составляющих |
| Источники угроз информационной безопасности и меры по их предотвращению |
| Современные программно-аппаратные средства и способы обеспечения информационной безопасности |
| Основы организации учета носителей информации с грифами конфиденциальной информации не составляющей государственную тайну |
| Другие характеристики | - |

**3.1.2. Трудовая функция**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Применение инженерно-технических средств обеспечения информацион­ной безопасности защищенных инфокоммуникационных систем | Код | A/02.6 | Уровень (подуровень) квалификации | 6 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Происхождение трудовой функции | Оригинал | X | Заимствовано из оригинала |  |  |  |
|  |  |  |  |  | Код оригинала | Регистрационный номер профессионального стандарта |

|  |  |
| --- | --- |
| Трудовые действия | Установка инженерно-технических средств обеспечения информационной безопасности защищенных инфокоммуникационных систем |
| Настройка инженерно-технических средств обеспечения информационной безопасности защищенных инфокоммуникационных систем |
| Поддержка инженерно-технических средств обеспечения информационной безопасности защищенных инфокоммуникационных систем |
| Необходимые умения | Эксплуатировать инженерно-технические средства обеспечения информационной безопасности |
| Проводить мониторинг эффективности инженерно-технических средств обеспечения информационной безопасности в инфокоммуникационных системах |
| Необходимые знания | Сущность и понятие информационной безопасности, основные характеристики ее составляющих |
| Источники угроз информационной безопасности и меры по их предотвращению |
| Современные инженерно-технические средства и способы обеспечения информационной безопасности в инфокоммуникационных системах |
| Другие характеристики | - |

**3.1.3. Трудовая функция**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Эксплуатация комплексных систем обеспечения информационной безопасности в инфокоммуникационных системах | Код | A/03.6 | Уровень (подуровень) квалификации | 6 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Происхождение трудовой функции | Оригинал | X | Заимствовано из оригинала |  |  |  |
|  |  |  |  |  | Код оригинала | Регистрационный номер профессионального стандарта |

|  |  |
| --- | --- |
| Трудовые действия | Контроль технического состояния комплексных систем обеспечения информационной безопасности в инфокоммуникационных системах |
| Настройка комплексных систем обеспечения информационной безопасности в инфокоммуникационных системах |
| Проведение технического обслуживания комплексных систем обеспечения информационной безопасности в инфокоммуникационных системах |
| Устранение отказов и восстановле­ние работоспособности комплексных систем обеспечения информационной безопасности в инфокоммуникационных системах |
| Необходимые умения | Выполнять работы по администрированию подсистем безопасности инфокоммуникационных систем |
| Производить установку и адаптацию компонентов подсистем безопасности инфокоммуникационных систем |
| Выявлять отказы, возникающие при работе комплексных систем обеспечения информационной безопасности в инфокоммуникационных системах |
| Вести техническую документацию, связанную с эксплуатацией средств технической защиты и контроля информации в инфокоммуникационных системах |
| Необходимые знания | Состав и принципы работы защищенных инфокоммуникационных систем, операционных систем и сред |
| Особенности применения программно-аппаратных и инженерно-технических средств обеспечения информационной безопасности в операционных системах, базах данных, инфокоммуникационных сетях |
| Источники угроз информационной безопасности и меры по их устранению |
| Другие характеристики | - |

**3.2. Обобщенная трудовая функция**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Администрирование и поддержка программно-аппаратных средств защиты информации в инфокоммуникационных системах | Код | B | Уровень (подуровень) квалификации | 6 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Происхождение трудовой функции | Оригинал | X | Заимствовано из оригинала |  |  |  |
|  |  |  |  |  | Код оригинала | Регистрационный номер профессионального стандарта |

|  |  |
| --- | --- |
| Возможные наименования должностей | Инженер по информационной безопасности инфокоммуникационных систем  Администратор информационной безопасности инфокоммуникационных систем |

|  |  |
| --- | --- |
| Требования к образованию и обучению | Среднее профессиональное образование - программы подготовки специалистов среднего звена или высшее образование - бакалавриат    Дополнительное профессиональное образование – программы повышения квалификации, программы профессиональной переподготовки в области информационной безопасности инфокоммуникационных систем и/или их составляющих |
| Требования к опыту практической работы | При высшем профессиональном (техническом) образовании - без предъявления требований к стажу работы, при среднем профессиональном (техническом) образовании и стаже работы в должности старшего техника по защите инфокоммуникационных систем - не менее 1 года |
| Особые условия допуска к работе | - |

Дополнительные характеристики

|  |  |  |
| --- | --- | --- |
| Наименование документа | Код | Наименование базовой группы, должности (профессии) или специальности |
| ОКЗ | 2139 | Специалисты по компьютерам, не вошедшие в другие группы |
| ОКЗ | 2144 | Инженеры-электроники, инженеры по связи и приборостроению |
| ОКСО | 220600 | Организация и технология защиты информации |
| ОКСО | 210400 | Телекоммуникации |
| ОКСО | 230101 | Вычислительные машины, комплексы, системы и сети |

**3.2.1. Трудовая функция**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Настройка программно-аппаратных средств защиты инфокоммуникационных систем | Код | B/01.6 | Уровень (подуровень) квалификации | 6 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Происхождение трудовой функции | Оригинал | X | Заимствовано из оригинала |  |  |  |
|  |  |  |  |  | Код оригинала | Регистрационный номер профессионального стандарта |

|  |  |
| --- | --- |
| Трудовые действия | Определение состава подсистем информационной безопасности |
| Настройка подсистем информационной безопасности |
| Контроль соответствия параметров подсистем информационной безопасности установленным требованиям |
| Установка программного обеспечения, необходимого для администрирования |
| Настройка программного обеспечения, необходимого для администрирования |
| Формирование политики информационной безопасности организации и контроль выполнения ее требований |
| Оценка полноты и качества выполнения сотрудниками организации требований политики безопасности |
| Проведение аттестации на предмет соответствия требованиям по защите инфокоммуникационных систем |
| Необходимые умения | Анализировать и оценивать угрозы информационной безопасности системы |
| Применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях |
| Осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты |
| Формулировать и настраивать политику безопасности основных операционных систем, а также локальных инфокоммуникационных сетей, построенных на их основе |
| Проводить анализ показателей качества сетей и систем связи |
| Необходимые знания | Требования по составу и характеристикам подсистем защиты информации для различных классов защищенных систем, методы их практической реализации |
| Основные виды политик управления доступом и информационными потоками в инфокоммуникационных системах |
| Принципы построения современных операционных систем и особенности их применения для решения задач защиты информации |
| Механизмы реализации вредоносных программно-технических и информационных воздействий в инфокоммуникационных системах |
| Защитные механизмы и средства обеспечения сетевой безопасности |
| Средства и методы предотвращения и обнаружения вторжений |
| Основные средства и методы анализа программных реализаций |
| Другие характеристики | - |

**3.2.2. Трудовая функция**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Проведение регламентов технического обслуживания и текущего ремонта систем безопасности инфокоммуникационных систем | Код | B/02.6 | Уровень (подуровень) квалификации | 6 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Происхождение трудовой функции | Оригинал | X | Заимствовано из оригинала |  |  |  |
|  |  |  |  |  | Код оригинала | Регистрационный номер профессионального стандарта |

|  |  |
| --- | --- |
| Трудовые действия | Установка аппаратно-программных средств защиты информации |
| Настройка аппаратно-программных средств защиты информации |
| Эксплуатация аппаратно-программных средств защиты информации |
| Обслуживание аппаратно-программных средств защиты информации |
| Профилактическая проверка технического состояния и остаточного ресурса оборудования защиты информации, организация профилактических проверок и текущего ремонта |
| Составление инструкций по эксплуатации аппаратно-программных средств защиты информации |
| Определение потребности в технических средствах защиты и контроля |
| Ведение эксплуатационной, технической и отчетной документации |
| Необходимые умения | Устанавливать аппаратно-программные средства защиты информации |
| Настраивать аппаратно-программные средства защиты информации |
| Эксплуатировать и обслуживать аппаратно-программные средства защиты информации |
| Оценивать остаточный ресурс оборудования защиты информации |
| Применять техническую литературу по ремонту средств защиты информации |
| Необходимые знания | Принципы работы и правила эксплуатации технических средств получения, обработки, передачи, отображения и хранения информации, аппаратуры контроля, защиты и другого оборудования |
| Регламенты организации ремонта и технического обслуживания |
| Методы измерений, контроля и технических расчетов |
| Порядок оформления технической документации по защите информации |
| Инструкции по соблюдению режима проведения работ, связанных с обеспечением информационной безопасности |
| Другие характеристики | - |

**3.2.3. Трудовая функция**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Внедрение программно-аппаратных средств защиты информации | Код | B/03.6 | Уровень (подуровень) квалификации | 6 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Происхождение трудовой функции | Оригинал | X | Заимствовано из оригинала |  |  |  |
|  |  |  |  |  | Код оригинала | Регистрационный номер профессионального стандарта |

|  |  |
| --- | --- |
| Трудовые действия | Приемка от поставщика и/или исполнителя работ программно-аппаратных средств защиты информации |
| Освоение вводимых программно-аппаратных средств защиты информации |
| Необходимые умения | Проверять и оценивать соответствие реальных характеристик программно-аппаратных средств защиты информации, заявленным в технической документации на эти средства |
| Оформлять необходимую документацию по приемке и постановке на учет в организации приобретаемых программно-аппаратных средств защиты информации |
| Использовать техническую документацию, техническую литературу и справочники при освоении программно-аппаратных средств защиты информации |
| Необходимые знания | Принципы работы и правила эксплуатации приобретаемых программно-аппаратных средств защиты информации |
| Методы измерений и контроля характеристик программно-аппаратных средств защиты информации |
| Порядок оформления документации по приемке и постановке на учет в организации приобретаемых программно-аппаратных средств защиты информации |
| Правила и нормы охраны труда, техники безопасности, производственной (промышленной) санитарии и противопожарной защиты |
| Другие характеристики | - |

**3.3. Обобщенная трудовая функция**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Разработка и применение методов оценки безопасности инфокоммуникационных систем, аттестация объектов информатизации | Код | С | Уровень квалификации | 7 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Происхождение обобщенной трудовой функции | Оригинал | X | Заимствовано из оригинала |  |  |  |
|  |  |  |  |  | Код оригинала | Регистрационный номер профессионального стандарта |

|  |  |
| --- | --- |
| Возможные наименования должностей | Специалист по безопасности инфокоммуникационных систем  Эксперт в области информационной безопасности |

|  |  |
| --- | --- |
| Требования к образованию и обучению | Высшее образование – магистратура или специалитет  Дополнительное профессиональное образование – программы повышения квалификации, программы профессиональной переподготовки в области информационной безопасности инфокоммуникационных систем и/или их составляющих |
| Требования к опыту практической работы | Стаж работы по защите информации на инженерно-технических должностях не менее 3 лет |
| Особые условия допуска к работе | - |

Дополнительные характеристики

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | Наименование документа | Код | Наименование базовой группы, должности (профессии) или специальности | | ОКЗ | 2139 | Специалисты по компьютерам не вошедшие в другие группы | | ОКЗ | 2144 | Инженеры-электроники, инженеры по связи и приборостроению | | ОКСО | 220600 | Организация и технология защиты информации | | ОКСО | 210400 | Телекоммуникации | | ОКСО | 230101 | Вычислительные машины, комплексы, системы и сети | |

**3.3.1. Трудовая функция**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Проведение контрольных проверок работоспособности и эффективности применяемых программно-аппаратных средств защиты информации | Код | C/01.7 | Уровень (подуровень) квалификации | 7 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Происхождение трудовой функции | Оригинал | X | Заимствовано из оригинала |  |  |  |
|  |  |  |  |  | Код оригинала | Регистрационный номер профессионального стандарта |

|  |  |
| --- | --- |
| Трудовые действия | Проведение контрольных проверок работоспособности и эффективности применяемых программно-аппаратных средств защиты информации |
| Мониторинг эффективности применяемых программно-аппаратных средств защиты информации |
| Необходимые умения | Оценивать работоспособность и эффективность применяемых программно-аппаратных средств защиты информации |
| Анализировать программно-аппаратных средства защиты с целью определения уровня обеспечиваемой ими защищенности и доверия |
| Необходимые знания | Действующие нормативно-правовые акты, в части информационной безопасности |
| Принципы работы и правила эксплуатации технических средств получения, обработки, передачи, отображения и хранения информации, аппаратуры контроля, защиты и другого оборудования |
| Другие характеристики | - |

**3.3.2. Трудовая функция**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Применение методов и методик оценки безопасности инфокоммуникационных систем при проведении контрольного анализа системы защиты | Код | C/02.7 | Уровень (подуровень) квалификации | 7 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Происхождение трудовой функции | Оригинал | X | Заимствовано из оригинала |  |  |  |
|  |  |  |  |  | Код оригинала | Регистрационный номер профессионального стандарта |

|  |  |
| --- | --- |
| Трудовые действия | Применение типовых методов и методик оценки безопасности инфокоммуникационных систем при проведении контрольного анализа системы защиты |
| Применение нетиповых методов и методик оценки безопасности инфокоммуникационных систем при проведении контрольного анализа системы защиты |
| Необходимые умения | Анализировать инфокоммуникационную систему с целью определения уровня защищенности и доверия |
| Готовить аналитический отчет по результатам проведенного анализа и формулировать предложения по устранению выявленных уязвимостей |
| Применять нормативные и правовые акты при проведении криминалистической экспертизы и криминалистического анализа |
| Необходимые знания | Действующие нормативно-правовые акты, в части информационной безопасности |
| Основные принципы построения защищенных инфокоммуникационных систем |
| Основные принципы построения систем обнаружения инфокоммуникационных атак |
| Способы обнаружения и нейтрализации последствий вторжений в инфокоммуникационную систему |
| Методы проведения расследования инфокоммуникационных инцидентов |
| Методы и методики оценки безопасности инфокоммуникационных систем |
| Другие характеристики | - |

**3.3.3. Трудовая функция**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Разработка требований по защите, составление политик безопасности инфокоммуникационных систем | Код | C/03.7 | Уровень (подуровень) квалификации | 7 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Происхождение трудовой функции | Оригинал | X | Заимствовано из оригинала |  |  |  |
|  |  |  |  |  | Код оригинала | Регистрационный номер профессионального стандарта |

|  |  |
| --- | --- |
| Трудовые действия | Разработка требований по защите инфокоммуникационных систем |
| Составление политик безопасности инфокоммуникационных систем |
| Консультирование по вопросам безопасности инфокоммуникационных cистем |
| Необходимые умения | Анализировать инфокоммуникационную систему с целью определения необходимого уровня защищенности и доверия |
| Разрабатывать профили защиты и формулировать задания по безопасности, формировать политики безопасности инфокоммуникационных систем |
| Необходимые знания | Действующие нормативно-правовые акты, в части информационной безопасности |
| Основные принципы построения защищенных инфокоммуникационных систем |
| Модели безопасности инфокоммуникационных систем |
| Основные виды политик безопасности инфокоммуникационных систем |
| Методы и методики оценки безопасности инфокоммуникационных систем |
| Другие характеристики | - |

**3.3.4. Трудовая функция**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Проведение экспериментально-исследовательских работ при аттестации объектов с учетом требований к обеспечению защищенности инфокоммуникационной системы | Код | C/04.7 | Уровень (подуровень) квалификации | 7 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Происхождение трудовой функции | Оригинал | X | Заимствовано из оригинала |  |  |  |
|  |  |  |  |  | Код оригинала | Регистрационный номер профессионального стандарта |

|  |  |
| --- | --- |
| Трудовые действия | Разработка программ аттестационных испытаний, определяющих порядок, методы, условия и объем проведения аттестационных испытаний объектов на соответствие требованиям по безопасности информации |
| Разработка методик аттестационных испытаний, определяющих порядок, методы, условия и объем проведения аттестационных испытаний объектов на соответствие требованиям по безопасности информации |
| Необходимые умения | Анализировать объекты информатизации и телекоммуникации с целью определения уровня защищенности |
| Применять нормативные и правовые акты по аттестации объектов с учетом требований к обеспечению защищенности инфокоммуникационной системы |
| Необходимые знания | Основные способы обеспечения защищенности объектов инфокоммуникационных систем |
| Основные принципы построения защищенных объектов инфокоммуникационных систем |
| Методы оценки безопасности инфокоммуникационных систем |
| Методики оценки безопасности инфокоммуникационных систем |
| Другие характеристики | - |

**3.3.5. Трудовая функция**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Проведение инструментального мониторинга защищенности инфокоммуникационных систем | Код | C/05.7 | Уровень (подуровень) квалификации | 7 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Происхождение трудовой функции | Оригинал | X | Заимствовано из оригинала |  |  |  |
|  |  |  |  |  | Код оригинала | Регистрационный номер профессионального стандарта |

|  |  |
| --- | --- |
| Трудовые действия | Установка аппаратных средств инструментального мониторинга защищенности инфокоммуникационных систем |
| Установка программных средств инструментального мониторинга защищенности инфокоммуникационных систем |
| Проведение мониторинга защищенности инфокоммуникационных систем |
| Необходимые умения | Устанавливать аппаратные средств инструментального мониторинга защищенности администрируемой инфокоммуникационной системы в соответствии с инструкцией по установке |
| Устанавливать программные средств инструментального мониторинга защищенности администрируемой инфокоммуникационной системы в соответствии с инструкцией по установке |
| Формализовать задачи управления безопасностью инфокоммуникационных систем |
| Применять современные инструментальные средства проведения мониторинга защищенности инфокоммуникационных систем |
| Необходимые знания | Основные принципы построения защищенных распределенных и локальных инфокоммуникационных систем |
| Основные принципы построения систем обнаружения инфокоммуникационных атак |
| Способы обнаружения и нейтрализации последствий вторжений в инфокоммуникационные системы |
| Инструкции по установке аппаратных и программных средств инструментального мониторинга защищенности администрируемой инфокоммуникационной системы |
| Инструкции по эксплуатации аппаратных и программных средств инструментального мониторинга защищенности администрируемой инфокоммуникационной системы |
| Другие характеристики | - |

**3.3.6. Трудовая функция**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Проведение экспертизы при расследовании инфокоммуникационных преступлений, правонарушений и инцидентов | Код | C/06.7 | Уровень (подуровень) квалификации | 7 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Происхождение трудовой функции | Оригинал | X | Заимствовано из оригинала |  |  |  |
|  |  |  |  |  | Код оригинала | Регистрационный номер профессионального стандарта |

|  |  |
| --- | --- |
| Трудовые действия | Проведение криминалистического анализа при расследовании инфокоммуникационных преступлений, правонарушений и инцидентов |
| Выработка предложений по устранению инфокоммуникационных преступлений, правонарушений, инцидентов, выявленных уязвимостей |
| Необходимые умения | Применять нормативные и правовые акты при проведении криминалистической экспертизы и криминалистического анализа |
| Проводить криминалистический анализ |
| Прогнозировать возможные пути развития новых видов инфокоммуникационных преступлений, правонарушений и инцидентов |
| Необходимые знания | Основные уязвимости защищенных инфокоммуникационных систем |
| Способы обнаружения и нейтрализации последствий вторжений в инфокоммуникационные системы |
| Методы и методики проведения расследования инфокоммуникационных преступлений, правонарушений и инцидентов |
| Действующие нормативно-правовые акты в области предупреждения и расследования инфокоммуникационных преступлений, правонарушений и инцидентов |
| Другие характеристики | - |

**3.4. Обобщенная трудовая функция**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Создание распределенных защищенных инфокоммуникационных | Код | D | Уровень квалификации | 7 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Происхождение обобщенной трудовой функции | Оригинал | X | Заимствовано из оригинала |  |  |  |
|  |  |  |  |  | Код оригинала | Регистрационный номер профессионального стандарта |

|  |  |
| --- | --- |
| Возможные наименования должностей | Специалист по защите информации  Главный специалист по защите информации  Руководитель проекта по информационной безопасности инфокоммуникационных систем |

|  |  |
| --- | --- |
| Требования к образованию и обучению | Высшее образование – магистратура или специалитет  Дополнительное профессиональное образование – программы повышения квалификации, программы профессиональной переподготовки в области информационной безопасности инфокоммуникационных систем и/или их составляющих |
| Требования к опыту практической работы | - |
| Особые условия допуска к работе | - |

Дополнительные характеристики

|  |  |  |
| --- | --- | --- |
| Наименование документа | Код | Наименование базовой группы, должности (профессии) или специальности |
| ОКЗ | 2139 | Специалисты по компьютерам не вошедшие в другие группы |
| ОКЗ | 2144 | Инженеры-электроники, инженеры по связи и приборостроению |
| ОКСО | 220600 | Организация и технология защиты информации |
| ОКСО | 210400 | Телекоммуникации |
| ОКСО | 230101 | Вычислительные машины, комплексы, системы и сети |

**3.4.1. Трудовая функция**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Разработка требований к распределенным защищенным системам и средствам защиты для них с учетом действующих нормативных и методических документов | Код | D/01.7 | Уровень (подуровень) квалификации | 7 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Происхождение трудовой функции | Оригинал | X | Заимствовано из оригинала |  |  |  |
|  |  |  |  |  | Код оригинала | Регистрационный номер профессионального стандарта |

|  |  |
| --- | --- |
| Трудовые действия | Определение угроз безопасности, возможных источников и каналов утечки информации |
| Выработка решений и мер по обеспечению защиты информации |
| Принятие решений и мер по обеспечению защиты информации |
| Оценка технико-экономического уровня и эффективности предлагаемых и реализуемых технических решений |
| Необходимые умения | Подбирать, изучать и обобщать научно-техническую литературу, нормативные и методические материалы по средствам и способам защиты информации |
| Разрабатывать модели угроз и модели нарушителя безопасности инфокоммуникационных систем |
| Оптимизировать подходы к обеспечению защиты информации инфокоммуникационной системы |
| Разрабатывать частные политики безопасности инфокоммуникационных систем, в том числе политики управления доступом и информационными потоками |
| Применять отечественные и зарубежные стандарты в области информационной безопасности для оценки защищенности инфокоммуникационной системы |
| Применять нормативно-правовые акты в области обеспечения информационной безопасности |
| Необходимые знания | Нормативно-правовые акты по вопросам, связанным с обеспечением информационной безопасностью |
| Методы и средства получения, обработки и передачи информации в современных операционных системах, системах управления базами данных и инфокоммуникационных сетях, методы и средства их защиты |
| Основные виды атак и механизмы их реализации в инфокоммуникационных системах |
| Методы выявления каналов утечки информации и организации технической разведки |
| Принципы построения защищенных систем и средств защиты информации инфокоммуникационных систем |
| Основные формальные модели управления доступом |
| Типовые криптографические протоколы и стандарты |
| Порядок сертификации средств защиты информации |
| Порядок лицензирования организаций, разрабатывающих средства защиты информации |
| Другие характеристики | - |

**3.4.2. Трудовая функция**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Проектирование распределенных защищенных инфокоммуникационных систем | Код | D/02.7 | Уровень (подуровень) квалификации | 7 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Происхождение трудовой функции | Оригинал | X | Заимствовано из оригинала |  |  |  |
|  |  |  |  |  | Код оригинала | Регистрационный номер профессионального стандарта |

|  |  |
| --- | --- |
| Трудовые действия | Разработка технических заданий на проектирование распределенных защищенных инфокоммуникационных систем |
| Разработка эскизных проектов распределенных защищенных инфокоммуникационных систем |
| Разработка технических проектов распределенных защищенных инфокоммуникационных систем |
| Разработка рабочих проектов распределенных защищенных инфокоммуникационных систем |
| Разработка планов и графиков проведения работ по проектированию распределенных защищенных инфокоммуникационных систем |
| Анализ существующих методов и средств, применяемых для контроля и защиты информации |
| Разработка предложений по совершенствованию и повышению эффективности существующих методов и средств, применяемых для контроля и защиты информации |
| Проектирование программных, аппаратных и программно-аппаратных средств защиты информации в соответствии с техническим заданием |
| Оценка технико-экономического уровня и эффективности предлагаемых и реализуемых технических решений |
| Необходимые умения | Проводить исследования с целью нахождения наиболее целесообразных практических решений по обеспечению защиты информации |
| Применять отечественные и зарубежные стандарты в области информационной безопасности для проектирования средств защиты информации инфокоммуникационной системы |
| Создавать и сопровождать архитектуру средств защиты информации |
| Подбирать, изучать и обобщать научно-техническую литературу, нормативные и методические материалы по техническим средствам и способам защиты информации |
| Необходимые знания | Нормативно-правовые акты по вопросам, связанным с обеспечением информационной безопасности |
| Основные виды атак и механизмы их реализации в инфокоммуникационных системах |
| Методы и средства получения, обработки и передачи информации в современных операционных системах, системах управления базами данных и инфокоммуникационных сетях, методы и средства их защиты |
| Принципы построения систем защиты информации инфокоммуникационных систем |
| Основные формальные модели управления доступом |
| Принципы и методы проектирования программно-аппаратного обеспечения, технологии разработки программного обеспечения |
| Другие характеристики | - |

**3.4.3. Трудовая функция**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Ввод в эксплуатацию и сопровождение распределенных инфокоммуникационных систем с использованием комплексов  средств защиты информации и организационно-технических мероприятий по информационной безопасности | Код | D/03.7 | Уровень (подуровень) квалификации | 7 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Происхождение трудовой функции | Оригинал | X | Заимствовано из оригинала |  |  |  |
|  |  |  |  |  | Код оригинала | Регистрационный номер профессионального стандарта |

|  |  |
| --- | --- |
| Трудовые действия | Применение программно-аппаратных средств обеспечения информационной безопасности в инфокоммуникационных системах |
| Применение инженерно-технических средств обеспечения информационной безопасности защищенных инфокоммуникационных систем |
| Контроль соответствия параметров подсистем информационной безопасности установленным требованиям |
| Установка программного обеспечения, необходимого для администрирования |
| Настройка программного обеспечения, необходимого для администрирования |
| Формирование политики информационной безопасности организации и контроль выполнения ее требований |
| Проведение аттестации на предмет соответствия требованиям по защите инфокоммуникационных систем |
| Проверка технического состояния и остаточного ресурса оборудования защиты информации |
| Организация профилактических проверок состояния и остаточного ресурса оборудования защиты информации |
| Организация текущего ремонта состояния и остаточного ресурса оборудования защиты информации |
| Определение потребности в технических средствах защиты и контроля |
| Проведение инструментального мониторинга защищенности инфокоммуникационных систем |
| Подготовка аналитических отчетов по результатам анализа инфокоммуникационных преступлений, правонарушений, инцидентов, выявленных уязвимостей |
| Выработка предложений по устранению инфокоммуникационных преступлений, правонарушений, инцидентов, выявленных уязвимостей |
| Определение угроз безопасности, возможных источников и каналов утечки информации |
| Выработка решений и мер по обеспечению защиты информации |
| Принятие решений и мер по обеспечению защиты информации |
| Необходимые умения | Руководить техническим обслуживанием и текущим ремонтом программно-аппаратных средств обеспечения информационной безопасности |
| Контролировать работы по администрированию подсистем безопасности инфокоммуникационных систем |
| Контролировать установку и адаптацию компонентов подсистем безопасности инфокоммуникационных систем |
| Анализировать и оценивать угрозы информационной безопасности системы |
| Осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты |
| Оценивать полноту и качество выполнения сотрудниками организации требований политики безопасности |
| Устанавливать, настраивать, эксплуатировать и обслуживать аппаратно-программных средств защиты информации |
| Использовать техническую документацию, техническую литературу и справочники при сопровождении распределенных инфокоммуникационных систем с использованием комплексов средств защиты информации и организационно-технических мероприятий по информационной безопасности |
| Использовать профили защиты и заданий по безопасности |
| Прогнозировать возможные пути развития новых видов инфокоммуникационных преступлений, правонарушений и инцидентов |
| Необходимые знания | Источники угроз информационной безопасности и меры по их предотвращению |
| Современные программно-аппаратные средства и способы обеспечения информационной безопасности |
| Современные инженерно-технические средства и способы обеспечения информационной безопасности в инфокоммуникационных системах |
| Состав и принципы работы защищенных инфокоммуникационных систем, операционных систем и сред |
| Источники угроз информационной безопасности и меры по их устранению |
| Требования по составу и характеристикам подсистем защиты информации для различных классов защищенных систем, методы их практической реализации |
| Механизмы реализации вредоносных программно-технических и информационных воздействий в инфокоммуникационных системах |
| Защитные механизмы и средства обеспечения сетевой безопасности |
| Средства и методы предотвращения и обнаружения вторжений |
| Содержание и порядок аттестации инфокоммуникационных систем на предмет их соответствия требованиям по защите информации |
| Знания по организации ремонта и технического обслуживания |
| Принципы работы и правила эксплуатации приобретаемых программно-аппаратных средств защиты информации |
| Основные принципы построения систем обнаружения инфокоммуникационных атак |
| Способы обнаружения и нейтрализации последствий вторжений в инфокоммуникационную систему |
| Методы проведения расследования инфокоммуникационных инцидентов |
| Основные принципы построения защищенных инфокоммуникационных систем |
| Основные принципы построения защищенных объектов и распределенных и локальных инфокоммуникационных систем, их основные уязвимости |
| Методы проведения расследования инфокоммуникационных преступлений, правонарушений и инцидентов |
| Методы выявления каналов утечки информации и организации технической разведки |
| Порядок сертификации средств защиты информации |
| Порядок лицензирования организаций, разрабатывающих средства защиты информации |
| Другие характеристики | - |

**IV. Сведения об организациях – разработчиках**

**профессионального стандарта**

**4.1.Ответственная организация-разработчик**

|  |
| --- |
| Общероссийское объединение работодателей "Российский союз промышленников и предпринимателей" |
| Исполнительный Вице-президент Кузьмин Д.В. |

**4.2.Наименования организаций-разработчиков**

|  |  |
| --- | --- |
| 1 | ЗАО «РНТ», город Москва |
| 2 | Некоммерческая организация «Ассоциация производителей оборудования связи» (НО АПОС), город Москва |
| 3 | ФГОБУ ВПО Московский технический университет связи и информатики (МТУСИ), город Москва |

1. Общероссийский классификатор занятий [↑](#endnote-ref-1)
2. Общероссийский классификатор видов экономической деятельности [↑](#endnote-ref-2)