



МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ЗАРЕГИСТРИРОВАНО

Регистрационный № 44464

от "28" ноября 2016 г.

**МИНИСТЕРСТВО ТРУДА И СОЦИАЛЬНОЙ ЗАЩИТЫ
РОССИЙСКОЙ ФЕДЕРАЦИИ**
(Минтруд России)

ПРИКАЗ

1 ноября 2016 г.

№ 598 н

Москва

**Об утверждении профессионального стандарта
«Специалист по безопасности компьютерных систем и сетей»**

В соответствии с пунктом 16 Правил разработки и утверждения профессиональных стандартов, утвержденных постановлением Правительства Российской Федерации от 22 января 2013 г. № 23 (Собрание законодательства Российской Федерации, 2013, № 4, ст. 293; 2014, № 39, ст. 5266; 2016, № 21, ст. 3002), п р и к а з ы в а ю:

Утвердить прилагаемый профессиональный стандарт «Специалист по безопасности компьютерных систем и сетей».

Министр

М.А. Топилин

КОПИЯ ВЕРНА
Консультант общего отдела Департамента
управления делами _____
1.11. _____ 20 16 г.



УТВЕРЖДЕН
приказом Министерства
труда и социальной защиты
Российской Федерации
от «1» ноября 2016 г. № 598н

ПРОФЕССИОНАЛЬНЫЙ СТАНДАРТ

Специалист по безопасности компьютерных систем и сетей

842

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 «Обслуживание средств защиты информации в компьютерных системах и сетях».....	5
3.2. Обобщенная трудовая функция «Администрирование средств защиты информации в компьютерных системах и сетях».....	10
3.3. Обобщенная трудовая функция «Оценивание уровня безопасности компьютерных систем и сетей».....	15
3.4. Обобщенная трудовая функция «Разработка программно-аппаратных средств защиты информации компьютерных систем и сетей».....	22
IV. Сведения об организациях – разработчиках профессионального стандарта.....	29

I. Общие сведения

Защита информации в компьютерных системах и сетях

(наименование вида профессиональной деятельности)

06.032

Код

Основная цель вида профессиональной деятельности:

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

Группа занятий:

1223	Руководители подразделений по научным исследованиям и разработкам	1330	Руководители служб и подразделений в сфере информационно-коммуникационных технологий
2425	Специалисты органов государственной власти	2511	Системные аналитики
2519	Разработчики и аналитики программного обеспечения и приложений, не входящие в другие группы	2522	Системные администраторы
2523	Специалисты по компьютерным сетям	2529	Специалисты по базам данных и сетям, не входящие в другие группы

3359	Среднетехнический персонал на государственной службе, не входящий в другие группы	3511	Специалисты-техники по эксплуатации ИКТ
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
62.09	Деятельность, связанная с использованием вычислительной техники и информационных технологий, 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
А	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
В	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
С	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, формированию 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	C/05.7	7

			защищенности компьютерных систем и сетей 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	Заемствовано 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	3511	Специалисты-техники по эксплуатации ИКТ
	3513	Специалисты-техники по компьютерным сетям и системам
	3359	Среднетехнический персонал на государственной службе, не входящий в другие группы
ЕКС ³	-	Техник по защите информации
ОКПДТР ⁴	27032	Техник по защите информации
ОКСО ⁵	090108	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	Заемствовано 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	<input checked="" type="checkbox"/>	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	<input checked="" type="checkbox"/>	Займствовано из оригинала	<input type="checkbox"/>	<input type="checkbox"/>
			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	В	Уровень квалификации	6
--------------	---	-----	---	----------------------	---

Происхождение обобщенной трудовой функции	Оригинал	X	Займствовано 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 (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	2425	Специалисты органов государственной власти
	2522	Системные администраторы
	2523	Специалисты по компьютерным сетям
	2529	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	26579	Специалист по защите информации
	40067	Администратор вычислительной сети
	22824	Инженер-программист
	40070	Администратор информационной безопасности вычислительной сети

3.2.1. Трудовая функция

Наименование	Администрирование подсистем защиты информации в операционных системах	Код	В/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	В/02.6	Уровень (подуровень) квалификации	6
--------------	--	-----	--------	-----------------------------------	---

Происхождение трудовой функции	Оригинал	<input checked="" type="checkbox"/>	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 межсетевое 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