

УТВЕРЖДЕН
приказом Министерства
труда и социальной защиты
Российской Федерации
от «» г. №

ПРОФЕССИОНАЛЬНЫЙ СТАНДАРТ

Специалист по защите информации в автоматизированных системах

843

Регистрационный номер

Содержание

| | |
|---|----|
| I. Общие сведения | 1 |
| II. Описание трудовых функций, входящих в профессиональный стандарт (функциональная карта вида профессиональной деятельности) | 3 |
| III. Характеристика обобщенных трудовых функций | 5 |
| 3.1. Обобщенная трудовая функция | 5 |
| 3.2. Обобщенная трудовая функция | 11 |
| 3.3. Обобщенная трудовая функция | 17 |
| 3.4. Обобщенная трудовая функция | 23 |
| 3.5. Обобщенная трудовая функция | 30 |
| IV. Сведения об организациях – разработчиках профессионального стандарта | 33 |

I. Общие сведения

Обеспечение безопасности информации в автоматизированных системах

(наименование вида профессиональной деятельности)

Код

Основная цель вида профессиональной деятельности:

Обеспечение безопасности информации в автоматизированных системах, функционирующих в условиях существования угроз в информационной сфере и обладающих информационно-технологическими ресурсами, подлежащими защите

Группа занятий:

| | | | |
|-------|---|-------|--|
| 1213. | Руководители в области определения политики и планирования деятельности | 1330. | Руководители служб и подразделений в сфере информационно-коммуникационных технологий |
|-------|---|-------|--|

| | | | |
|-------------------------|---|-----------|---|
| 2511. | Системные аналитики | 2519. | Разработчики и аналитики программного обеспечения и приложений, не входящие в другие группы |
| 2519. | Разработчики и аналитики программного обеспечения и приложений, не входящие в другие группы | 3359. | Среднетехнический персонал на государственной службе, не входящий в другие группы |
| 1223. | Руководители подразделений по научным исследованиям и разработкам | 2425. | Специалисты органов государственной власти |
| 2512. | Разработчики программного обеспечения | 2523. | Специалисты по компьютерным сетям |
| 3513. | Специалисты-техники по компьютерным сетям и системам | - | - |
| (код ОКЗ ¹) | (наименование) | (код ОКЗ) | (наименование) |

Отнесение к видам экономической деятельности:

| | |
|---------------------------|---|
| 62.01 | Разработка компьютерного программного обеспечения |
| 62.02.1 | Деятельность по планированию, проектированию компьютерных систем |
| 62.02.2 | Деятельность по обследованию и экспертизе компьютерных систем |
| 62.02.3 | Деятельность по обучению пользователей |
| 62.02.4 | Деятельность по подготовке компьютерных систем к эксплуатации |
| 62.02.9 | Деятельность консультативная в области компьютерных технологий прочая |
| 62.09 | Деятельность, связанная с использованием вычислительной техники и информационных технологий, прочая |
| 71.20.9 | Деятельность по техническому контролю, испытаниям и анализу прочая |
| 72.19.2 | Научные исследования и разработки в области технических наук |
| (код ОКВЭД ²) | (наименование вида экономической деятельности) |

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

| Обобщенные трудовые функции | | | Трудовые функции | | |
|-----------------------------|---|----------------------|--|--------|-----------------------------------|
| код | наименование | уровень квалификации | наименование | код | уровень (подуровень) квалификации |
| Е | Формирование требований к защите информации в автоматизированных системах | 8 | Моделирование защищенных автоматизированных систем с целью анализа их уязвимостей и эффективности средств и способов защиты информации | Е/04.8 | 8 |
| | | | Разработка архитектуры системы защиты информации автоматизированной системы | Е/03.8 | 8 |
| | | | Определение угроз безопасности информации, обрабатываемой автоматизированной системой | Е/02.8 | 8 |
| | | | Обоснование необходимости защиты информации в автоматизированной системе | Е/01.8 | 8 |
| D | Разработка систем защиты информации автоматизированных систем | 7 | Разработка программных и программно-аппаратных средств для систем защиты информации автоматизированных систем | D/04.7 | 7 |
| | | | Разработка эксплуатационной документации на системы защиты информации автоматизированных систем | D/03.7 | 7 |
| | | | Разработка проектных решений по защите информации в автоматизированных системах | D/02.7 | 7 |
| | | | Тестирование систем защиты информации автоматизированных систем | D/01.7 | 7 |
| C | Внедрение систем защиты информации автоматизированных систем | 6 | Внедрение организационных мер по защите информации в автоматизированных системах | C/04.6 | 6 |
| | | | Анализ уязвимостей внедряемой | C/03.6 | 6 |

| | | | | | |
|---|--|---|--|--------|---|
| | | | системы защиты информации | | |
| | | | Разработка организационно-распорядительных документов по защите информации в автоматизированных системах | С/02.6 | 6 |
| | | | Установка и настройка средств защиты информации в автоматизированных системах | С/01.6 | 6 |
| В | Обеспечение защиты информации в автоматизированных системах в процессе их эксплуатации | 6 | Аудит защищенности информации в автоматизированных системах | В/06.6 | 6 |
| | | | Мониторинг защищенности информации в автоматизированных системах | В/05.6 | 6 |
| | | | Обеспечение работоспособности систем защиты информации при возникновении нештатных ситуаций | В/04.6 | 6 |
| | | | Управление защитой информации в автоматизированных системах | В/03.6 | 6 |
| | | | Администрирование систем защиты информации автоматизированных систем | В/02.6 | 6 |
| | | | Диагностика систем защиты информации автоматизированных систем | В/01.6 | 6 |
| А | Обслуживание систем защиты информации в автоматизированных системах | 5 | Обеспечение защиты информации при выводе из эксплуатации автоматизированных систем | А/03.5 | 5 |
| | | | Ведение технической документации, связанной с эксплуатацией систем защиты информации автоматизированных систем | А/02.5 | 5 |
| | | | Проведение регламентных работ по эксплуатации систем защиты информации автоматизированных систем | А/01.5 | 5 |

III. Характеристика обобщенных трудовых функций

3.1. Обобщенная трудовая функция

| | | | | | |
|--------------|---|-----|---|----------------------|---|
| Наименование | Формирование требований к защите информации в автоматизированных системах | Код | Е | Уровень квалификации | 8 |
|--------------|---|-----|---|----------------------|---|

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

| | |
|--|--|
| Возможные наименования должностей, профессий | Главный специалист по защите информации |
| | Руководитель отдела систем защиты информации |
| | Заместитель руководителя департамента (отдела) исследований и разработок |
| | Руководитель департамента (отдела) исследований и разработок |

| | |
|--|---|
| Требования к образованию и обучению | Высшее образование - специалитет, или магистратура в области информационной безопасности |
| | и |
| | Дополнительное профессиональное образование - программы повышения квалификации в области информационной безопасности |
| | или |
| | Высшее образование - аспирантура (адъюнктура) |
| Требования к опыту практической работы | Не менее пяти лет в области защиты информации, в том числе на руководящих должностях не менее трех лет, для имеющих высшее образование - специалитет или магистратура в области информационной безопасности |
| | или |
| | Не менее трех лет в области защиты информации, в том числе на руководящих должностях не менее двух лет, для имеющих высшее образование - аспирантура (адъюнктура) |
| Особые условия допуска к работе | Наличие допуска к государственной тайне (при необходимости) |
| Другие характеристики | |

Дополнительные характеристики

| Наименование документа | Код | Наименование базовой группы, должности (профессии) или специальности |
|------------------------|------|--|
| ОКЗ | 1223 | Руководители подразделений по научным исследованиям и разработкам |
| | 1330 | Руководители служб и подразделений в сфере |

| | | |
|---------------------|--------|---|
| | | информационно-коммуникационных технологий |
| | 1213 | Руководители в области определения политики и планирования деятельности |
| ЕКС ³ | - | Директор (начальник) вычислительного (информационно-вычислительного) центра |
| | - | Начальник отдела информации |
| | - | Начальник отдела (лаборатории, сектора) по защите информации |
| | - | Начальник технического отдела |
| ОКПДТР ⁴ | 1213 | Руководители в области определения политики и планирования деятельности |
| ОКСО ⁵ | 090102 | Компьютерная безопасность |
| | 090103 | Организация и технология защиты информации |
| | 090104 | Комплексная защита объектов информатизации |
| | 090105 | Комплексное обеспечение информационной безопасности автоматизированных систем |
| | 090106 | Информационная безопасность телекоммуникационных систем |
| | 090107 | Противодействие техническим разведкам |
| ОКСВНК ⁶ | 090107 | Противодействие техническим разведкам |

3.1.1. Трудовая функция

| | | | | | |
|--------------|--|-----|--------|-----------------------------------|---|
| Наименование | Моделирование защищенных автоматизированных систем с целью анализа их уязвимостей и эффективности средств и способов защиты информации | Код | Е/04.8 | Уровень (подуровень) квалификации | 8 |
|--------------|--|-----|--------|-----------------------------------|---|

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

| | |
|-------------------|--|
| Трудовые действия | Разработка аналитических и компьютерных моделей автоматизированных систем и подсистем безопасности автоматизированных систем |
| | Исследование аналитических и компьютерных моделей автоматизированных систем и подсистем безопасности автоматизированных систем |
| | Разработка модели угроз безопасности информации и нарушителей в автоматизированных системах |
| | Исследование программных, архитектурно-технических и схмотехнических решений компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах |
| | Анализ информационной инфраструктуры и безопасности информации автоматизированных систем |
| | Разработка предложений по совершенствованию системы управления |

| | |
|-----------------------|--|
| | информационной безопасностью автоматизированных систем |
| Необходимые умения | Методы и технологии проектирования, моделирования, исследования систем защиты информации автоматизированных систем |
| | Основные угрозы безопасности информации и модели нарушителя в автоматизированных системах |
| | Основные меры по защите информации в автоматизированных системах |
| | Национальные, межгосударственные и международные стандарты в области защиты информации |
| | Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации |
| | Основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах |
| | Принципы построения средств защиты информации от утечки по техническим каналам |
| | Принципы построения и функционирования систем и сетей передачи информации |
| Необходимые знания | Выполнять сбор, обработку, анализ и систематизацию научно-технической информации в области защиты информации |
| | Разрабатывать и исследовать математические модели конкретных явлений и процессов для решения расчетных и исследовательских задач |
| | Применять математические модели при проектировании систем защиты информации автоматизированных систем |
| | Проектировать и реализовывать политику безопасности вычислительных сетей |
| | Анализировать основные характеристики и возможности телекоммуникационных систем по передаче информации |
| Другие характеристики | |

3.1.2. Трудовая функция

| | | | | | |
|--------------|---|-----|--------|-----------------------------------|---|
| Наименование | Разработка архитектуры системы защиты информации автоматизированной системы | Код | E/03.8 | Уровень (подуровень) квалификации | 8 |
|--------------|---|-----|--------|-----------------------------------|---|

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

| | |
|-------------------|--|
| Трудовые действия | Проведение оценки показателей качества и эффективности работы вычислительных систем, программных и программно-аппаратных средств, используемых для построения систем защиты информации |
| | Проведение технико-экономической оценки целесообразности создания системы защиты информации автоматизированной системы |
| | Определение порядка обработки информации в автоматизированной системе |
| | Формирование разделов технических заданий на создание систем защиты информации автоматизированных систем |

| | |
|-----------------------|---|
| | Разработка проектной документации на системы защиты автоматизированных систем |
| | Оформление заявки на разработку системы защиты информации автоматизированной системы |
| Необходимые умения | Основные информационные технологии, используемые в автоматизированных системах |
| | Способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации |
| | Основные средства и способы обеспечения безопасности информации, принципы построения систем защиты информации |
| | Программно-аппаратные средства обеспечения защиты информации автоматизированных систем |
| | Принципы построения средств защиты информации от утечки по техническим каналам |
| | Национальные, межгосударственные и международные стандарты в области защиты информации |
| | Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации |
| | Организационные меры по защите информации |
| | Методы тестирования и отладки, принципы организации документирования разработки, процесса сопровождения программного обеспечения |
| Необходимые знания | Определять комплекс мер для обеспечения безопасности информационной в автоматизированных системах |
| | Выявлять уязвимости информационно-технологических ресурсов автоматизированных систем |
| | Разрабатывать предложения по совершенствованию системы управления защиты информации автоматизированных систем |
| | Проводить выбор программно-аппаратных средств обеспечения безопасности информации для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности автоматизированной системы |
| | Классифицировать и оценивать угрозы безопасности информации для автоматизированной системы |
| | Определять информационную инфраструктуру и информационные ресурсы автоматизированной системы, подлежащие защите |
| | Разрабатывать модели угроз безопасности информации и нарушителей в автоматизированных системах |
| | Определять эффективность применения средств информатизации |
| Другие характеристики | |

3.1.3. Трудовая функция

| | | | | | |
|--------------|---|-----|--------|-----------------------------------|---|
| Наименование | Определение угроз безопасности информации, обрабатываемой автоматизированной системой | Код | E/02.8 | Уровень (подуровень) квалификации | 8 |
|--------------|---|-----|--------|-----------------------------------|---|

| | | | | |
|--------------------------------|----------|---------------------------|--|--|
| Происхождение трудовой функции | Оригинал | Заимствовано из оригинала | | |
|--------------------------------|----------|---------------------------|--|--|

| | |
|---|--|
| Трудовые действия | Формирование разделов технических заданий на создание систем защиты информации автоматизированных систем |
| | Разработка систем защиты информации автоматизированных систем с учетом действующих нормативно-правовых документов |
| | Определение комплекса мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для защиты информации автоматизированных систем |
| | Определение оценки возможностей внешних и внутренних нарушителей |
| | Разработка модели угроз безопасности информации автоматизированной системы |
| | Обоснование перечня сертифицированных средств защиты информации, необходимых для создания системы защиты информации автоматизированной системы |
| | Анализ требований к назначению, структуре и конфигурации создаваемой автоматизированной системы с целью выявления угроз безопасности информации |
| | Определение структурно-функциональных характеристик информационной системы в соответствии с требованиями нормативных правовых документов в области защиты информации |
| | Необходимые умения |
| Основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности в вычислительных сетях | |
| Программно-аппаратные средства обеспечения защиты информации автоматизированных систем | |
| Способы реализации угроз безопасности в автоматизированных системах | |
| Последствия от нарушения свойств безопасности информации | |
| Основные угрозы безопасности информации и модели нарушителя в автоматизированных системах | |
| Национальные, межгосударственные и международные стандарты в области защиты информации | |
| Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации | |
| Методики сертификационных испытаний технических средств защиты информации от утечки по техническим каналам на соответствие требованиям по безопасности информации | |
| Методы защиты информации от утечки по техническим каналам | |
| Необходимые знания | Производить выбор программно-аппаратных средств защиты информации для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности информации в автоматизированной системе |
| | Формировать перечень мероприятий по предотвращению угроз безопасности информации автоматизированной системы |
| | Систематизировать результаты проведенных исследований |

| | |
|-----------------------|--|
| | Анализировать возможные уязвимости информационных систем |
| | Выявлять известные уязвимости информационных систем |
| | Разрабатывать проекты нормативных документов, регламентирующих работу по защите информации в автоматизированных системах |
| Другие характеристики | |

3.1.4. Трудовая функция

| | | | | | |
|--------------|--|-----|--------|-----------------------------------|---|
| Наименование | Обоснование необходимости защиты информации в автоматизированной системе | Код | Е/01.8 | Уровень (подуровень) квалификации | 8 |
|--------------|--|-----|--------|-----------------------------------|---|

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

| | |
|--------------------|--|
| Трудовые действия | Анализ характера обрабатываемой информации и определение перечня информации, подлежащей защите |
| | Выявление степени участия персонала в обработке защищаемой информации |
| | Планирование мероприятий по обеспечению защиты информации в автоматизированной системе |
| | Определение требуемого класса (уровня) защищенности автоматизированной системы |
| | Обоснование необходимости использования криптографических средств защиты информации |
| | Разработка отчетных документов и разделов технических заданий |
| Необходимые умения | Основные информационные технологии, используемые в автоматизированных системах |
| | Основные угрозы безопасности информации и модели нарушителя в автоматизированных системах |
| | Виды информационных воздействий и критерии оценки защищенности информации в автоматизированных системах |
| | Методы защиты информации от утечки по техническим каналам |
| | Программно-аппаратные средства обеспечения защиты информации в программном обеспечении автоматизированных систем |
| | Методы, способы и средства обеспечения отказоустойчивости автоматизированных систем |
| | Принципы формирования политики информационной безопасности в автоматизированных системах |
| | Нормативные правовые акты в области защиты информации |
| | Национальные, межгосударственные и международные стандарты в области защиты информации |
| | Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации |
| | Организационные меры по защите информации |
| | Методики сертификационных испытаний технических средств защиты |

| | |
|-----------------------|--|
| | информации от утечки по техническим каналам на соответствие требованиям по безопасности информации |
| | Содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем защиты информации |
| Необходимые знания | Анализировать цели создания автоматизированных систем и задачи, решаемые автоматизированными системами |
| | Выявлять уязвимости информационно-технологических ресурсов автоматизированных систем |
| | Классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности и оценивать угрозы безопасности информации |
| | Организовывать работы по созданию, внедрению, проектированию, разработке и сопровождению защищенных автоматизированных систем |
| | Использовать рисковую методологию управления защитой информации в автоматизированной системе |
| | Определять класс защищенности автоматизированных систем и ее составных частей |
| Другие характеристики | |

3.2. Обобщенная трудовая функция

| | | | | | |
|--------------|---|-----|---|----------------------|---|
| Наименование | Разработка систем защиты информации автоматизированных систем | Код | D | Уровень квалификации | 7 |
|--------------|---|-----|---|----------------------|---|

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

| | |
|--|---|
| Возможные наименования должностей, профессий | Ведущий инженер-разработчик систем защиты информации |
| | Ведущий специалист по защите информации |
| | Руководитель проектов в области разработки систем защиты информации |
| | Руководитель отдела систем защиты информации |

| | |
|--|---|
| Требования к образованию и обучению | Высшее образование - специалитет или магистратура в области информационной безопасности |
| Требования к опыту практической работы | |
| Особые условия допуска к работе | Наличие допуска к государственной тайне (при необходимости) |
| Другие характеристики | Рекомендуется дополнительное профессиональное образование - программы повышения квалификации в области информационной |

| | |
|--|--------------|
| | безопасности |
|--|--------------|

Дополнительные характеристики

| Наименование документа | Код | Наименование базовой группы, должности (профессии) или специальности |
|------------------------|--------|---|
| ОКЗ | 2519 | Разработчики и аналитики программного обеспечения и приложений, не входящие в другие группы |
| | 2425 | Специалисты органов государственной власти |
| | 2511 | Системные аналитики |
| | 2512 | Разработчики программного обеспечения |
| | 2523 | Специалисты по компьютерным сетям |
| ЕКС | - | Инженер-программист (программист) |
| | - | Инженер-программист по технической защите информации |
| ОКПДТР | 2523 | Специалисты по компьютерным сетям |
| | 22567 | Инженер по защите информации |
| | 26579 | Специалист по защите информации |
| ОКСО | 090102 | Компьютерная безопасность |
| | 090103 | Организация и технология защиты информации |
| | 090104 | Комплексная защита объектов информатизации |
| | 090105 | Комплексное обеспечение информационной безопасности автоматизированных систем |
| | 090106 | Информационная безопасность телекоммуникационных систем |
| | 090107 | Противодействие техническим разведкам |

3.2.1. Трудовая функция

| | | | | | |
|--------------|---|-----|--------|-----------------------------------|---|
| Наименование | Разработка программных и программно-аппаратных средств для систем защиты информации автоматизированных систем | Код | D/04.7 | Уровень (подуровень) квалификации | 7 |
|--------------|---|-----|--------|-----------------------------------|---|

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

| | |
|-------------------|---|
| Трудовые действия | Разработка технической документации в соответствии с требованиями Единой системы конструкторской документации (ЕСКД) и Единой системы программной документации (ЕСПД) на компоненты автоматизированных систем |
| | Применение средств схемотехнического проектирования и современной измерительной аппаратуры |
| | Синтез структурных и функциональных схем защищенных автоматизированных систем |
| | Разработка программного обеспечения, технических средств, баз данных |

| | |
|-----------------------|--|
| | и компьютерных сетей с учетом требований по обеспечению защиты информации |
| | Разработка электронных схем с учетом требований по защите информации |
| | Оптимизация работы электронных схем с учетом требований по защите информации |
| Необходимые умения | Профессиональная и криптографическая терминология в области безопасности информации |
| | Основные информационные технологии, используемые в автоматизированных системах |
| | Средства и способы обеспечения безопасности информации, принципы построения систем защиты информации |
| | Основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах |
| | Современные технологии программирования |
| | Эталонная модель взаимодействия открытых систем, основные протоколы, последовательность и содержание этапов построения и функционирования современных локальных и глобальных компьютерных сетей |
| | Особенности защиты информации в автоматизированных системах управления технологическими процессами |
| | Принципы работы элементов и функциональных узлов электронной аппаратуры, типовые схемотехнические решения основных узлов и блоков электронной аппаратуры |
| | Принципы организации документирования разработки и процесса сопровождения программного и аппаратного обеспечения |
| | Методы тестирования и отладки программного и аппаратного обеспечения |
| | Архитектура, основные модели, последовательность и содержание этапов проектирования, физическая организация баз данных |
| | Нормативные правовые акты в области защиты информации |
| | Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации |
| Необходимые знания | Оценивать сложность алгоритмов и вычислений |
| | Разрабатывать технические задания на создание подсистем безопасности информации автоматизированных систем, проектировать такие подсистемы с учетом требований нормативных документов, ЕСКД и ЕСПД |
| | Анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах |
| | Проводить комплексное тестирование аппаратных и программных средств |
| Другие характеристики | |

3.2.2. Трудовая функция

| | | | | | |
|--------------|--|-----|--------|----------------------|---|
| Наименование | Разработка эксплуатационной документации на системы защиты | Код | D/03.7 | Уровень (подуровень) | 7 |
|--------------|--|-----|--------|----------------------|---|

информации автоматизированных систем

квалификации

Происхождение
трудоустройства

| | | | |
|----------|---------------------------|---------------|---|
| Оригинал | Заимствовано из оригинала | Код оригинала | Регистрационный номер профессионального стандарта |
|----------|---------------------------|---------------|---|

| | |
|--|---|
| Трудовые действия | Анализ технической документации информационной инфраструктуры автоматизированной системы |
| | Анализ защищенности информационной инфраструктуры автоматизированной системы |
| | Формирование требований по защите информации, включая использование математического аппарата для решения прикладных задач |
| | Документирование программного обеспечения, технических средств, баз данных и компьютерных сетей с учетом требований по обеспечению защиты информации |
| | Анализ структурных и функциональных схем защищенных автоматизированных информационных систем |
| | Обоснование критериев эффективности функционирования защищенных автоматизированных информационных систем |
| | Использование программно-аппаратных средств обеспечения безопасности информации в автоматизированных системах |
| Необходимые умения | Основные методы управления информационной безопасностью |
| | Основные понятия теории автоматов, математической логики, теории алгоритмов и теории графов |
| | Основные методы управления проектами в области информационной безопасности |
| | Национальные, межгосударственные и международные стандарты в области защиты информации |
| | Основные меры по защите информации в автоматизированных системах |
| | Особенности защиты информации в автоматизированных системах управления технологическими процессами |
| | Угрозы безопасности, информационные воздействия, критерии оценки защищенности и методы защиты информации в автоматизированных системах |
| | Методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем и систем защиты информации автоматизированных систем |
| | Программно-аппаратные средства обеспечения защиты информации в программном обеспечении автоматизированных систем |
| | Основные средства, способы и принципы построения систем защиты информации автоматизированных систем |
| | Нормативные правовые акты в области защиты информации |
| Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации | |
| Необходимые знания | Определять меры (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для защиты информации в автоматизированных системах |
| | Разрабатывать технические задания на создание подсистем |

| | |
|-----------------------|---|
| | информационной безопасности автоматизированных систем |
| | Проектировать подсистемы безопасности информации с учетом действующих нормативных и методических документов |
| | Разрабатывать модели автоматизированных систем и систем защиты информации автоматизированных систем |
| | Исследовать модели автоматизированных систем и систем защиты безопасности автоматизированных систем |
| | Анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей систем защиты информации автоматизированных систем |
| | Оценивать информационные риски в автоматизированных системах и определять информационную инфраструктуру и информационные ресурсы, подлежащие защите |
| | Проводить технико-экономическое обоснование проектных решений программно-аппаратных средств обеспечения защиты информации в автоматизированной системе с целью обеспечения требуемого уровня защищенности |
| | Исследовать эффективность проектных решений программно-аппаратных средств обеспечения защиты информации в автоматизированной системе с целью обеспечения требуемого уровня защищенности |
| | Проводить комплексное тестирование и отладку аппаратных и программных систем защиты информации |
| Другие характеристики | |

3.2.3. Трудовая функция

| | | | | | |
|--------------|---|-----|--------|-----------------------------------|---|
| Наименование | Разработка проектных решений по защите информации в автоматизированных системах | Код | D/02.7 | Уровень (подуровень) квалификации | 7 |
|--------------|---|-----|--------|-----------------------------------|---|

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

| | |
|--------------------|---|
| Трудовые действия | Разработка модели угроз безопасности информации и модели нарушителя в автоматизированных системах |
| | Разработка моделей автоматизированных систем и подсистем безопасности автоматизированных систем |
| | Разработка проектов нормативных документов, регламентирующих работу по защите информации |
| | Разработка предложений по совершенствованию системы управления безопасностью информации в автоматизированных системах |
| Необходимые умения | Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации |
| | Нормативные правовые акты и национальные стандарты по лицензированию в области обеспечения защиты государственной тайны |

| | |
|-----------------------|---|
| | и сертификации средств защиты информации |
| | Принципы построения и функционирования, примеры реализаций современных локальных и глобальных компьютерных сетей и их компонентов |
| | Особенности защиты информации в автоматизированных системах управления технологическими процессами |
| | Критерии оценки эффективности и надежности средств защиты информации программного обеспечения автоматизированных систем |
| | Принципы организации и структура систем защиты информации программного обеспечения автоматизированных систем |
| | Основные характеристики технических средств защиты информации от утечек по техническим каналам |
| | Принципы формирования политики информационной безопасности в автоматизированных системах |
| Необходимые знания | Применять действующую нормативную базу в области обеспечения защиты информации |
| | Применять нормативные документы по противодействию технической разведке |
| | Классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности |
| | Определять типы субъектов доступа и объектов доступа, являющихся объектами защиты |
| | Определять методы управления доступом, типы доступа и правила разграничения доступа к объектам доступа, подлежащим реализации в автоматизированной системе |
| | Выбирать меры защиты информации, подлежащие реализации в системе защиты информации автоматизированной системы |
| | Определять виды и типы средств защиты информации, обеспечивающих реализацию технических мер защиты информации |
| | Определять структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области защиты информации автоматизированных систем |
| Другие характеристики | |

3.2.4. Трудовая функция

| | | | | | |
|--------------|---|-----|--------|-----------------------------------|---|
| Наименование | Тестирование систем защиты информации автоматизированных систем | Код | D/01.7 | Уровень (подуровень) квалификации | 7 |
|--------------|---|-----|--------|-----------------------------------|---|

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

| | |
|-------------------|--|
| Трудовые действия | Проведение анализа структурных и функциональных схем защищенных автоматизированных информационных систем с целью выявления потенциальных уязвимостей информационной безопасности |
|-------------------|--|

| | |
|-----------------------|---|
| | автоматизированных систем |
| | Выявление уязвимости информационно-технологических ресурсов автоматизированных систем |
| | Выявление основных угроз безопасности информации в автоматизированных системах |
| | Составление методик тестирования систем защиты информации автоматизированных систем |
| | Подбор инструментальных средств тестирования систем защиты информации автоматизированных систем |
| | Составление протоколов тестирования систем защиты информации автоматизированных систем |
| Необходимые умения | Принципы построения и функционирования систем и сетей передачи информации |
| | Эталонная модель взаимодействия открытых систем |
| | Основные угрозы безопасности информации и модели нарушителя в автоматизированных системах |
| | Основные меры по защите информации в автоматизированных системах |
| | Особенности защиты информации в автоматизированных системах управления технологическими процессами |
| | Принципы построения средств защиты информации от утечки по техническим каналам |
| | Основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах |
| | Технические каналы утечки информации |
| | Технические средства контроля эффективности мер защиты информации |
| | Организация защиты информации от утечки по техническим каналам на объектах информатизации |
| | Нормативные правовые акты в области защиты информации |
| | Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации |
| | Организационные меры по защите информации |
| Необходимые знания | Анализировать основные характеристики и возможности телекоммуникационных систем по передаче информации |
| | Анализировать основные узлы и устройства современных автоматизированных систем |
| | Применять действующую нормативную базу в области обеспечения безопасности информации |
| | Контролировать безотказное функционирование технических средств защиты информации |
| | Восстанавливать (заменять) отказавшие технические средства защиты информации |
| Другие характеристики | |

3.3. Обобщенная трудовая функция

| | | | | | |
|--------------|--|-----|---|----------------------|---|
| Наименование | Внедрение систем защиты информации автоматизированных систем | Код | С | Уровень квалификации | 6 |
|--------------|--|-----|---|----------------------|---|

Происхождение обобщенной
трудовой функции

| | | | |
|----------|---------------------------|---------------|---|
| Оригинал | Заимствовано из оригинала | | |
| | | Код оригинала | Регистрационный номер профессионального стандарта |

| | |
|--|---|
| Возможные наименования должностей, профессий | Инженер по защите информации |
| | Специалист по защите информации I категории |
| | Специалист по защите информации II категории |
| | Специалист по защите информации |
| | Инженер-программист по технической защите информации I категории |
| | Инженер-программист по технической защите информации II категории |
| | Инженер-программист по технической защите информации |
| | Инженер-программист I категории |
| | Инженер-программист II категории |
| | Инженер-программист III категории |
| | Инженер-программист |

| | |
|--|--|
| Требования к образованию и обучению | Высшее образование - бакалавриат в области информационной безопасности |
| Требования к опыту практической работы | Не менее одного года в области защиты информации или не менее двух лет в области информационных технологий для должностей без категорий Для должностей с категорией - опыт работы в должности с более низкой (предшествующей) категорией не менее одного года |
| Особые условия допуска к работе | Наличие допуска к государственной тайне (при необходимости) |
| Другие характеристики | Рекомендуется дополнительное профессиональное образование - программы повышения квалификации в области информационной безопасности |

Дополнительные характеристики

| Наименование документа | Код | Наименование базовой группы, должности (профессии) или специальности |
|------------------------|------|---|
| ОКЗ | 2519 | Разработчики и аналитики программного обеспечения и приложений, не входящие в другие группы |
| | 2425 | Специалисты органов государственной власти |
| ЕКС | - | Инженер-программист (программист) |
| | - | Инженер-программист по технической защите |

| | | |
|--------|-------|---------------------------------|
| | | информации |
| ОКПДТР | 22567 | Инженер по защите информации |
| | 26579 | Специалист по защите информации |

3.3.1. Трудовая функция

| | | | | | |
|--------------|--|-----|--------|-----------------------------------|---|
| Наименование | Внедрение организационных мер по защите информации в автоматизированных системах | Код | C/04.6 | Уровень (подуровень) квалификации | 6 |
|--------------|--|-----|--------|-----------------------------------|---|

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

| | |
|--------------------|--|
| Трудовые действия | Проведение проверки полноты описания в организационно-распорядительных документах на автоматизированную систему действий персонала по реализации организационных мер защиты информации |
| | Проведение занятий с персоналом по работе с системой защиты информации автоматизированной системы, включая проведение практических занятий на макетах или в тестовой зоне |
| | Подготовка документов, определяющих правила и процедуры, реализуемые оператором для обеспечения защиты информации в информационной системе в ходе ее эксплуатации |
| | Проведение проверки готовности персонала к эксплуатации системы защиты информации автоматизированной системы |
| | Подготовка документов, определяющих правила и процедуры контроля обеспеченности уровня защищенности информации, содержащейся в информационной системе |
| | Подготовка документов, определяющих правила и процедуры выявления инцидентов, которые могут привести к сбоям или нарушению функционирования информационной системы и возникновению угроз безопасности информации |
| | Подготовка документов, определяющих правила и процедуры управления конфигурацией аттестованной информационной системой и системой защиты информации информационной системы |
| Необходимые умения | Нормативные правовые акты и национальные стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации |
| | Методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем и систем защиты автоматизированных систем |
| | Нормативные правовые акты в области защиты информации |
| | Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации |
| | Организационные меры по защите информации |
| | Методики сертификационных испытаний технических средств защиты информации от утечки по техническим каналам на соответствие |

| | |
|-----------------------|--|
| | требованиям по безопасности информации |
| | Методы, способы и средства обеспечения отказоустойчивости автоматизированных информационных систем |
| Необходимые знания | Реализовывать правила разграничения доступа персонала к объектам доступа |
| | Анализировать программные и программно-аппаратные решения при проектировании системы защиты информации с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах |
| | Обучать персонал автоматизированной системы комплексу мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения защиты информации |
| | Осуществлять планирование и организацию работы персонала автоматизированной системы с учетом требований по защите информации |
| | Конфигурировать аттестованную информационную систему и системы защиты информации информационной системы |
| Другие характеристики | |

3.3.2. Трудовая функция

| | | | | | |
|--------------|---|-----|--------|-----------------------------------|---|
| Наименование | Анализ уязвимостей внедряемой системы защиты информации | Код | C/03.6 | Уровень (подуровень) квалификации | 6 |
|--------------|---|-----|--------|-----------------------------------|---|

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

| | |
|--------------------|--|
| Трудовые действия | Выбор и обоснование критериев эффективности функционирования защищенных автоматизированных систем |
| | Проведение анализа уязвимости программных и программно-аппаратных средств системы защиты информации автоматизированной системы |
| | Проведение экспертизы состояния защищенности информации автоматизированных систем |
| | Уточнение модели угроз безопасности информации автоматизированной системы |
| | Проведение предварительных испытаний системы защиты информации автоматизированной системы |
| | Проведение анализа уязвимостей автоматизированных и информационных систем |
| Необходимые умения | Основные методы и средства криптографической защиты информации |
| | Способы защиты информации от утечки по техническим каналам |
| | Способы контроля эффективности защиты информации от утечки по техническим каналам |
| | Нормативные правовые акты в области защиты информации |
| | Руководящие и методические документы уполномоченных федеральных |

| | |
|-----------------------|---|
| | органов исполнительной власти по защите информации |
| | Организационные меры по защите информации |
| | Содержание эксплуатационной документации автоматизированной системы |
| Необходимые знания | Классифицировать и оценивать угрозы безопасности информации автоматизированной системы |
| | Разрабатывать предложения по совершенствованию системы управления защитой информации автоматизированной системы |
| | Проводить анализ доступных информационных источников с целью выявления известных уязвимостей используемых в системе защиты информации программных и программно-аппаратных средств |
| | Устранять выявленные уязвимости автоматизированной системы, приводящие к возникновению угроз безопасности информации |
| Другие характеристики | |

3.3.3. Трудовая функция

| | | | | | |
|--------------|--|-----|--------|-----------------------------------|---|
| Наименование | Разработка организационно-распорядительных документов по защите информации в автоматизированных системах | Код | C/02.6 | Уровень (подуровень) квалификации | 6 |
|--------------|--|-----|--------|-----------------------------------|---|

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

| | |
|--------------------|---|
| Трудовые действия | Определение правил и процедур управления системой защиты информации автоматизированной системы |
| | Определение правил и процедур выявления инцидентов |
| | Определение правил и процедур мониторинга обеспечения уровня защищенности информации автоматизированной системы |
| | Определение правил и процедур защиты информации при выводе автоматизированной системы из эксплуатации |
| | Определение правил и процедур реагирования на инциденты |
| Необходимые умения | Содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем защиты информации |
| | Основные угрозы безопасности информации и модели нарушителя в автоматизированных системах |
| | Основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах |
| | Принципы построения средств защиты информации от утечки по техническим каналам |
| | Нормативные правовые акты в области защиты информации |
| | Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации |
| Необходимые знания | Классифицировать и оценивать угрозы информационной безопасности |
| | Применять нормативные документы по противодействию технической |

| | |
|-----------------------|--|
| | разведке |
| | Определять параметры настройки программного обеспечения системы защиты информации автоматизированной системы |
| | Контролировать эффективность принятых мер по защите информации в автоматизированных системах |
| Другие характеристики | |

3.3.4. Трудовая функция

| | | | | | |
|--------------|---|-----|--------|-----------------------------------|---|
| Наименование | Установка и настройка средств защиты информации в автоматизированных системах | Код | C/01.6 | Уровень (подуровень) квалификации | 6 |
|--------------|---|-----|--------|-----------------------------------|---|

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

| | |
|--------------------|---|
| Трудовые действия | Входной контроль качества комплектующих изделий системы защиты информации автоматизированной системы |
| | Осуществление автономной наладки технических и программных средств системы защиты информации автоматизированной системы |
| | Проведение приемочных испытаний системы защиты информации автоматизированной системы |
| | Внесение в эксплуатационную документацию изменений, направленных на устранение недостатков, выявленных в процессе испытаний |
| Необходимые умения | Основные угрозы безопасности информации и модели нарушителя в автоматизированных системах |
| | Содержание эксплуатационной документации автоматизированной системы |
| | Типовые средства, методы и протоколы идентификации, аутентификации и авторизации |
| | Основные меры по защите информации в автоматизированных системах |
| | Нормативные правовые акты в области защиты информации |
| | Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации |
| Необходимые знания | Администрировать программные средства системы защиты информации автоматизированных систем |
| | Устранять известные уязвимости автоматизированной системы, приводящие к возникновению угроз безопасности информации |
| | Применять нормативные документы по противодействию технической разведке |
| | Применять аналитические и компьютерные модели автоматизированных систем и систем защиты информации |
| | Проводить анализ структурных и функциональных схем защищенной автоматизированной системы |
| | Определять параметры настройки программного обеспечения системы защиты информации автоматизированной системы |

| | |
|-----------------------|--|
| Другие характеристики | |
|-----------------------|--|

3.4. Обобщенная трудовая функция

| | | | | | |
|--------------|--|-----|---|----------------------|---|
| Наименование | Обеспечение защиты информации в автоматизированных системах в процессе их эксплуатации | Код | В | Уровень квалификации | 6 |
|--------------|--|-----|---|----------------------|---|

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

| | |
|--|---|
| Возможные наименования должностей, профессий | Инженер по защите информации |
| | Специалист по защите информации I категории |
| | Специалист по защите информации II категории |
| | Специалист по защите информации |
| | Инженер-программист по технической защите информации I категории |
| | Инженер-программист по технической защите информации II категории |
| | Инженер-программист по технической защите информации |
| | Инженер-программист I категории |
| | Инженер-программист II категории |
| | Инженер-программист III категории |
| | Инженер-программист |

| | |
|--|---|
| Требования к образованию и обучению | Высшее образование - бакалавриат в области информационной безопасности |
| Требования к опыту практической работы | Для должностей без категорий - опыт работы не требуется |
| | Для должностей с категорией - опыт работы в должности с более низкой (предшествующей) категорией не менее одного года |
| Особые условия допуска к работе | Наличие допуска к государственной тайне (при необходимости) |
| Другие характеристики | |

Дополнительные характеристики

| Наименование документа | Код | Наименование базовой группы, должности (профессии) или специальности |
|------------------------|-------|---|
| ОКЗ | 2519 | Разработчики и аналитики программного обеспечения и приложений, не входящие в другие группы |
| | 2425 | Специалисты органов государственной власти |
| | 2425 | Специалисты органов государственной власти |
| ЕКС | - | Инженер-программист (программист) |
| | - | Инженер-программист по технической защите информации |
| ОКПДТР | 22824 | Инженер-программист |
| | 26579 | Специалист по защите информации |
| | 22567 | Инженер по защите информации |

3.4.1. Трудовая функция

| | | | | | |
|--------------|---|-----|--------|-----------------------------------|---|
| Наименование | Аудит защищенности информации в автоматизированных системах | Код | В/06.6 | Уровень (подуровень) квалификации | 6 |
|--------------|---|-----|--------|-----------------------------------|---|

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

| | |
|--------------------|---|
| Трудовые действия | Оценка информационных рисков |
| | Обоснование и контроль результатов управленческих решений в области безопасности информации автоматизированных систем |
| | Экспертиза состояния защищенности информации автоматизированных систем |
| | Обоснование критериев эффективности функционирования защищенных автоматизированных систем |
| Необходимые умения | Основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах |
| | Способы защиты информации от утечки по техническим каналам |
| | Методы контроля эффективности защиты информации от утечки по техническим каналам |
| | Принципы построения систем защиты информации |
| | Нормативные правовые акты в области защиты информации |
| | Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации |
| | Организационные меры по защите информации |
| Необходимые знания | Классифицировать и оценивать угрозы безопасности информации для объекта информатизации |
| | Разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем |
| | Разрабатывать политики безопасности информации автоматизированных систем |

| | |
|-----------------------|--|
| | систем |
| | Применять инструментальные средства контроля защищенности информации в автоматизированных системах |
| Другие характеристики | |

3.4.2. Трудовая функция

| | | | | | |
|--------------|--|-----|--------|-----------------------------------|---|
| Наименование | Мониторинг защищенности информации в автоматизированных системах | Код | В/05.6 | Уровень (подуровень) квалификации | 6 |
|--------------|--|-----|--------|-----------------------------------|---|

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

| | |
|--------------------|--|
| Трудовые действия | Выработка рекомендаций для принятия решения о модернизации системы защиты информации автоматизированной системы |
| | Выработка рекомендаций для принятия решения о повторной аттестации автоматизированной системы или о проведении дополнительных аттестационных испытаний |
| | Выявление угроз безопасности информации в автоматизированных системах |
| | Принятие мер защиты информации при выявлении новых угроз безопасности информации |
| | Анализ недостатков в функционировании системы защиты информации автоматизированной системы |
| | Устранение недостатков в функционировании системы защиты информации автоматизированной системы |
| Необходимые умения | Содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем |
| | Основные угрозы безопасности информации и модели нарушителя в автоматизированных системах |
| | Основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах |
| | Программно-аппаратные средства обеспечения защиты информации автоматизированных систем |
| | Методы защиты информации от утечки по техническим каналам |
| | Нормативные правовые акты в области защиты информации |
| | Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации |
| | Организационные меры по защите информации |
| Необходимые знания | Классифицировать и оценивать угрозы информационной безопасности |
| | Анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах |

| | |
|-----------------------|---|
| | Применять нормативные документы по противодействию технической разведке |
| | Контролировать эффективность принятых мер по реализации политик безопасности информации автоматизированных систем |
| | Контролировать события безопасности и действия пользователей автоматизированных систем |
| | Применять технические средства контроля эффективности мер защиты информации |
| | Документировать процедуры и результаты контроля функционирования системы защиты информации автоматизированной системы |
| Другие характеристики | |

3.4.3. Трудовая функция

| | | | | | |
|--------------|---|-----|--------|-----------------------------------|---|
| Наименование | Обеспечение работоспособности систем защиты информации при возникновении нештатных ситуаций | Код | В/04.6 | Уровень (подуровень) квалификации | 6 |
|--------------|---|-----|--------|-----------------------------------|---|

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

| | |
|--------------------|--|
| Трудовые действия | Обнаружение неисправностей в работе системы защиты информации автоматизированной системы |
| | Устранение неисправностей в работе системы защиты информации автоматизированной системы |
| | Резервирование программного обеспечения, технических средств, каналов передачи данных автоматизированной системы управления на случай возникновения нештатных ситуаций |
| | Создание альтернативных мест хранения и обработки информации на случай возникновения нештатных ситуаций |
| | Восстановление после сбоев и отказов программного обеспечения автоматизированных систем |
| Необходимые умения | Методы и способы обеспечения отказоустойчивости автоматизированных систем |
| | Содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем |
| | Основные информационные технологии, используемые в автоматизированных системах |
| | Принципы построения средств защиты информации от утечки по техническим каналам |
| | Программно-аппаратные средства обеспечения защиты информации автоматизированных систем |
| | Нормативные правовые акты в области защиты информации |
| | Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации |

| | |
|-----------------------|---|
| | Организационные меры по защите информации |
| Необходимые знания | Применять типовые программные средства резервирования и восстановления информации в автоматизированных системах |
| | Применять средства обеспечения отказоустойчивости автоматизированных систем |
| | Классифицировать и оценивать угрозы информационной безопасности |
| | Применять программные средства обеспечения безопасности данных |
| | Документировать действия по устранению неисправностей в работе системы защиты информации автоматизированной системы |
| Другие характеристики | |

3.4.4. Трудовая функция

| | | | | | |
|--------------|---|-----|--------|-----------------------------------|---|
| Наименование | Управление защитой информации в автоматизированных системах | Код | В/03.6 | Уровень (подуровень) квалификации | 6 |
|--------------|---|-----|--------|-----------------------------------|---|

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

| | |
|--------------------|---|
| Трудовые действия | Анализ воздействия изменений конфигурации автоматизированной системы на ее защищенность |
| | Составление комплекса правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе |
| | Оценка последствий от реализации угроз безопасности информации в автоматизированной системе |
| | Анализ изменения угроз безопасности информации автоматизированной системы, возникающих в ходе ее эксплуатации |
| Необходимые умения | Основные методы управления защитой информации |
| | Основные угрозы безопасности информации и модели нарушителя в автоматизированных системах |
| | Методы защиты информации от утечки по техническим каналам |
| | Нормативные правовые акты в области защиты информации |
| | Национальные, межгосударственные и международные стандарты в области защиты информации |
| | Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации |
| Необходимые знания | Оценивать информационные риски в автоматизированных системах |
| | Классифицировать и оценивать угрозы безопасности информации |
| | Определять подлежащие защите информационные ресурсы автоматизированных систем |
| | Применять нормативные документы по противодействию технической разведке |
| | Разрабатывать предложения по совершенствованию системы управления защиты информации автоматизированных систем |
| | Конфигурировать параметры системы защиты информации |

| | |
|-----------------------|---|
| | автоматизированных систем |
| | Применять технические средства контроля эффективности мер защиты информации |
| Другие характеристики | |

3.4.5. Трудовая функция

| | | | | | |
|--------------|--|-----|--------|-----------------------------------|---|
| Наименование | Администрирование систем защиты информации автоматизированных систем | Код | В/02.6 | Уровень (подуровень) квалификации | 6 |
|--------------|--|-----|--------|-----------------------------------|---|

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

| | |
|--------------------|--|
| Трудовые действия | Установка обновлений программного обеспечения автоматизированной системы |
| | Обеспечение безопасности информации с учетом требования эффективного функционирования автоматизированной системы |
| | Управление полномочиями пользователей автоматизированной системы |
| | Информирование пользователей о правилах эксплуатации автоматизированной системы с учетом требований по защите информации |
| | Проведение занятий с персоналом по работе с системой защиты информации автоматизированной системы, включая проведение практических занятий с персоналом на макетах или в тестовой зоне |
| | Внесение изменений в эксплуатационную документацию и организационно-распорядительные документы по системе защиты информации автоматизированной системы |
| Необходимые умения | Принципы формирования политики информационной безопасности в автоматизированных системах |
| | Программно-аппаратные средства защиты информации автоматизированных систем |
| | Основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах |
| | Методы контроля эффективности защиты информации от утечки по техническим каналам |
| | Критерии оценки эффективности и надежности средств защиты программного обеспечения автоматизированных систем |
| | Технические средства контроля эффективности мер защиты информации |
| | Принципы организации и структура систем защиты программного обеспечения автоматизированных систем |
| | Содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем безопасности автоматизированных систем |
| | Основные меры по защите информации в автоматизированных системах |
| Необходимые знания | Создавать, удалять и изменять учетные записи пользователей |

| | |
|-----------------------|--|
| | автоматизированной системы |
| | Планировать политику безопасности программных компонентов автоматизированных систем |
| | Устанавливать и настраивать операционные системы, системы управления базами данных, компьютерные сети и программные системы с учетом требований по обеспечению защиты информации |
| | Использовать криптографические методы и средства защиты информации в автоматизированных системах |
| | Регистрировать события, связанные с защитой информации в автоматизированных системах |
| | Анализировать события, связанные с защитой информации в автоматизированных системах |
| Другие характеристики | |

3.4.6. Трудовая функция

| | | | | | |
|--------------|--|-----|--------|-----------------------------------|---|
| Наименование | Диагностика систем защиты информации автоматизированных систем | Код | V/01.6 | Уровень (подуровень) квалификации | 6 |
|--------------|--|-----|--------|-----------------------------------|---|

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

| | |
|---|---|
| Трудовые действия | Обнаружение инцидентов в процессе эксплуатации автоматизированной системы |
| | Идентификация инцидентов в процессе эксплуатации автоматизированной системы |
| | Оценка защищенности автоматизированных систем с помощью типовых программных средств |
| | Устранение инцидентов, возникших в процессе эксплуатации автоматизированной системы |
| | Расчет показателей эффективности защиты информации, обрабатываемой в автоматизированных системах |
| | Инструментальный контроль показателей эффективности защиты информации, обрабатываемой в автоматизированных системах |
| Необходимые умения | Нормативные правовые акты в области защиты информации |
| | Национальные, межгосударственные и международные стандарты в области защиты информации |
| | Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации |
| | Организационные меры по защите информации |
| | Принципы построения средств защиты информации от утечки по техническим каналам |
| | Критерии оценки защищенности автоматизированной системы |
| | Технические средства контроля эффективности мер защиты информации |
| Регламент информирования персонала автоматизированной системы о | |

| | |
|-----------------------|---|
| | выявленных инцидентах |
| | Регламент учета выявленных инцидентов |
| | Регламент устранения инцидентов |
| | Основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения защиты информации в автоматизированных системах |
| Необходимые знания | Определять источники и причины возникновения инцидентов |
| | Оценивать последствия выявленных инцидентов |
| | Обнаруживать нарушения правил разграничения доступа |
| | Устранять нарушения правил разграничения доступа |
| | Осуществлять контроль обеспечения уровня защищенности в автоматизированных системах |
| | Использовать криптографические методы и средства защиты информации в автоматизированных системах |
| Другие характеристики | |

3.5. Обобщенная трудовая функция

| | | | | | |
|--------------|---|-----|---|----------------------|---|
| Наименование | Обслуживание систем защиты информации в автоматизированных системах | Код | А | Уровень квалификации | 5 |
|--------------|---|-----|---|----------------------|---|

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

| | |
|--|--|
| Возможные наименования должностей, профессий | Техник по защите информации I категории |
| | Техник по защите информации II категории |
| | Техник по защите информации |

| | |
|--|--|
| Требования к образованию и обучению | Среднее профессиональное образование - программы подготовки специалистов среднего звена по профилю деятельности |
| Требования к опыту практической работы | Для должностей без категорий - опыт работы не требуется |
| | Для должностей с категорией - опыт работы в должности с более низкой (предшествующей) категорией не менее одного года |
| Особые условия допуска к работе | |
| Другие характеристики | Рекомендуется дополнительное профессиональное образование - программы повышения квалификации в области информационной безопасности |

Дополнительные характеристики

| Наименование документа | Код | Наименование базовой группы, должности (профессии) или специальности |
|------------------------|--------|---|
| ОКЗ | 22567 | Инженер по защите информации |
| | 3513 | Специалисты-техники по компьютерным сетям и системам |
| | 3359 | Среднетехнический персонал на государственной службе, не входящий в другие группы |
| ЕКС | - | Техник по защите информации |
| ОКПДТР | 27032 | Техник по защите информации |
| ОКСО | 090108 | Информационная безопасность |

3.5.1. Трудовая функция

| | | | | | |
|--------------|--|-----|--------|-----------------------------------|---|
| Наименование | Обеспечение защиты информации при выводе из эксплуатации автоматизированных систем | Код | A/03.5 | Уровень (подуровень) квалификации | 5 |
|--------------|--|-----|--------|-----------------------------------|---|

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

| | |
|-----------------------|---|
| Трудовые действия | Уничтожение информации, обрабатываемой автоматизированной системой |
| | Уничтожение машинных носителей информации, обрабатываемой автоматизированной системой |
| | Архивирование информации, обрабатываемой автоматизированной системой |
| Необходимые умения | Процедуры по архивированию информации, обрабатываемой автоматизированной системой |
| | Назначение и принципы работы основных узлов современных технических средств информатизации |
| | Организация ремонтного обслуживания компонентов автоматизированной системы |
| | Регламент автоматизированной системы по уничтожению информации и машинных носителей информации |
| | Нормативные правовые акты в области защиты информации |
| | Основные методические и руководящие документы уполномоченных федеральных органов исполнительной власти по защите информации |
| Необходимые знания | Использовать программные средства для архивирования информации |
| | Использовать программные и программно-аппаратные средства для уничтожения информации и носителей информации |
| | Использовать типовые криптографические средства защиты информации, в том числе электронную подпись |
| Другие характеристики | |

3.5.2. Трудовая функция

| | | | | | |
|--------------|--|-----|--------|-----------------------------------|---|
| Наименование | Ведение технической документации, связанной с эксплуатацией систем защиты информации автоматизированных систем | Код | A/02.5 | Уровень (подуровень) квалификации | 5 |
|--------------|--|-----|--------|-----------------------------------|---|

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

| | |
|-----------------------|--|
| Трудовые действия | Ведение документов учета, обработки, хранения и передачи информации, составляющей тайну |
| | Информирование персонала об угрозах безопасности информации |
| | Информирование персонала о правилах эксплуатации системы защиты автоматизированной системы и отдельных средств защиты информации |
| | Ведение протоколов и журналов учета при изменении конфигурации систем защиты информации автоматизированных систем |
| | Ведение протоколов и журналов учета при осуществлении мониторинга систем защиты информации автоматизированных систем |
| | Ведение протоколов и журналов учета при осуществлении аудита систем защиты информации автоматизированных систем |
| Необходимые умения | Нормативные правовые акты в области защиты информации |
| | Основные методические и руководящие документы уполномоченных федеральных органов исполнительной власти по защите информации |
| | Эксплуатационная и проектная документация на автоматизированную систему |
| | Основные методы организации и проведения технического обслуживания технических средств информатизации |
| | Организационные меры по защите информации |
| Необходимые знания | Оформлять документацию по регламентации мероприятий и оказанию услуг в области защиты информации |
| | Оформлять техническую документацию в соответствии с нормативными правовыми актами в области защиты информации |
| Другие характеристики | |

3.5.3. Трудовая функция

| | | | | | |
|--------------|--|-----|--------|-----------------------------------|---|
| Наименование | Проведение регламентных работ по эксплуатации систем защиты информации автоматизированных систем | Код | A/01.5 | Уровень (подуровень) квалификации | 5 |
|--------------|--|-----|--------|-----------------------------------|---|

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

| | |
|-----------------------|--|
| Трудовые действия | Проверка работоспособности системы защиты информации автоматизированной системы |
| | Контроль соответствия конфигурации системы защиты информации автоматизированной системы ее эксплуатационной документации |
| | Контроль стабильности характеристик системы защиты информации автоматизированной системы |
| Необходимые умения | Типовые средства и методы защиты информации в локальных и глобальных вычислительных сетях |
| | Базовая конфигурация системы защиты информации автоматизированной системы |
| | Особенности применения программных и программно-аппаратных средств защиты информации в автоматизированных системах |
| | Типовые средства, методы и протоколы идентификации, аутентификации и авторизации |
| | Нормативные правовые акты в области защиты информации |
| | Организационные меры по защите информации |
| Необходимые знания | Конфигурировать параметры системы защиты информации автоматизированной системы в соответствии с ее эксплуатационной документацией |
| | Обнаруживать и устранять неисправности системы защиты информации автоматизированной системы согласно эксплуатационной документации |
| | Производить монтаж и диагностику компьютерных сетей |
| | Использовать типовые криптографические средства защиты информации, в том числе средства электронной подписи |
| Другие характеристики | |

IV. Сведения об организациях – разработчиках профессионального стандарта

4.1. Ответственная организация-разработчик

| | |
|--|-------------------------------------|
| ЗАО «Ассоциация специалистов информационных систем», город Санкт-Петербург | |
| Генеральный директор | Солодянников Александр Владимирович |

4.2. Наименования организаций-разработчиков

| | |
|---|--|
| 1 | Межрегиональная общественная организация «Ассоциация защиты информации», город Москва |
| 2 | ФГКОУ ВО «Академия Федеральной службы безопасности Российской Федерации», город Москва |
| 3 | ФГУП «Научно-технический центр «Атлас», город Москва |

¹ Общероссийский классификатор занятий.

² Общероссийский классификатор видов экономической деятельности.

³ Единый квалификационный справочник должностей руководителей, специалистов и других служащих.

⁴ Общероссийский классификатор профессий рабочих, должностей служащих и тарифных разрядов.

⁵ Общероссийский классификатор специальностей по образованию.

⁶ Общероссийский классификатор специальностей высшей научной квалификации.