Документ предоставлен [КонсультантПлюс](http://www.consultant.ru)

Зарегистрировано в Минюсте России 28 ноября 2016 г. N 44464

МИНИСТЕРСТВО ТРУДА И СОЦИАЛЬНОЙ ЗАЩИТЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ

от 1 ноября 2016 г. N 598н

ОБ УТВЕРЖДЕНИИ ПРОФЕССИОНАЛЬНОГО СТАНДАРТА

"СПЕЦИАЛИСТ ПО БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ И СЕТЕЙ"

В соответствии с [пунктом 16](consultantplus://offline/ref=7F61548AB8AC225E8BEB5C597F5382E27D7D890E0BD3A1402C970A2103594481EA3C21W9jFL) Правил разработки и утверждения профессиональных стандартов, утвержденных постановлением Правительства Российской Федерации от 22 января 2013 г. N 23 (Собрание законодательства Российской Федерации, 2013, N 4, ст. 293; 2014, N 39, ст. 5266; 2016, N 21, ст. 3002), приказываю:

Утвердить прилагаемый профессиональный [стандарт](#P28) "Специалист по безопасности компьютерных систем и сетей".

Министр

М.А.ТОПИЛИН

Утвержден

приказом Министерства труда

и социальной защиты

Российской Федерации

от 1 ноября 2016 г. N 598н

ПРОФЕССИОНАЛЬНЫЙ СТАНДАРТ

СПЕЦИАЛИСТ ПО БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ И СЕТЕЙ

|  |  |
| --- | --- |
|  | 842 |
|  | Регистрационный номер |

I. Общие сведения

|  |  |  |
| --- | --- | --- |
| Защита информации в компьютерных системах и сетях |  | 06.032 |
| (наименование вида профессиональной деятельности) |  | Код |

Основная цель вида профессиональной деятельности:

|  |
| --- |
| Обеспечение безопасности информации в компьютерных системах и сетях в условиях существования угроз их информационной безопасности |

Группа занятий:

|  |  |  |  |
| --- | --- | --- | --- |
| [1223](consultantplus://offline/ref=7F61548AB8AC225E8BEB5C597F5382E27D73890E09D7A1402C970A2103594481EA3C219728F4A84EWCj6L) | Руководители подразделений по научным исследованиям и разработкам | [1330](consultantplus://offline/ref=7F61548AB8AC225E8BEB5C597F5382E27D73890E09D7A1402C970A2103594481EA3C219728F4A841WCjCL) | Руководители служб и подразделений в сфере информационно-коммуникационных технологий |
| [2425](consultantplus://offline/ref=7F61548AB8AC225E8BEB5C597F5382E27D73890E09D7A1402C970A2103594481EA3C219728F4AC49WCj6L) | Специалисты органов государственной власти | [2511](consultantplus://offline/ref=7F61548AB8AC225E8BEB5C597F5382E27D73890E09D7A1402C970A2103594481EA3C219728F4AC4BWCj2L) | Системные аналитики |
| [2519](consultantplus://offline/ref=7F61548AB8AC225E8BEB5C597F5382E27D73890E09D7A1402C970A2103594481EA3C219728F4AC4CWCjCL) | Разработчики и аналитики программного обеспечения и приложений, не входящие в другие группы | [2522](consultantplus://offline/ref=7F61548AB8AC225E8BEB5C597F5382E27D73890E09D7A1402C970A2103594481EA3C219728F4AC4DWCj3L) | Системные администраторы |
| [2523](consultantplus://offline/ref=7F61548AB8AC225E8BEB5C597F5382E27D73890E09D7A1402C970A2103594481EA3C219728F4AC4EWCj4L) | Специалисты по компьютерным сетям | [2529](consultantplus://offline/ref=7F61548AB8AC225E8BEB5C597F5382E27D73890E09D7A1402C970A2103594481EA3C219728F4AC4EWCj7L) | Специалисты по базам данных и сетям, не входящие в другие группы |
| [3359](consultantplus://offline/ref=7F61548AB8AC225E8BEB5C597F5382E27D73890E09D7A1402C970A2103594481EA3C219728F4A048WCj5L) | Среднетехнический персонал на государственной службе, не входящий в другие группы | [3511](consultantplus://offline/ref=7F61548AB8AC225E8BEB5C597F5382E27D73890E09D7A1402C970A2103594481EA3C219728F4A04DWCj1L) | Специалисты-техники по эксплуатации ИКТ |
| [3513](consultantplus://offline/ref=7F61548AB8AC225E8BEB5C597F5382E27D73890E09D7A1402C970A2103594481EA3C219728F4A04EWCj5L) | Специалисты-техники по компьютерным сетям и системам | - | - |
| (код [ОКЗ](consultantplus://offline/ref=7F61548AB8AC225E8BEB5C597F5382E27D73890E09D7A1402C970A2103W5j9L) [<1>](#P1316)) | (наименование) | (код [ОКЗ](consultantplus://offline/ref=7F61548AB8AC225E8BEB5C597F5382E27D73890E09D7A1402C970A2103W5j9L)) | (наименование) |

Отнесение к видам экономической деятельности:

|  |  |
| --- | --- |
| [62.01](consultantplus://offline/ref=7F61548AB8AC225E8BEB5C597F5382E27E74890109D0A1402C970A2103594481EA3C219728F0AD41WCjCL) | Разработка компьютерного программного обеспечения |
| [62.02.1](consultantplus://offline/ref=7F61548AB8AC225E8BEB5C597F5382E27E74890109D0A1402C970A2103594481EA3C219728F0AC48WCj6L) | Деятельность по планированию, проектированию компьютерных систем |
| [62.02.2](consultantplus://offline/ref=7F61548AB8AC225E8BEB5C597F5382E27E74890109D0A1402C970A2103594481EA3C219728F0AC48WCj0L) | Деятельность по обследованию и экспертизе компьютерных систем |
| [62.09](consultantplus://offline/ref=7F61548AB8AC225E8BEB5C597F5382E27E74890109D0A1402C970A2103594481EA3C219728F0AC4AWCj0L) | Деятельность, связанная с использованием вычислительной техники и информационных технологий, прочая |
| КонсультантПлюс: примечание.  Изменением [8/2016](consultantplus://offline/ref=7F61548AB8AC225E8BEB5C597F5382E27E7489030BD7A1402C970A2103594481EA3C219728F4A948WCjDL) ОКВЭД2 код 72.19.2 аннулирован с [1 ноября 2016 года](consultantplus://offline/ref=7F61548AB8AC225E8BEB5C597F5382E27E7489030BD7A1402C970A2103594481EA3C219728F4A948WCj6L). | |
| [72.19.2](consultantplus://offline/ref=7F61548AB8AC225E8BEB5C597F5382E27E74890109D0A1402C970A2103594481EA3C219728F1A04CWCj3L) | Научные исследования и разработки в области технических наук |
| (код [ОКВЭД](consultantplus://offline/ref=7F61548AB8AC225E8BEB5C597F5382E27E74890109D0A1402C970A2103W5j9L) [<2>](#P1317)) | (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 |
| A | Обслуживание средств защиты информации в компьютерных системах и сетях | 5 | Обслуживание программно-аппаратных средств защиты информации в операционных системах | A/01.5 | 5 |
| Обслуживание программно-аппаратных средств защиты информации в компьютерных сетях | A/02.5 | 5 |
| Обслуживание средств защиты информации прикладного и системного программного обеспечения | A/03.5 | 5 |
| B | Администрирование средств защиты информации в компьютерных системах и сетях | 6 | Администрирование подсистем защиты информации в операционных системах | B/01.6 | 6 |
| Администрирование программно-аппаратных средств защиты информации в компьютерных сетях | B/02.6 | 6 |
| Администрирование средств защиты информации прикладного и системного программного обеспечения | B/03.6 | 6 |
| C | Оценивание уровня безопасности компьютерных систем и сетей | 7 | Проведение контрольных проверок работоспособности и эффективности применяемых программно-аппаратных средств защиты информации | C/01.7 | 7 |
| Разработка требований по защите, формирование политик безопасности компьютерных систем и сетей | C/02.7 | 7 |
| Проведение анализа безопасности компьютерных систем | C/03.7 | 7 |
| Проведение сертификации программно-аппаратных средств защиты информации и анализ результатов | C/04.7 | 7 |
| Проведение инструментального мониторинга защищенности компьютерных систем и сетей | C/05.7 | 7 |
| Проведение экспертизы при расследовании компьютерных преступлений, правонарушений и инцидентов | C/06.7 | 7 |
| D | Разработка программно-аппаратных средств защиты информации компьютерных систем и сетей | 8 | Разработка требований к программно-аппаратным средствам защиты информации компьютерных систем и сетей | D/01.8 | 8 |
| Проектирование программно-аппаратных средств защиты информации компьютерных систем и сетей | D/02.8 | 8 |
| Разработка и тестирование средств защиты информации компьютерных систем и сетей | D/03.8 | 8 |
| Сопровождение разработки средств защиты информации компьютерных систем и сетей | D/04.8 | 8 |

III. Характеристика обобщенных трудовых функций

3.1. Обобщенная трудовая функция

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Обслуживание средств защиты информации в компьютерных системах и сетях | Код | A | Уровень квалификации | 5 |

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

|  |  |
| --- | --- |
| Возможные наименования должностей, профессий | Техник по безопасности компьютерных систем и сетей  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](consultantplus://offline/ref=7F61548AB8AC225E8BEB5C597F5382E27D73890E09D7A1402C970A2103W5j9L) | [3511](consultantplus://offline/ref=7F61548AB8AC225E8BEB5C597F5382E27D73890E09D7A1402C970A2103594481EA3C219728F4A04DWCj1L) | Специалисты-техники по эксплуатации ИКТ |
| [3513](consultantplus://offline/ref=7F61548AB8AC225E8BEB5C597F5382E27D73890E09D7A1402C970A2103594481EA3C219728F4A04EWCj5L) | Специалисты-техники по компьютерным сетям и системам |
| [3359](consultantplus://offline/ref=7F61548AB8AC225E8BEB5C597F5382E27D73890E09D7A1402C970A2103594481EA3C219728F4A048WCj5L) | Среднетехнический персонал на государственной службе, не входящий в другие группы |
| ЕКС [<3>](#P1318) | - | Техник по защите информации |
| [ОКПДТР](consultantplus://offline/ref=7F61548AB8AC225E8BEB5C597F5382E27D778B0E05D2A1402C970A2103594481EA3C219728F4A949WCj4L) [<4>](#P1319) | [27032](consultantplus://offline/ref=7F61548AB8AC225E8BEB5C597F5382E27D778B0E05D2A1402C970A2103594481EA3C219728F3AA48WCjDL) | Техник по защите информации |
| [ОКСО](consultantplus://offline/ref=7F61548AB8AC225E8BEB5C597F5382E27D758B0F08D4A1402C970A2103W5j9L) [<5>](#P1320) | [090108](consultantplus://offline/ref=7F61548AB8AC225E8BEB5C597F5382E27D758B0F08D4A1402C970A2103594481EA3C219728F5A94AWCj3L) | Информационная безопасность |

3.1.1. Трудовая функция

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Обслуживание программно-аппаратных средств защиты информации в операционных системах | Код | A/01.5 | Уровень (подуровень) квалификации | 5 |

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

|  |  |
| --- | --- |
| Трудовые действия | Ввод в эксплуатацию программно-аппаратных средств защиты информации в операционных системах |
| Установка программно-аппаратных средств защиты информации |
| Настройка программно-аппаратных средств защиты информации, в том числе средств антивирусной защиты, в операционных системах по заданным шаблонам |
| Установка средств антивирусной защиты в соответствии с действующими требованиями |
| Инструктаж пользователей по порядку безопасной работы в операционных системах |
| Оформление эксплуатационной документации на программно-аппаратные средства защиты информации в операционных системах |
| Восстановление работоспособности программно-аппаратных средств защиты информации в операционных системах согласно технической документации |
| Проверка корректности работы программно-аппаратных средств защиты информации при их взаимодействии с техническими средствами и программным обеспечением |
| Необходимые умения | Настраивать компоненты подсистем защиты информации операционных систем |
| Управлять учетными записями пользователей, в том числе генерацией, сменой и восстановлением паролей |
| Применять программно-аппаратные средства защиты информации в операционных системах |
| Применять антивирусные средства защиты информации в операционных системах |
| Работать в операционных системах с соблюдением действующих требований по защите информации |
| Проводить мониторинг, анализ и сравнение эффективности программно-аппаратных средств защиты информации в операционных системах |
| Устанавливать обновления программного обеспечения, включая программное обеспечение средств защиты информации |
| Выполнять резервное копирование и аварийное восстановление работоспособности средств защиты информации |
| Контролировать целостность подсистем защиты информации операционных систем |
| Устранять неисправности подсистем защиты информации операционных систем и программно-аппаратных средств защиты информации согласно технической документации |
| Оформлять эксплуатационную документацию программно-аппаратных средств защиты информации |
| Необходимые знания | Архитектура и пользовательские интерфейсы операционных систем |
| Порядок обеспечения безопасности информации при эксплуатации операционных систем |
| Источники угроз информационной безопасности и меры по их предотвращению |
| Сущность и содержание понятия информационной безопасности, характеристики ее составляющих |
| Типовые средства защиты информации в операционных системах |
| Программно-аппаратные средства и методы защиты информации |
| Порядок эксплуатации средств антивирусной защиты в операционных системах |
| Формы и методы инструктажа пользователей по порядку работы в операционных системах |
| Общие принципы функционирования программно-аппаратных средств криптографической защиты информации |
| Порядок оформления эксплуатационной документации |
| Нормативные правовые акты в области защиты информации |
| Основные руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации |
| Организационные меры по защите информации |
| Другие характеристики | - |

3.1.2. Трудовая функция

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Обслуживание программно-аппаратных средств защиты информации в компьютерных сетях | Код | A/02.5 | Уровень (подуровень) квалификации | 5 |

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

|  |  |
| --- | --- |
| Трудовые действия | Ввод в эксплуатацию программно-аппаратных средств защиты информации в компьютерных сетях |
| Установка программно-аппаратных средств защиты информации в компьютерных сетях |
| Установка средств межсетевого экранирования в соответствии с действующими требованиями по защите информации |
| Настройка программно-аппаратных средств защиты информации в компьютерных сетях по заданным шаблонам |
| Устранение неисправностей программно-аппаратных средств защиты информации в компьютерных сетях согласно технической документации |
| Инструктаж пользователей по порядку безопасной работы в компьютерных сетях |
| Оформление эксплуатационной документации на программно-аппаратные средства защиты информации в компьютерных сетях |
| Необходимые умения | Применять программно-аппаратные средства защиты информации в компьютерных сетях |
| Устанавливать межсетевые экраны в компьютерных сетях |
| Конфигурировать межсетевые экраны в соответствии с заданными правилами |
| Контролировать корректность настройки межсетевых экранов в соответствии с заданными правилами |
| Работать в компьютерных сетях с соблюдением действующих требований по защите информации |
| Проводить мониторинг, анализ и сравнение эффективности программно-аппаратных средств защиты информации в компьютерных сетях |
| Устанавливать обновления программного обеспечения, включая программное обеспечение средств защиты информации |
| Формулировать предложения по применению программно-аппаратных средств защиты информации в компьютерных сетях |
| Необходимые знания | Топологии и протоколы сетевого взаимодействия, применяемые в эксплуатируемых компьютерных сетях |
| Состав и основные характеристики оборудования, применяемого при построении компьютерных сетей |
| Типовые методы и протоколы идентификации, аутентификации и авторизации в компьютерных сетях |
| Типовые сетевые атаки и способы защиты от них |
| Сущность и содержание понятия информационной безопасности, характеристики ее составляющих |
| Основные источники угроз информационной безопасности и меры по их предотвращению |
| Программно-аппаратные средства и методы защиты информации |
| Основные методы организации и проведения технического обслуживания коммутационного оборудования компьютерных сетей |
| Порядок оформления эксплуатационной документации |
| Общие принципы функционирования средств криптографической защиты информации в компьютерных сетях |
| Порядок обеспечения безопасности информации при эксплуатации компьютерных сетей |
| Формы и методы инструктажа пользователей по порядку работы в компьютерных сетях |
| Нормативные правовые акты в области защиты информации |
| Основные руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации |
| Организационные меры по защите информации |
| Другие характеристики | - |

3.1.3. Трудовая функция

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Обслуживание средств защиты информации прикладного и системного программного обеспечения | Код | A/03.5 | Уровень (подуровень) квалификации | 5 |

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

|  |  |
| --- | --- |
| Трудовые действия | Установка программного обеспечения |
| Настройка программного обеспечения с соблюдением требований по защите информации |
| Настройка средств антивирусной защиты для корректной работы программного обеспечения по заданным шаблонам |
| Инструктаж пользователей о соблюдении требований по защите информации при работе с программным обеспечением |
| Настройка встроенных средств защиты информации программного обеспечения по заданным шаблонам |
| Проверка функционирования встроенных средств защиты информации программного обеспечения |
| Своевременное обнаружение признаков наличия вредоносного программного обеспечения |
| Необходимые умения | Устанавливать программное обеспечение в соответствии с технической документацией |
| Выполнять настройку параметров работы программного обеспечения, включая системы управления базами данных и средства электронного документооборота |
| Работать с программным обеспечением с соблюдением действующих требований по защите информации |
| Устанавливать обновления программного обеспечения, включая программное обеспечение средств защиты информации |
| Необходимые знания | Порядок настройки программного обеспечения, систем управления базами данных и средств электронного документооборота |
| Общие принципы функционирования вредоносного программного обеспечения |
| Принципы функционирования средств антивирусной защиты |
| Сущность и содержание понятия информационной безопасности, характеристики ее составляющих |
| Источники угроз информационной безопасности и меры по их предотвращению |
| Особенности источников угроз информационной безопасности, связанных с эксплуатацией программного обеспечения |
| Признаки наличия вредоносного программного обеспечения |
| Типовые уязвимости программного обеспечения и методы их эксплуатации |
| Общие принципы функционирования средств защиты информации программного обеспечения, в том числе, средств криптографической защиты информации |
| Порядок эксплуатации средств антивирусной защиты |
| Порядок обеспечения безопасности информации при эксплуатации программного обеспечения |
| Нормативные правовые акты в области защиты информации |
| Основные руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации |
| Организационные меры по защите информации |
| Другие характеристики | - |

3.2. Обобщенная трудовая функция

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Администрирование средств защиты информации в компьютерных системах и сетях | Код | B | Уровень квалификации | 6 |

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

|  |  |
| --- | --- |
| Возможные наименования должностей, профессий | Администратор безопасности компьютерных систем и сетей  Администратор по обеспечению безопасности 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 [<6>](#P1321) (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](consultantplus://offline/ref=7F61548AB8AC225E8BEB5C597F5382E27D73890E09D7A1402C970A2103W5j9L) | [2425](consultantplus://offline/ref=7F61548AB8AC225E8BEB5C597F5382E27D73890E09D7A1402C970A2103594481EA3C219728F4AC49WCj6L) | Специалисты органов государственной власти |
| [2522](consultantplus://offline/ref=7F61548AB8AC225E8BEB5C597F5382E27D73890E09D7A1402C970A2103594481EA3C219728F4AC4DWCj3L) | Системные администраторы |
| [2523](consultantplus://offline/ref=7F61548AB8AC225E8BEB5C597F5382E27D73890E09D7A1402C970A2103594481EA3C219728F4AC4EWCj4L) | Специалисты по компьютерным сетям |
| [2529](consultantplus://offline/ref=7F61548AB8AC225E8BEB5C597F5382E27D73890E09D7A1402C970A2103594481EA3C219728F4AC4EWCj7L) | Специалисты по базам данных и сетям, не входящие в другие группы |
| ЕКС | - | Инженер-программист |
| - | Инженер-программист по технической защите информации |
| - | Администратор по обеспечению безопасности информации |
| [ОКПДТР](consultantplus://offline/ref=7F61548AB8AC225E8BEB5C597F5382E27D778B0E05D2A1402C970A2103594481EA3C219728F4A949WCj4L) | [26579](consultantplus://offline/ref=7F61548AB8AC225E8BEB5C597F5382E27D778B0E05D2A1402C970A2103594481EA3C219728F3AB48WCj0L) | Специалист по защите информации |
| [40067](consultantplus://offline/ref=7F61548AB8AC225E8BEB5C597F5382E27D778B0E05D2A1402C970A2103594481EA3C219728FCAB4DWCj5L) | Администратор вычислительной сети |
| [22824](consultantplus://offline/ref=7F61548AB8AC225E8BEB5C597F5382E27D778B0E05D2A1402C970A2103594481EA3C219728F2AB48WCj0L) | Инженер-программист |
| [40070](consultantplus://offline/ref=7F61548AB8AC225E8BEB5C597F5382E27D778B0E05D2A1402C970A2103594481EA3C219728FCAB4DWCj7L) | Администратор информационной безопасности вычислительной сети |

3.2.1. Трудовая функция

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Администрирование подсистем защиты информации в операционных системах | 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 применяемых программно-аппаратных средств защиты информации в операционных системах |
| Разработка порядка применения программно-аппаратных средств защиты информации в операционных системах |
| Формирование шаблонов установки программно-аппаратных средств защиты информации в операционных системах |
| Установка программно-аппаратных средств защиты информации в операционных системах, включая средства криптографической защиты информации |
| Конфигурирование программно-аппаратных средств защиты информации в операционных системах |
| Контроль корректности функционирования программно-аппаратных средств защиты информации в операционных системах |
| Управление антивирусной защитой операционных систем в соответствии с действующими требованиями |
| Необходимые умения | Формулировать политики безопасности операционных систем |
| Настраивать политики безопасности операционных систем |
| Оценивать угрозы безопасности информации операционных систем |
| Противодействовать угрозам безопасности информации с использованием встроенных средств защиты информации операционных систем |
| Выбирать режимы работы программно-аппаратных средств защиты информации в операционных системах |
| Настраивать антивирусные средства защиты информации в операционных системах |
| Устанавливать обновления программного обеспечения и средств антивирусной защиты |
| Проводить мониторинг функционирования программно-аппаратных средств защиты информации в операционных системах |
| Производить анализ эффективности программно-аппаратных средств защиты информации в операционных системах |
| Оценивать оптимальность выбора программно-аппаратных средств защиты информации и их режимов функционирования в операционных системах |
| Необходимые знания | Архитектура и принципы построения операционных систем |
| Программные интерфейсы операционных систем |
| Виды политик управления доступом и информационными потоками применительно к операционным системам |
| Архитектура подсистем защиты информации в операционных системах |
| Принципы функционирования средств защиты информации в операционных системах, в том числе использующих криптографические алгоритмы |
| Состав типовых конфигураций программно-аппаратных средств защиты информации |
| Требования по составу и характеристикам подсистем защиты информации применительно к операционным системам |
| Порядок реализации методов и средств антивирусной защиты в операционных системах |
| Программно-аппаратные средства и методы защиты информации в операционных системах |
| Принципы работы и правила эксплуатации программно-аппаратных средств 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 |
| Другие характеристики | - |

3.2.2. Трудовая функция

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Администрирование программно-аппаратных средств защиты информации в компьютерных сетях | Код | B/02.6 | Уровень (подуровень) квалификации | 6 |

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

|  |  |
| --- | --- |
| Трудовые действия | Определение состава применяемых программно-аппаратных средств защиты информации в компьютерных сетях |
| Разработка порядка применения программно-аппаратных средств защиты информации в компьютерных сетях |
| Формирование шаблонов конфигурации программно-аппаратных средств защиты информации в компьютерных сетях |
| Настройка программных и аппаратных средств построения компьютерных сетей, использующих криптографическую защиту информации |
| Управление функционированием программно-аппаратных средств защиты информации в компьютерных сетях |
| Контроль корректности функционирования программно-аппаратных средств защиты информации в компьютерных сетях |
| Управление средствами межсетевого экранирования в компьютерных сетях в соответствии с действующими требованиями |
| Необходимые умения | Оценивать угрозы безопасности информации в компьютерных сетях |
| Настраивать правила фильтрации пакетов в компьютерных сетях |
| Обосновывать выбор используемых программно-аппаратных средств защиты информации в компьютерных сетях |
| Конфигурировать и контролировать корректность настройки программно-аппаратных средств защиты информации в компьютерных сетях |
| Выбирать режимы работы программно-аппаратных средств защиты информации в компьютерных сетях |
| Проводить мониторинг функционирования программно-аппаратных средств защиты информации в компьютерных сетях |
| Производить анализ эффективности программно-аппаратных средств защиты информации в компьютерных сетях |
| Оценивать оптимальность выбора программно-аппаратных средств защиты информации и их режимов функционирования в компьютерных сетях |
| Необходимые знания | Принципы построения компьютерных сетей |
| Стек сетевых протоколов операционных систем |
| Стек протоколов сетевого оборудования |
| Порядок реализации методов и средств межсетевого экранирования |
| Принципы функционирования сетевых протоколов, включающих криптографические алгоритмы |
| Виды политик управления доступом и информационными потоками в компьютерных сетях |
| Источники угроз информационной безопасности в компьютерных сетях и меры по их предотвращению |
| Состав типовых конфигураций программно-аппаратных средств защиты информации и их режимов функционирования в компьютерных сетях |
| Методы измерений, контроля и технических расчетов характеристик программно-аппаратных средств защиты информации |
| Принципы работы и правила эксплуатации эксплуатируемых программно-аппаратных средств защиты информации |
| Программно-аппаратные средства и методы защиты информации в компьютерных сетях |
| Нормативные правовые акты в области защиты информации |
| Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации |
| Организационные меры по защите информации |
| Другие характеристики | - |

3.2.3. Трудовая функция

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Администрирование средств защиты информации прикладного и системного программного обеспечения | Код | B/03.6 | Уровень (подуровень) квалификации | 6 |

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

|  |  |
| --- | --- |
| Трудовые действия | Определение порядка установки программного обеспечения с целью соблюдения требований по защите информации |
| Контроль над соблюдением требований по защите информации при установке программного обеспечения, включая антивирусное программное обеспечение |
| Формулирование требований к параметрам средств антивирусной защиты для корректной работы программного обеспечения |
| Выполнение работ по обнаружению вредоносного программного обеспечения |
| Ликвидация обнаруженного вредоносного программного обеспечения и последствий его функционирования |
| Формулирование требований к встроенным средствам защиты информации программного обеспечения |
| Необходимые умения | Анализировать угрозы безопасности информации программного обеспечения |
| Формулировать правила безопасной эксплуатации программного обеспечения |
| Обосновывать правила безопасной эксплуатации программного обеспечения |
| Анализировать функционирование программного обеспечения с целью определения возможного вредоносного воздействия |
| Производить проверку соответствия реальных характеристик программно-аппаратных средств защиты информации заявленным в их технической документации |
| Осуществлять мероприятия по противодействию угрозам безопасности информации, возникающим при эксплуатации программного обеспечения |
| Определять порядок функционирования программного обеспечения с целью обеспечения защиты информации |
| Анализировать эффективность сформулированных требований к встроенным средствам защиты информации программного обеспечения |
| Необходимые знания | Архитектура подсистем защиты информации в операционных системах |
| Принципы построения систем управления базами данных |
| Основные средства и методы анализа программных реализаций |
| Принципы построения антивирусного программного обеспечения |
| Виды политик управления доступом и информационными потоками применительно к прикладному программному обеспечению |
| Источники угроз информационной безопасности программного обеспечения и меры по их предотвращению |
| Уязвимости используемого программного обеспечения и методы их эксплуатации |
| Виды и формы функционирования вредоносного программного обеспечения |
| Характерные признаки наличия вредоносного программного обеспечения |
| Средства и методы обнаружения ранее неизвестного вредоносного программного обеспечения |
| Принципы функционирования программных средств криптографической защиты информации |
| Порядок обеспечения безопасности информации при эксплуатации программного обеспечения |
| Нормативные правовые акты в области защиты информации |
| Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации |
| Организационные меры по защите информации |
| Другие характеристики | - |

3.3. Обобщенная трудовая функция

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Оценивание уровня безопасности компьютерных систем и сетей | Код | C | Уровень квалификации | 7 |

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

|  |  |
| --- | --- |
| Возможные наименования должностей, профессий | Специалист по защите информации в компьютерных системах и сетях  Эксперт по анализу защищенности компьютерных систем и сетей  Ведущий (старший) специалист по защите информации  Руководитель группы (специализированной в прочих отраслях)  Руководитель группы (функциональной в прочих областях деятельности) |

|  |  |
| --- | --- |
| 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](consultantplus://offline/ref=7F61548AB8AC225E8BEB5C597F5382E27D73890E09D7A1402C970A2103W5j9L) | [2425](consultantplus://offline/ref=7F61548AB8AC225E8BEB5C597F5382E27D73890E09D7A1402C970A2103594481EA3C219728F4AC49WCj6L) | Специалисты органов государственной власти |
| [2511](consultantplus://offline/ref=7F61548AB8AC225E8BEB5C597F5382E27D73890E09D7A1402C970A2103594481EA3C219728F4AC4BWCj2L) | Системные аналитики |
| [2523](consultantplus://offline/ref=7F61548AB8AC225E8BEB5C597F5382E27D73890E09D7A1402C970A2103594481EA3C219728F4AC4EWCj4L) | Специалисты по компьютерным сетям |
| [2529](consultantplus://offline/ref=7F61548AB8AC225E8BEB5C597F5382E27D73890E09D7A1402C970A2103594481EA3C219728F4AC4EWCj7L) | Специалисты по базам данных и сетям, не входящие в другие группы |
| ЕКС | - | Инженер-программист по технической защите информации |
| - | Администратор по обеспечению безопасности информации |
| - | Специалист по технической защите информации |
| [ОКПДТР](consultantplus://offline/ref=7F61548AB8AC225E8BEB5C597F5382E27D778B0E05D2A1402C970A2103594481EA3C219728F4A949WCj4L) | [26579](consultantplus://offline/ref=7F61548AB8AC225E8BEB5C597F5382E27D778B0E05D2A1402C970A2103594481EA3C219728F3AB48WCj0L) | Специалист по защите информации |
| [46155](consultantplus://offline/ref=7F61548AB8AC225E8BEB5C597F5382E27D778B0E05D2A1402C970A2103594481EA3C219728FCAD48WCj1L) | Руководитель группы подразделения по комплексной защите информации |
| [ОКСО](consultantplus://offline/ref=7F61548AB8AC225E8BEB5C597F5382E27D758B0F08D4A1402C970A2103W5j9L) | [090101](consultantplus://offline/ref=7F61548AB8AC225E8BEB5C597F5382E27D758B0F08D4A1402C970A2103594481EA3C219728F4AA41WCjCL) | Криптография |
| [090102](consultantplus://offline/ref=7F61548AB8AC225E8BEB5C597F5382E27D758B0F08D4A1402C970A2103594481EA3C219728F4AA41WCjDL) | Компьютерная безопасность |
| [090103](consultantplus://offline/ref=7F61548AB8AC225E8BEB5C597F5382E27D758B0F08D4A1402C970A2103594481EA3C219728F4AD48WCj4L) | Организация и технология защиты информации |
| [090104](consultantplus://offline/ref=7F61548AB8AC225E8BEB5C597F5382E27D758B0F08D4A1402C970A2103594481EA3C219728F4AD48WCj5L) | Комплексная защита объектов информатизации |
| [090105](consultantplus://offline/ref=7F61548AB8AC225E8BEB5C597F5382E27D758B0F08D4A1402C970A2103594481EA3C219728F4AD48WCj6L) | Комплексное обеспечение информационной безопасности автоматизированных систем |
| [090106](consultantplus://offline/ref=7F61548AB8AC225E8BEB5C597F5382E27D758B0F08D4A1402C970A2103594481EA3C219728F4AD48WCj7L) | Информационная безопасность телекоммуникационных систем |
| [090107](consultantplus://offline/ref=7F61548AB8AC225E8BEB5C597F5382E27D758B0F08D4A1402C970A2103594481EA3C219728F4AD48WCj0L) | Противодействие техническим разведкам |

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 | Оценка работоспособности применяемых программно-аппаратных средств защиты информации с использованием штатных средств и методик |
| Оценка эффективности применяемых программно-аппаратных средств защиты информации с использованием штатных средств и методик |
| Определение уровня защищенности и доверия программно-аппаратных средств защиты информации |
| Необходимые умения | Определять параметры функционирования программно-аппаратных средств защиты информации |
| Разрабатывать методики оценки защищенности программно-аппаратных средств защиты информации |
| Оценивать эффективность защиты информации |
| Применять разработанные методики оценки защищенности программно-аппаратных средств защиты информации |
| Анализировать программно-аппаратные средства защиты с целью определения уровня обеспечиваемой ими защищенности и доверия |
| Необходимые знания | Принципы построения компьютерных систем и сетей |
| Методы и методики оценки безопасности программно-аппаратных средств защиты информации |
| Принципы построения программно-аппаратных средств защиты информации |
| Принципы построения подсистем защиты информации в компьютерных системах |
| Методы оценки эффективности политики безопасности, реализованной в программно-аппаратных средствах защиты информации |
| Методы и средства оценки корректности и эффективности программных реализаций алгоритмов защиты информации |
| Методы анализа программного кода с целью поиска потенциальных уязвимостей и недокументированных возможностей |
| Способы анализа применяемых методов и средств защиты информации на предмет соответствия политике безопасности |
| Национальные, межгосударственные и международные стандарты в области 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 |
| Другие характеристики | - |

3.3.2. Трудовая функция

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Разработка требований по защите, формирование политик безопасности компьютерных систем и сетей | Код | C/02.7 | Уровень (подуровень) квалификации | 7 |

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

|  |  |
| --- | --- |
| Трудовые действия | Формирование политик безопасности компьютерных систем |
| Консультирование по вопросам безопасности компьютерных систем |
| Разработка профилей защиты и заданий по безопасности |
| Разработка технических заданий на создание средств защиты информации |
| Принятие решения о необходимости защиты информации, содержащейся в информационной системе |
| Классификация информационной системы по требованиям защиты информации |
| Определение угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в компьютерной системе и сети |
| Разработка модели угроз безопасности информации |
| Задание требований к защите информации компьютерной системы |
| Разработка руководящих документов по защите информации в организации |
| Необходимые умения | Анализировать компьютерную систему с целью определения необходимого уровня защищенности и доверия |
| Разрабатывать профили защиты компьютерных систем |
| Формулировать задания по безопасности компьютерных систем |
| Выполнять анализ безопасности компьютерных систем и разрабатывать рекомендации по эксплуатации системы защиты информации |
| Формировать политики безопасности компьютерных систем и сетей |
| Необходимые знания | Принципы построения компьютерных систем и сетей |
| Модели безопасности компьютерных систем |
| Виды политик безопасности компьютерных систем и сетей |
| Принципы построения средств криптографической защиты информации |
| Национальные, межгосударственные и международные стандарты в области защиты информации |
| Возможности используемых и планируемых к использованию средств 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 |
| Другие характеристики | - |

3.3.3. Трудовая функция

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Проведение анализа безопасности компьютерных 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 | Определение уровня защищенности и доверия в компьютерных системах |
| Оценка рисков, связанных с осуществлением угроз безопасности в отношении компьютерных систем |
| Оценка соответствия механизмов безопасности компьютерной системы требованиям существующих нормативных документов, а также их адекватности существующим рискам |
| Подготовка аналитического отчета по результатам проведенного анализа |
| Формулирование предложений по устранению выявленных уязвимостей |
| Необходимые умения | Анализировать компьютерную систему с целью определения уровня защищенности и доверия |
| Прогнозировать возможные пути развития действий нарушителя информационной безопасности |
| Производить анализ политики безопасности на предмет адекватности |
| Проводить мониторинг, анализ и сравнение эффективности программно-аппаратных средств защиты информации в операционных системах |
| Составлять и оформлять аналитический отчет по результатам проведенного анализа |
| Разрабатывать предложения по устранению выявленных уязвимостей |
| Необходимые знания | Принципы построения компьютерных систем и сетей |
| Уязвимости компьютерных систем и сетей |
| Криптографические методы защиты информации |
| Принципы построения систем управления базами данных |
| Средства анализа конфигураций |
| Национальные, межгосударственные и международные стандарты в области 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 |
| Другие характеристики | - |

3.3.4. Трудовая функция

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Проведение сертификации программно-аппаратных средств защиты информации и анализ результатов | Код | C/04.7 | Уровень (подуровень) квалификации | 7 |

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

|  |  |
| --- | --- |
| Трудовые действия | Проведение теоретических исследований уровней защищенности компьютерных систем и сетей |
| Проведение экспериментальных исследований уровней защищенности компьютерных систем и сетей |
| Проведение сертификационных испытаний с использованием инструментальных средств |
| Подготовка аналитического отчета по результатам проведенных сертификационных испытаний |
| Формулирование выводов по оценке защищенности |
| Необходимые умения | Анализировать компьютерную систему с целью определения уровня защищенности и доверия |
| Использовать профили защиты и задания по безопасности |
| Применять инструментальные средства проведения сертификационных испытаний |
| Составлять и оформлять аналитический отчет по проведенным сертификационным испытаниям |
| Делать выводы по оценке защищенности на основании аналитического отчета |
| Необходимые знания | Национальные, межгосударственные и международные стандарты в области защиты информации |
| Национальные стандарты на проведение научно-исследовательских и опытно-конструкторских работ, сертификационных испытаний и создание систем защиты информации |
| Способы организации работ при проведении сертификации программно-аппаратных средств защиты |
| Принципы построения средств криптографической 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 |
| Другие характеристики | - |

3.3.5. Трудовая функция

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

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

|  |  |
| --- | --- |
| Трудовые действия | Выполнение анализа защищенности компьютерных систем с использованием сканеров безопасности |
| Выполнение анализа защищенности сетевых сервисов с использованием средств автоматического реагирования на попытки несанкционированного доступа к ресурсам компьютерных систем и сетей |
| Составление отчетов по результатам проверок |
| Необходимые умения | Формализовывать задачу управления безопасностью компьютерных систем |
| Применять инструментальные средства проведения мониторинга защищенности компьютерных систем |
| Применять методы анализа защищенности компьютерных систем и сетей |
| Структурировать аналитическую информацию для включения в отчет |
| Необходимые знания | Принципы построения компьютерных систем и сетей |
| Формальные модели безопасности компьютерных систем и сетей |
| Принципы построения систем обнаружения компьютерных атак |
| Методы обработки данных мониторинга безопасности компьютерных систем и сетей |
| Порядок создания и структура отчета, создаваемого по результатам проверок |
| Способы обнаружения и нейтрализации последствий вторжений в компьютерные системы |
| Криптографические протоколы, применяемые в компьютерных сетях |
| Нормативные правовые акты в области защиты информации |
| Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации |
| Организационные меры по защите информации |
| Другие характеристики | - |

3.3.6. Трудовая функция

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Проведение экспертизы при расследовании компьютерных 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 | Определение свойств аппаратных средств в составе компьютерной системы и их фактического и первоначального состояния |
| Классификация свойств аппаратных средств в составе компьютерной системы |
| Диагностика причин, условий изменения свойств (эксплуатационных режимов) аппаратных средств в составе компьютерной системы |
| Определение характеристик операционной системы и используемых технологий системного программирования |
| Анализ функциональных свойств программного обеспечения |
| Исследование алгоритма программного продукта и типов поддерживаемых аппаратных платформ |
| Определение причин, целей и условий изменения свойств (состояния) программного обеспечения |
| Индивидуальное отождествление оригинала программы (инсталляционной версии) и ее копии на носителях данных компьютерной системы |
| Установление групповой принадлежности программного обеспечения |
| Выработка предложений по устранению выявленных уязвимостей |
| Выявление индивидуальных признаков программы, позволяющих впоследствии идентифицировать ее автора, а также взаимосвязи с информационным обеспечением исследуемой компьютерной системы |
| Установление вида, свойств и состояния информации (фактического и первоначального, в том числе до ее удаления и модификации) в компьютерной системе |
| Определение причин и условий изменения свойств исследуемой информации |
| Определение механизма, динамики и обстоятельств события по имеющейся информации на носителе данных или ее копиям |
| Установление участников события, их роли, места, условий, при которых была создана, модифицирована или удалена информация |
| Установление соответствия либо несоответствия действий с информацией специальному регламенту (правилам) |
| Составление экспертного заключения |
| Необходимые умения | Применять нормативные и правовые акты при проведении криминалистической экспертизы и криминалистического анализа |
| Анализировать структуру механизма возникновения и обстоятельства события |
| Определять причину и условия изменения программного обеспечения |
| Выделять свойства и признаки информации, позволяющие установить ее принадлежность определенному источнику |
| Определять принципы деления программного обеспечения на группы, их специфические свойства и взаимосвязь с компьютерной системой |
| Применять действующую законодательную базу в области обеспечения защиты информации |
| Выявлять возможные траектории состояний функционирования системы |
| Выявлять несоответствия имеющейся информации ее расположению в системе |
| Прогнозировать возможные пути развития новых видов компьютерных преступлений, правонарушений и инцидентов |
| Необходимые знания | Форматы хранения информации в анализируемой компьютерной системе |
| Основные форматы файлов, используемые в компьютерных системах |
| Особенности хранения конфигурационной и системной информации в компьютерных системах |
| Уязвимости компьютерных систем и сетей |
| Технологии поиска и анализа следов компьютерных преступлений, правонарушений и инцидентов |
| Порядок фиксации и документирования следов компьютерных преступлений, правонарушений и инцидентов |
| Нормы уголовного и административного права в сфере компьютерной информации |
| Характеристики правонарушений в области связи и информации |
| Виды преступлений в сфере компьютерной информации |
| Порядок проведения экспертизы вычислительной техники и носителей компьютерной информации с учетом нормативных правовых актов |
| Способы обнаружения и нейтрализации последствий вторжений в компьютерные системы |
| Методы анализа систем обеспечения информационной безопасности объектов информатизации на базе компьютерных систем в защищенном исполнении |
| Порядок подготовки научно-технических экспертных заключений по результатам выполненных работ по информационно-аналитической и технической экспертизе компьютерных систем |
| Методы проведения расследования компьютерных преступлений, правонарушений и инцидентов |
| Методы анализа остаточной информации и поиска следов для фиксации компьютерных инцидентов |
| Криптографические алгоритмы и особенности их программной реализации |
| Нормативные правовые акты в области защиты информации |
| Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации |
| Организационные меры по защите информации |
| Другие характеристики | - |

3.4. Обобщенная трудовая функция

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Разработка программно-аппаратных средств защиты информации компьютерных систем и сетей | Код | D | Уровень квалификации | 8 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Происхождение обобщенной трудовой функции | Оригинал | X | 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)  и  Дополнительное профессиональное образование - программы повышения квалификации в области информационной безопасности |
| Требования к опыту практической работы | Не менее пяти лет работы по применению и анализу эффективности средств защиты информации компьютерных систем, 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 работы по применению и анализу эффективности средств защиты информации компьютерных систем, 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](consultantplus://offline/ref=7F61548AB8AC225E8BEB5C597F5382E27D73890E09D7A1402C970A2103W5j9L) | [1223](consultantplus://offline/ref=7F61548AB8AC225E8BEB5C597F5382E27D73890E09D7A1402C970A2103594481EA3C219728F4A84EWCj6L) | Руководители подразделений по научным исследованиям и разработкам |
| [1330](consultantplus://offline/ref=7F61548AB8AC225E8BEB5C597F5382E27D73890E09D7A1402C970A2103594481EA3C219728F4A841WCjCL) | Руководители служб и подразделений в сфере информационно-коммуникационных технологий |
| [2519](consultantplus://offline/ref=7F61548AB8AC225E8BEB5C597F5382E27D73890E09D7A1402C970A2103594481EA3C219728F4AC4CWCjCL) | Разработчики и аналитики программного обеспечения и приложений, не входящие в другие группы |
| ЕКС | - | Главный специалист по технической защите информации |
| - | Начальник отдела (лаборатории, сектора) по технической защите информации |
| - | Специалист по обеспечению безопасности информации в ключевых системах информационной инфраструктуры |
| [ОКПДТР](consultantplus://offline/ref=7F61548AB8AC225E8BEB5C597F5382E27D778B0E05D2A1402C970A2103594481EA3C219728F4A949WCj4L) | [20911](consultantplus://offline/ref=7F61548AB8AC225E8BEB5C597F5382E27D778B0E05D2A1402C970A2103594481EA3C219728F3AF4CWCj2L) | Главный специалист по защите информации |
| [46115](consultantplus://offline/ref=7F61548AB8AC225E8BEB5C597F5382E27D778B0E05D2A1402C970A2103594481EA3C219728FCAD48WCj0L) | Руководитель аналитической группы подразделения по комплексной защите информации |
| [46155](consultantplus://offline/ref=7F61548AB8AC225E8BEB5C597F5382E27D778B0E05D2A1402C970A2103594481EA3C219728FCAD48WCj0L) | Руководитель группы подразделения по комплексной защите информации |
| [ОКСО](consultantplus://offline/ref=7F61548AB8AC225E8BEB5C597F5382E27D758B0F08D4A1402C970A2103W5j9L) | [090101](consultantplus://offline/ref=7F61548AB8AC225E8BEB5C597F5382E27D758B0F08D4A1402C970A2103594481EA3C219728F4AA41WCjCL) | Криптография |
| [090102](consultantplus://offline/ref=7F61548AB8AC225E8BEB5C597F5382E27D758B0F08D4A1402C970A2103594481EA3C219728F4AA41WCjDL) | Компьютерная безопасность |
| [090103](consultantplus://offline/ref=7F61548AB8AC225E8BEB5C597F5382E27D758B0F08D4A1402C970A2103594481EA3C219728F4AD48WCj4L) | Организация и технология защиты информации |
| [090104](consultantplus://offline/ref=7F61548AB8AC225E8BEB5C597F5382E27D758B0F08D4A1402C970A2103594481EA3C219728F4AD48WCj5L) | Комплексная защита объектов информатизации |
| [090105](consultantplus://offline/ref=7F61548AB8AC225E8BEB5C597F5382E27D758B0F08D4A1402C970A2103594481EA3C219728F4AD48WCj6L) | Комплексное обеспечение информационной безопасности автоматизированных систем |
| [090106](consultantplus://offline/ref=7F61548AB8AC225E8BEB5C597F5382E27D758B0F08D4A1402C970A2103594481EA3C219728F4AD48WCj7L) | Информационная безопасность телекоммуникационных систем |
| [ОКСВНК](consultantplus://offline/ref=7F61548AB8AC225E8BEB5540785382E27A7786040CD2A1402C970A2103W5j9L) [<7>](#P1322) | [051319](consultantplus://offline/ref=7F61548AB8AC225E8BEB5540785382E27A7786040CD2A1402C970A2103594481EA3C219728F4A140WCjCL) | Методы и системы защиты информации и информационной безопасности |

3.4.1. Трудовая функция

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Разработка требований к программно-аппаратным средствам защиты информации компьютерных систем и сетей | Код | D/01.8 | Уровень (подуровень) квалификации | 8 |

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

|  |  |
| --- | --- |
| Трудовые действия | Определение угроз безопасности и их возможных источников |
| Определение каналов утечки информации |
| Разработка математических моделей, реализуемых в средствах защиты информации |
| Оценка эффективности реализуемых технических решений |
| Оценка технико-экономического уровня реализуемых технических решений |
| Выбор средств и методов защиты информации |
| Необходимые умения | Обобщать научно-техническую литературу, нормативные и методические материалы в области защиты информации |
| Формировать модели угроз и модели нарушителя безопасности компьютерных систем |
| Выявлять наиболее целесообразные подходы к обеспечению защиты информации компьютерной системы |
| Разрабатывать частные политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками |
| Применять национальные, межгосударственные и международные стандарты в области защиты информации для оценки защищенности компьютерной системы |
| Применять действующую законодательную базу в области обеспечения компьютерной безопасности |
| Читать и понимать нормативные и методические документы по информационной безопасности на английском языке |
| Осуществлять принятие решений о необходимости использования программно-аппаратных средств защиты информации |
| Необходимые знания | Порядок организации работ по защите информации |
| Методы и средства получения, обработки и передачи информации в операционных системах, системах управления базами данных и компьютерных сетях |
| Методы анализа безопасности компьютерных систем |
| Виды атак и механизмы их реализации в компьютерных системах |
| Методы выявления каналов утечки информации |
| Методы и средства защиты информации в компьютерных сетях, операционных системах и системах управления базами данных |
| Принципы построения средств защиты информации компьютерных систем |
| Формальные модели управления доступом |
| Криптографические алгоритмы и особенности их программной реализации |
| Нормативные правовые акты в области защиты информации |
| Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации |
| Организационные меры по защите информации |
| Национальные, межгосударственные и международные стандарты в области защиты информации |
| Другие характеристики | - |

3.4.2. Трудовая функция

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Проектирование программно-аппаратных средств защиты информации компьютерных систем и сетей | Код | D/02.8 | Уровень (подуровень) квалификации | 8 |

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

|  |  |
| --- | --- |
| Трудовые действия | Разработка технических заданий, эскизных, технических и рабочих проектов работ по защите информации |
| Разработка планов и графиков проведения работ по защите информации |
| Анализ существующих методов и средств, применяемых для контроля и защиты информации |
| Разработка предложения по совершенствованию существующих методов и средств, применяемых для контроля и защиты информации и повышению эффективности этой защиты |
| Разработка проектов программных и аппаратных средств защиты информации в соответствии с техническим заданием |
| Оценка технико-экономического уровня и эффективности предлагаемых и реализуемых технических решений |
| Проведение аттестации программ и алгоритмов на предмет соответствия требованиям защиты информации |
| Необходимые умения | Проводить исследования с целью нахождения наиболее целесообразных практических решений по обеспечению защиты информации |
| Применять отечественные стандарты в области защиты информации для проектирования средств защиты информации компьютерной системы |
| Разрабатывать архитектуру и интерфейсы средств защиты информации, процедуры восстановления работоспособности средств и систем защиты после сбоев |
| Подбирать и обобщать научно-техническую литературу, методические материалы по программным и аппаратным средствам и способам защиты информации, в том числе на английском языке |
| Необходимые знания | Методы и средства получения, обработки и передачи информации в операционных системах, системах управления базами данных и компьютерных сетях |
| Виды атак и механизмы их реализации в компьютерных системах |
| Методы и средства защиты информации в компьютерных сетях, операционных системах и системах управления базами данных |
| Принципы построения систем защиты информации компьютерных систем, в том числе антивирусного программного обеспечения |
| Методы анализа безопасности компьютерных систем |
| Теоретико-числовые методы и алгоритмы, применяемые в средствах защиты информации |
| Формальные модели управления доступом |
| Принципы и методы проектирования программно-аппаратного обеспечения |
| Методологии и технологии разработки программного обеспечения |
| Принципы и методы управления проектами в области информационной безопасности |
| Криптографические алгоритмы и особенности их программной реализации |
| Нормативные правовые акты в области защиты информации |
| Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации |
| Организационные меры по защите информации |
| Национальные, межгосударственные и международные стандарты в области защиты информации |
| Другие характеристики | - |

3.4.3. Трудовая функция

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Разработка и тестирование средств защиты информации компьютерных систем и сетей | Код | D/03.8 | Уровень (подуровень) квалификации | 8 |

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

|  |  |
| --- | --- |
| Трудовые действия | Разработка средств защиты информации в соответствии с техническим заданием |
| Исследование программно-аппаратных средств защиты информации в компьютерных системах |
| Разработка программно-аппаратных средств защиты информации в компьютерных системах |
| Отладка создаваемых средств защиты информации |
| Проведение аттестации программ и алгоритмов на предмет соответствия требованиям защиты информации |
| Разработка математических моделей безопасности компьютерных систем |
| Выполнение контрольных проверок работоспособности и эффективности систем и средств защиты информации |
| Необходимые умения | Использовать приемы защитного программирования |
| Использовать приемы защиты от типовых атак компьютерных систем |
| Применять методы и приемы отладки |
| Применять методы и средства тестирования |
| Необходимые знания | Методы и средства получения, обработки и передачи информации в операционных системах, системах управления базами данных и компьютерных сетях |
| Методы и средства защиты информации в компьютерных сетях, операционных системах и системах управления базами данных |
| Методы анализа безопасности компьютерных систем |
| Принципы проектирования антивирусного программного обеспечения |
| Виды атак и механизмы их реализации в компьютерных системах |
| Принципы построения систем защиты информации компьютерных систем |
| Методологии и технологии разработки программного и аппаратного обеспечения |
| Криптографические алгоритмы и особенности их программной реализации |
| Нормативные правовые акты в области защиты информации |
| Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации |
| Организационные меры по защите информации |
| Национальные, межгосударственные и международные стандарты в области защиты информации |
| Другие характеристики | - |

3.4.4. Трудовая функция

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Сопровождение разработки средств защиты информации компьютерных систем и сетей | Код | D/04.8 | Уровень (подуровень) квалификации | 8 |

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

|  |  |
| --- | --- |
| Трудовые действия | Разработка технических заданий, планов и графиков проведения работ по защите информации в соответствии с действующим нормативными и методическими документами |
| Разработка рекомендаций и предложений по совершенствованию и повышению эффективности защиты информации |
| Составление и оформление разделов научно-технических отчетов |
| Определение потребности в средствах защиты информации, составление заявок на их приобретение с необходимыми обоснованиями и расчетами |
| Подготовка предложений по заключению соглашений и договоров с другими учреждениями, организациями, предоставляющими услуги в области защиты информации |
| Выполнение аттестации программ и алгоритмов на предмет соответствия требованиям защиты информации |
| Выполнение контрольных проверок работоспособности и эффективности систем и средств защиты информации |
| Анализ существующих методов и средств, применяемых для контроля и защиты информации |
| Разработка предложений по совершенствованию и повышению эффективности методов и средств, применяемых для контроля и защиты информации |
| Подготовка проектов нормативных и методических материалов, регламентирующих работу по защите информации |
| Разработка организационно-распорядительных документов по защите информации |
| Контроль над работой по оценке технико-экономического уровня разрабатываемых мер по защите информации |
| Методическое руководство работой по оценке технико-экономического уровня разрабатываемых мер по защите информации |
| Контроль над соблюдением установленного порядка выполнения работ, а также действующего законодательства Российской Федерации при решении вопросов, касающихся защиты информации |
| Организация проведения специальных исследований и контрольных проверок по выявлению возможных каналов утечки информации |
| Необходимые умения | Формировать модели угроз и модели нарушителя безопасности компьютерных систем |
| Разрабатывать частные политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками |
| Применять национальные, межгосударственные и международные стандарты в области защиты информации |
| Применять действующую законодательную базу в области обеспечения защиты информации |
| Читать и понимать нормативные и методические документы по информационной безопасности на английском языке |
| Необходимые знания | Методы и средства получения, обработки и передачи информации |
| Методы выявления каналов утечки информации |
| Порядок организации работ по защите информации |
| Методы планирования и организации проведения работ по защите информации и обеспечению государственной тайны |
| Методы проведения специальных исследований и проверок, работ по защите информации |
| Методы и средства защиты информации в компьютерных сетях, операционных системах и системах управления базами данных |
| Методы анализа безопасности компьютерных систем |
| Принципы проектирования антивирусного программного обеспечения |
| Виды атак и механизмы их реализации в компьютерных системах |
| Принципы построения систем защиты информации компьютерных систем |
| Формальные модели управления доступом |
| Криптографические алгоритмы и особенности их программной реализации |
| Нормативные правовые акты в области защиты информации |
| Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации |
| Организационные меры по защите информации |
| Национальные, межгосударственные и международные стандарты в области защиты информации |
| 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 |
| 4 | Федеральное учебно-методическое объединение по укрупненной группе специальностей и направлений подготовки "Информационная безопасность", город Москва |

--------------------------------

<1> Общероссийский [классификатор](consultantplus://offline/ref=7F61548AB8AC225E8BEB5C597F5382E27D73890E09D7A1402C970A2103W5j9L) занятий.

<2> Общероссийский [классификатор](consultantplus://offline/ref=7F61548AB8AC225E8BEB5C597F5382E27E74890109D0A1402C970A2103W5j9L) видов экономической деятельности.

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

<4> Общероссийский [классификатор](consultantplus://offline/ref=7F61548AB8AC225E8BEB5C597F5382E27D778B0E05D2A1402C970A2103594481EA3C219728F4A949WCj4L) профессий рабочих, должностей служащих и тарифных разрядов.

<5> Общероссийский [классификатор](consultantplus://offline/ref=7F61548AB8AC225E8BEB5C597F5382E27D758B0F08D4A1402C970A2103W5j9L) специальностей по образованию.

<6> [Закон](consultantplus://offline/ref=7F61548AB8AC225E8BEB5C597F5382E27D7388040DD1A1402C970A2103W5j9L) Российской Федерации от 21 июля 1993 г. N 5485-1 "О государственной тайне" (Собрание законодательства Российской Федерации, 1996, N 15, ст. 1768; 1997, N 41, ст. ст. 4673, 8220, 8221, 8222, 8223, 8224, 8225, 8226, 8227, 8228, 8229, 8230, 8231, 8232, 8233, 8234, 8235; 2002, N 52, ст. 5288; 2003, N 6, ст. 549, N 27, ст. 2700, N 46, ст. 4449; 2004, N 27, ст. 2711, N 35, ст. 3607; 2007, N 49, ст. 6055, ст. 6079; 2009, N 29, ст. 3617; 2010, N 47, ст. 6033; 2011, N 30, ст. 4590, ст. 4596, N 46, ст. 6407; 2013, N 51, ст. 6697; 2015, N 10, ст. 1393).

<7> Общероссийский [классификатор](consultantplus://offline/ref=7F61548AB8AC225E8BEB5540785382E27A7786040CD2A1402C970A2103W5j9L) специальностей высшей научной квалификации.