

УТВЕРЖДЕН  
приказом Министерства  
труда и социальной защиты  
Российской Федерации  
от «\_\_» \_\_\_\_\_ 2015 г. №\_\_

# ПРОФЕССИОНАЛЬНЫЙ СТАНДАРТ

## Специалист по безопасности компьютерных систем и сетей

Регистрационный номер

### Содержание

I. Общие сведения .....	2
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 защищенных компьютерных систем и сетей» .....	5
3.2. Обобщенная трудовая функция «Администрирование программно-аппаратных средств защиты информации в компьютерных системах и сетях» .....	8
3.3. Обобщенная трудовая функция «Разработка и применение методов оценивания безопасности компьютерных систем и сетей» .....	11
3.4. Обобщенная трудовая функция «Проектирование технических и программно-математических средств защиты информации компьютерных систем и сетей» .....	18
IV. Сведения об организациях-разработчиках профессионального стандарта .....	24

## I. Общие сведения

Разработка, внедрение, эксплуатация, экспертиза и менеджмент средств и систем обеспечения информационной безопасности компьютерных систем и сетей

(наименование вида профессиональной деятельности)

Код

Основная цель вида профессиональной деятельности:

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

Группа занятий:

311	Техники в области физических и технических наук	2523	Специалисты по компьютерным сетям
3511	Специалисты-техники по эксплуатации информационно-коммуникационных технологий	251	Разработчики и аналитики программного обеспечения и приложений
3513	Специалисты-техники по компьютерным сетям и системам	1223	Руководители подразделений по научным исследованиям и разработкам
21	Специалисты в области науки и техники	1330	Руководители служб в сфере информационно-коммуникационных технологий
2512	Разработчики программного обеспечения		
(код ОКЗ <sup>1</sup> )	(наименование)	(код ОКЗ)	(наименование)

Отнесение к видам экономической деятельности:

62.02.1	Деятельность по планированию, проектированию компьютерных систем
62.02.2	Деятельность по обследованию и экспертизе компьютерных систем
(код ОКВЭД <sup>2</sup> )	(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 защищенных компьютерных систем и сетей	5	Обслуживание программно-аппаратных средств защиты информации компьютерных систем и сетей	А/01.5	5
			Обслуживание технических средств защиты информации в компьютерных системах и сетях	А/02.5	5
			Применение методов и средств защиты информации в компьютерных системах и сетях	А/03.5	5
В	Администрирование программно-аппаратных средств защиты информации в компьютерных системах и сетях	6	Администрирование подсистем защиты информации в компьютерных системах и сетях	В/01.6	6
			Приемка и внедрение программно-аппаратных средств защиты информации	В/02.6	6
			Сопровождение и обслуживание программно-аппаратных средств защиты информации	В/03.6	6
С	Разработка и применение методов оценивания безопасности компьютерных систем и сетей	7	Проведение контрольных проверок работоспособности и эффективности применяемых программно-аппаратных средств защиты информации	С/01.7	7
			Разработка требований по защите, формирование политик безопасности компьютерных систем и сетей	С/02.7	7

			Проведение криминалистического анализа компьютерных систем	C/03.7	7
			Выполнение экспериментально-исследовательских работ при проведении сертификации программно-аппаратных средств защиты информации и анализ результатов	C/04.7	7
			Проведение экспериментально-исследовательских работ при аттестации объектов с учетом требований к обеспечению защищенности	C/05.7	7
			Проведение инструментального мониторинга защищенности компьютерных систем и сетей	C/06.7	7
			Проведение экспертизы при расследовании компьютерных преступлений, правонарушений и инцидентов	C/07.7	7
D	Проектирование специальных технических и программно-математических средств защиты информации компьютерных систем и сетей	8	Разработка требований к специальным техническим средствам защиты информации компьютерных систем с учетом действующих нормативных и методических документов	D/01.8	8
			Проектирование программных и аппаратных средств защиты информации компьютерных систем и сетей	D/02.8	8
			Разработка, отладка 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 защищенных компьютерных систем и сетей	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 Специалист-техник по безопасности компьютерных систем и сетей
--	---

Требования к образованию и обучению	Среднее профессиональное образование по УГС (направлению подготовки) «Информационная безопасность»
Требования к опыту практической работы	-
Особые условия допуска к работе	Наличие допуска к сведениям, составляющим государственную тайну <sup>3</sup> ; наличие допуска к работе на электроустановках (не ниже III группы электробезопасности) <sup>4</sup>
Другие характеристики	-

#### Дополнительные характеристики

Наименование документа	Код	Наименование базовой группы, должности (профессии) или специальности
ОКЗ	311	Техники в области физических и технических наук
	3511	Специалисты-техники по эксплуатации информационно-коммуникационных технологий
	3513	Специалисты-техники по компьютерным сетям и системам
ЕКС <sup>5</sup>	-	Техник по технической защите информации
ОКПДТР <sup>6</sup>	27032	Техник по защите информации
	27099	Техник-программист
ОКСО <sup>7</sup>	10.02.01	Организация и технология защиты информации

#### 3.1.1. Трудовая функция

Наименование	Обслуживание программно-аппаратных средств защиты информации компьютерных систем и сетей	Код	A/0 1.5	Уровень (подуровень) квалификации	5
--------------	--	-----	------------	-----------------------------------	---

Происхождение трудовой функции	Оригинал	X	Заимствовано из оригинала		

Трудовые действия	Ввод в эксплуатацию программно-аппаратных средств защиты информации в компьютерных системах и сетях
	Установка программных средств защиты информации в компьютерных системах и сетях
	Настройка программно-аппаратных средств защиты информации
	Оформление документации программно-аппаратных средств защиты информации
Необходимые умения	Применять программно-аппаратные средства защиты информации в компьютерных системах и сетях
	Обладать навыками использования современных информационных технологий, применения общего и специального программного обеспечения
	Осуществлять техническое обслуживание и текущий ремонт программно-аппаратных средств защиты информации
Необходимые знания	Сущность и содержание понятия информационной безопасности, характеристики ее составляющих
	Источники угроз информационной безопасности и меры по их предотвращению
	Современные программно-аппаратные средства и способы обеспечения информационной безопасности в компьютерных системах и сетях
	Математические и алгоритмические основы построения программных средств защиты информации
	Общие принципы функционирования программных компонентов криптографической защиты информации
Другие характеристики	-

### 3.1.2. Трудовая функция

Наименование	Обслуживание технических средств защиты информации в компьютерных системах и сетях	Код	A/0 2.5	Уровень (подуровень) квалификации	5
--------------	--	-----	------------	---	---

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

Трудовые действия	Ввод в эксплуатацию технических средств защиты информации
	Монтаж технических средств защиты информации
	Настройка технических средств защиты информации в соответствии с заданными эксплуатационными характеристиками
	Оформление документации технических средств защиты информации
Необходимые умения	Применять технические средства защиты информации
	Осуществлять настройку технических средств защиты информации
	Проводить мониторинг эффективности технических средств защиты информации в компьютерных системах и сетях

Необходимые знания	Сущность и содержание понятия информационной безопасности, характеристики ее составляющих
	Источники угроз информационной безопасности и меры по их предотвращению
	Современные технические средства защиты информации в компьютерных системах и сетях
	Типовые схемы построения технических средств защиты информации и особенности их аппаратной реализации
	Порядок эксплуатации технических средств защиты информации
	Общие принципы функционирования аппаратных компонент криптографической защиты информации
Другие характеристики	-

### 3.1.3. Трудовая функция

Наименование	Применение методов и средств защиты информации в компьютерных системах и сетях	Код	A/0 3.5	Уровень (подуровень) квалификации	5
--------------	--	-----	------------	-----------------------------------	---

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

Трудовые действия	Настройка средств защиты информации компьютерных систем
	Техническая поддержка эксплуатации средств защиты информации компьютерных систем
	Обобщение научно-технической литературы, нормативных и методических материалов по программно-аппаратным средствам и способам защиты информации компьютерных систем
	Обслуживание в комплексе технических и программно-аппаратных средств защиты информации
Необходимые умения	Выполнять настройку технических и программно-аппаратных средств защиты информации
	Обобщать статистическую информацию по вопросам эксплуатации средств защиты информации
	Осуществлять мероприятия по осуществлению бесперебойной работы средств защиты информации
Необходимые знания	Сущность и содержание понятия информационной безопасности, характеристики ее составляющих
	Источники угроз информационной безопасности и меры по их предотвращению
	Современные технические и программно-аппаратные средства защиты информации в компьютерных системах и сетях
	Правила восстановления работоспособности эксплуатируемых средств защиты информации
	Порядок совместного использования технических и программно-аппаратных средств защиты информации
	Основные нормативно-правовые акты и методические документы уполномоченных федеральных органов исполнительной власти в области информационной безопасности.

	Общие принципы функционирования программных и аппаратных компонент криптографической защиты информации
Другие характеристики	-

### 3.2. Обобщенная трудовая функция

Наименование	Администрирование программно-аппаратных средств защиты информации в компьютерных системах и сетях	Код	В	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
--	--

Требования к образованию и обучению	Высшее образование – магистратура или специалитет по УГС (направлению подготовки) «Информационная безопасность» Дополнительное профессиональное образование
Требования к опыту практической работы	-
Особые условия допуска к работе	Наличие допуска к сведениям, составляющим государственную тайну <sup>3</sup> ; наличие допуска к работе на электроустановках (не ниже III группы электробезопасности) <sup>4</sup>
Другие характеристики	-

Дополнительные характеристики

Наименование документа	Код	Наименование базовой группы, должности (профессии) или специальности
ОКЗ	21	Специалисты в области науки и техники
	2512	Разработчики программного обеспечения
ЕКС	-	Инженер по технической защите информации
	-	Инженер-программист по технической защите информации
	-	Администратор по обеспечению безопасности информации
ОКПДТР	26579	Специалист по защите информации
	40070	Администратор информационной безопасности вычислительной сети
ОКСО	10.04.01	Информационная безопасность
	10.05.01	Компьютерная безопасность

#### 3.2.1. Трудовая функция

Наименование	Администрирование подсистем защиты информации в компьютерных системах и сетях	Код	B/0 1.6	Уровень (подуровень) квалификации	6
--------------	---	-----	------------	-----------------------------------	---

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

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

### 3.2.2. Трудовая функция

Наименование	Приемка и внедрение программно-аппаратных средств защиты информации	Код	B/0 2.6	Уровень (подуровень) квалификации	6
--------------	---	-----	------------	-----------------------------------	---

Происхождение трудовой функции

Оригинал	X	Заимствовано из оригинала		
			Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Приемка программно-аппаратных средств защиты информации
	Проверка и оценка соответствия реальных характеристик программно-аппаратных средств защиты информации заявленным в технической документации на эти средства информации
	Оформление документации по приемке и постановке на учет приобретаемых программно-аппаратных средств защиты информации
Необходимые умения	Проводить проверку и оценивать соответствие реальных характеристик программно-аппаратных средств защиты информации заявленным в технической документации на эти средства
	Оформлять необходимую документацию по приемке приобретаемых программно-аппаратных средств защиты информации
	Выполнять установку и начальную настройку программно-аппаратных средств защиты информации
	Осуществлять включение программно-аппаратных средств защиты информации в состав действующей компьютерной системы и сети
	Оформлять установленную документацию по учету и использованию средств криптографической защиты информации
Необходимые знания	Основы защиты в операционных системах
	Основы построения защищенных компьютерных сетей
	Основы построения защищенных баз данных
	Принципы работы и правила эксплуатации приобретаемых программно-аппаратных средств защиты информации
	Методы измерений, контроля и технических расчетов характеристик программно-аппаратных средств защиты информации
	Порядок оформления документации по приемке и постановке на учет в организации приобретаемых программно-аппаратных средств защиты информации
	Порядок оформления документации при эксплуатации средств криптографической защиты информации
Другие характеристики	-

### 3.2.3. Трудовая функция

Наименование	Сопровождение и обслуживание программно-аппаратных средств защиты информации	Код	В/0 3.6	Уровень (подуровень) квалификации	6
--------------	--	-----	------------	-----------------------------------	---

Происхождение трудовой функции

Оригинал	X	Заимствовано из оригинала		
			Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Контроль за соблюдением и порядком настройки программно-аппаратных средств защиты информации
-------------------	--

	Подготовка замечаний и предложений по изменению документации на программно-аппаратных средств защиты информации
	Оформление эксплуатационной документации программно-аппаратных средств защиты информации
	Использование технической документации, технической литературы и справочников при освоении новых программно-аппаратных средств защиты информации
Необходимые умения	Анализировать программно-аппаратные средства защиты информации в целях определения направлений эффективного применения
	Готовить аналитический отчет по результатам проведенного анализа и формулировать предложения применению и доработке программно-аппаратных средств защиты информации
	Оформлять документацию по процессу обслуживания программно-аппаратных средств защиты информации
	Выполнять проверку настроек и режимов работы программно-аппаратных средств защиты информации
Необходимые знания	Защитные механизмы и средства обеспечения сетевой безопасности
	Основы построения защищенных компьютерных сетей
	Основные средства и методы анализа программных реализаций
	Принципы работы и правила эксплуатации приобретаемых программно-аппаратных средств защиты информации
	Методы измерений, контроля и технических расчетов характеристик программно-аппаратных средств защиты информации
Другие характеристики	-

### 3.3. Обобщенная трудовая функция

Наименование	Разработка и применение методов оценивания безопасности компьютерных систем и сетей	Код	С	Уровень квалификации	7
--------------	---	-----	---	----------------------	---

Происхождение обобщенной трудовой функции

Оригинал	X	Заемствовано 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
--	--

Требования к образованию и обучению	Высшее образование – магистратура или специалитет по УГС (направлению подготовки) «Информационная безопасность», дополнительное профессиональное образование или повышение квалификации по программам обучения, связанным с проведением экспертизы безопасности компьютерных систем
Требования к опыту практической работы	-
Особые условия допуска к работе	Наличие допуска к сведениям, составляющим государственную тайну <sup>3</sup> ;

	наличие допуска к работе на электроустановках (не ниже III группы электробезопасности) <sup>4</sup>
Другие характеристики	-

## Дополнительные характеристики

Наименование документа	Код	Наименование базовой группы, должности (профессии) или специальности
ОКЗ	2523	Специалисты по компьютерным сетям
	251	Разработчики и аналитики программного обеспечения и приложений
ЕКС	-	Инженер-программист по технической защите информации
	-	Администратор по обеспечению безопасности информации
	-	Специалист по технической защите информации
ОКПДТР	26579	Специалист по защите информации
	40070	Администратор информационной безопасности вычислительной сети
ОКСО	10.04.01	Информационная безопасность
	10.05.01	Компьютерная безопасность

**3.3.1. Трудовая функция**

Наименование	Проведение контрольных проверок работоспособности и эффективности применяемых программно-аппаратных средств защиты информации	Код	C/0 1.7	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	Оценивать работоспособность программно-аппаратных средств защиты информации
	Оценивать эффективность программно-аппаратных средств 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	Стандарты оценивания защищенности компьютерных систем и сетей

	Принципы построения защищенных компьютерных систем
	Нормативно-правовые основания для проведения, методические материалы по проведению, порядок оформления заявок на проведение, порядок организации, порядок анализа и реализации результатов контрольно-технических мероприятий по оценке защищенности
	Возможности и особенности использования специализированных программно-аппаратных средств при проведении контрольно-технических мероприятий по оценке защищенности
	Методы статистического анализа данных
	Способы анализа применяемых методов и средств защиты информации на предмет соответствия политике безопасности
Другие характеристики	-

### 3.3.2. Трудовая функция

Наименование	Разработка требований по защите, формирование политик безопасности компьютерных систем и сетей	Код	C/0 2.7	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
Необходимые умения	Разработка руководящих документов по защите информации в организации
	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
Необходимые знания	Формировать политики безопасности компьютерных систем и сетей
	Стандарты оценивания защищенности компьютерных систем и сетей
	Принципы построения защищенных компьютерных систем и сетей
	Модели безопасности компьютерных систем
	Виды политик безопасности компьютерных систем и сетей
	Нормативно-правовые акты и методические документы уполномоченных федеральных органов исполнительной власти в области информационной безопасности
	Международные стандарты и практики по менеджменту, аудиту и оценке рисков информационной безопасности
Возможности используемых и планируемых к использованию средств защиты информации	
Другие характеристики	-

### 3.3.3. Трудовая функция

Наименование	Проведение криминалистического анализа компьютерных систем	Код	C/0 3.7	Уровень (подуровень) квалификации	7
--------------	--	-----	------------	-----------------------------------	---

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

Трудовые действия	Выполнение анализа компьютерной системы с целью определения уровня защищенности и доверия
	Подготовка аналитического отчета по результатам проведенного анализа и формулировка предложений по устранению выявленных уязвимостей
	Применение нормативных и правовых актов при проведении криминалистической экспертизы и криминалистического анализа
Необходимые умения	Анализировать компьютерную систему с целью определения уровня защищенности и доверия
	Готовить аналитический отчет по результатам проведенного анализа и формулировать предложения по устранению выявленных уязвимостей
	Применять нормативные и правовые акты при проведении криминалистической экспертизы и криминалистического анализа
Необходимые знания	Стандарты оценивания защищенности компьютерных систем и сетей
	Принципы построения защищенных распределенных компьютерных систем
	Принципы построения систем обнаружения компьютерных атак
	Способы обнаружения и нейтрализации последствий вторжений в компьютерные системы
	Методы проведения расследования компьютерных инцидентов
	Основные нормативно-правовые акты и методические документы уполномоченных федеральных органов исполнительной власти в области информационной безопасности.
Другие характеристики	-

### 3.3.4. Трудовая функция

Наименование	Выполнение экспериментально-исследовательских работ при проведении сертификации программно-аппаратных средств защиты информации и анализ результатов	Код	C/0 4.7	Уровень (подуровень) квалификации	7
--------------	--	-----	------------	-----------------------------------	---

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

Трудовые действия	Проведение теоретических и экспериментальных исследований уровней защищенности и доверия компьютерных систем и сетей
-------------------	--

	Проведение сертификационных испытаний с использованием современных инструментальных средств
	Подготовка аналитического отчета по результатам проведенных сертификационных испытаний и 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 современные инструментальные средства проведения сертификационных испытаний
	Готовить аналитический отчет по результатам проведенных сертификационных испытаний и формулировать выводы по оценке защищенности
Необходимые знания	Стандарты оценивания защищенности компьютерных систем
	Национальные стандарты на проведение научно-исследовательских и опытно-конструкторских работ, сертификационные испытания и создание систем защиты информации
	Способы организации экспериментально-исследовательских работ при проведении сертификации программно-аппаратных средств защиты
Другие характеристики	-

### 3.3.5. Трудовая функция

Наименование	Проведение экспериментально-исследовательских работ при аттестации объектов с учетом требований к обеспечению защищенности	Код	C/0 5.7	Уровень (подуровень) квалификации	7
--------------	--	-----	------------	-----------------------------------	---

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

Трудовые действия	Проведение проверки объекта информатизации на соответствие организационно-техническим требованиям по защите информации
	Проведение испытаний объекта информатизации на соответствие требованиям по защите информации от утечки по техническим каналам
	Проведение испытаний объекта информатизации на соответствие требованиям по защите информации от несанкционированного доступа (НСД)
	Проведение комплексных испытаний с целью оценки соответствия использованного комплекса мер и средств защиты требуемому уровню безопасности информации
	Подготовка отчетной документации и оценка результатов испытаний аттестуемых объектов
	Оформление результатов аттестационных испытаний в виде протоколов испытаний
	Оформление заключения о соответствии объектов информатизации требованиям по безопасности информации

Необходимые умения	Анализировать объекты информатизации с целью определения уровня защищенности
	Применять нормативно-правовые акты, руководящие и методические документы уполномоченных федеральных органов исполнительной власти в области информационной безопасности по аттестации объектов с учетом требований к обеспечению защищенности компьютерной системы
	Выполнять испытания использованного комплекса мер и средств защиты
	Оформлять документально результаты испытания.
	Выполнять оценку результатов испытаний на основании требований по защите информации
Необходимые знания	Способы обеспечения защищенности объектов информатизации
	Организационно-технические требования по защите информации
	Требования по защите информации от утечки по техническим каналам
	Требования по защите информации от несанкционированного доступа
	Программно-математические методы анализа защищенности объектов информатизации
	Порядок ведения протоколов аттестационных испытаний
	Порядок оформления заключений по результатам аттестационных испытаний
Принципы построения защищенных объектов информатизации	
Другие характеристики	-

### 3.3.6. Трудовая функция

Наименование	Проведение инструментального мониторинга защищенности компьютерных систем и сетей	Код	С/0 6.7	Уровень (подуровень) квалификации	7
--------------	---	-----	------------	-----------------------------------	---

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

Трудовые действия	Использование инструментария защищенных компьютерных систем, в том числе сканеров безопасности
	Выполнение анализа защищенности сетевых сервисов с использованием средств автоматического реагирования на попытки НСД к ресурсам компьютерных систем и сетей
	Составление отчетов по результатам проверок
Необходимые умения	Формализовать задачу управления безопасностью компьютерных систем
	Применять современные инструментальные средства проведения мониторинга защищенности компьютерных систем
Необходимые знания	Принципы построения защищенных компьютерных систем
	Принципы построения систем обнаружения компьютерных атак
	Методы обработки данных мониторинга безопасности компьютерных систем
	Программно-математические методы анализа защищенных компьютерных систем

	Способы обнаружения и нейтрализации последствий вторжений в компьютерные системы
Другие характеристики	-

### 3.3.7. Трудовая функция

Наименование	Проведение экспертизы при расследовании компьютерных преступлений, правонарушений и инцидентов	Код	С/0 7.7	Уровень (подуровень) квалификации	7
--------------	--	-----	------------	-----------------------------------	---

Происхождение трудовой функции	Оригинал	X	Заемствовано из оригинала		
				Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Классификация и определение свойств аппаратных средств в составе компьютерной системы, определение их фактического и первоначального состояния
	Диагностика технологии изготовления, причин и условий изменения свойств (эксплуатационных режимов) аппаратных средств в составе компьютерной системы
	Определение структуры механизма и обстоятельств события за счет использования выявленных аппаратных средств
	Классификация и определение характеристик операционной системы, используемых технологий системного программирования
	Выявление, исследование функциональных свойств и состояния программного обеспечения
	Исследование алгоритма программного продукта, типов поддерживаемых аппаратных платформ
	Определение причин, целей и условий изменения свойств и состояния программного обеспечения
	Индивидуальное отождествление оригинала программы (инсталляционной версии) и ее копии на носителях данных компьютерной системы
	Установление групповой принадлежности программного обеспечения
	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 и обстоятельства события
	Определять причину и условия изменения программного обеспечения
	Выделять свойства и признаки информации, позволяющие определить ее принадлежность определенному источнику
	Выявлять возможные траектории изменения информации
	Выявлять несоответствия имеющейся информации ее расположению в системе
	Прогнозировать возможные пути развития новых видов компьютерных преступлений, правонарушений и инцидентов
Необходимые знания	Уязвимости защищенных компьютерных систем
	Способы обнаружения и нейтрализации последствий вторжений в компьютерные системы
	Методы проведения расследования компьютерных преступлений, правонарушений и инцидентов
	Методы анализа остаточной информации и поиска следов для фиксации компьютерных инцидентов.
	Основные нормативно-правовые акты и методические документы уполномоченных федеральных органов исполнительной власти в области информационной безопасности.
	Форматы хранения информации в анализируемой компьютерной системе
	Основные форматы файлов, используемые в компьютерных системах
	Особенности хранения конфигурационной и системной информации в компьютерных системах
	Методы статистического анализа данных
	Методы корреляционного и регрессионного анализа
	Криптографические алгоритмы и особенности их программной реализации

### 3.4. Обобщенная трудовая функция

Наименование	Проектирование специальных технических и программно-математических 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(группы)
--	--

Требования к образованию и обучению	Высшее образование – магистратура или специалитет по УГС (направлению подготовки) «Информационная безопасность»
-------------------------------------	---

Требования к опыту практической работы	Наличие опыта работы не менее 5 лет по применению и анализу эффективности средств защиты информации компьютерных систем
Особые условия допуска к работе	Наличие допуска к сведениям, составляющим государственную тайну <sup>3</sup> ; наличие допуска к работе на электроустановках (не ниже III группы электробезопасности) <sup>4</sup>
Другие характеристики	-

## Дополнительные характеристики

Наименование документа	Код	Наименование базовой группы, должности (профессии) или специальности
ОКЗ	1223	Руководители подразделений по научным исследованиям и разработкам
	1330	Руководители служб в сфере информационно-коммуникационных технологий
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	20911	Главный специалист по защите информации
	46115	Руководитель аналитической группы подразделения по комплексной защите информации
	46155	Руководитель группы подразделения по комплексной защите информации
ОКСО	10.04.01	Информационная безопасность
	10.05.01	Компьютерная безопасность
ОКСВНК <sup>8</sup>	10.06.01	Информационная безопасность
	10.07.01	Информационная безопасность

## 3.4.1. Трудовая функция

Наименование	Разработка требований к специальным техническим средствам защиты информации компьютерных систем с учетом действующих нормативных и методических документов	Код	D/0 1.8	Уровень (подуровень) квалификации	8
--------------	--	-----	------------	-----------------------------------	---

Происхождение трудовой функции	Оригинал	<input checked="" type="checkbox"/>	Заимствовано из оригинала	<input type="checkbox"/>	<input type="checkbox"/>
				Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Определение угроз безопасности, возможных источников и каналов утечки информации
	Выработка и принятие решений и мер по обеспечению защиты информации
	Оценка технико-экономического уровня и эффективности предлагаемых и реализуемых технических решений

Необходимые умения	Обобщать научно-техническую литературу, нормативные и методические материалы по техническим средствам и способам защиты информации
	Разрабатывать 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 отечественные и зарубежные стандарты в области компьютерной безопасности для оценки защищенности компьютерной системы
	Применять действующую законодательную базу в области обеспечения компьютерной безопасности
Необходимые знания	Нормативно-правовые акты и методические документы уполномоченных федеральных органов исполнительной власти, связанные с обеспечением технической защиты информации
	Порядок организации работ по защите информации
	Методы и средства получения, обработки и передачи информации в современных операционных системах, системах управления базами данных и компьютерных сетях
	Программно-математические методы защиты информации
	Теоретико-числовые методы и алгоритмы, применяемые в средствах защиты информации
	Виды атак и механизмы их реализации в компьютерных системах
	Методы противодействия техническим разведкам при эксплуатации компьютерных систем
	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
Типовые криптографические протоколы и стандарты	
Другие характеристики	Наличие опыта работы не менее 5 лет по применению и анализу эффективности средств защиты информации компьютерных систем

### 3.4.2. Трудовая функция

Наименование	Проектирование программных и аппаратных средств защиты информации компьютерных систем и сетей		Код	D/0 2.8	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, планов и графиков проведения работ по защите информации					

	Анализ существующих методов и средств, применяемых для контроля и защиты информации, и разработка предложения по их совершенствованию и повышению эффективности этой защиты
	Создание 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 и зарубежные стандарты в области компьютерной безопасности для проектирования средств защиты информации компьютерной системы
	Разрабатывать архитектуру средств защиты информации
	Подбирать и обобщать научно-техническую литературу, нормативно-правовые и методические материалы по программным и аппаратным средствам и способам защиты информации
Необходимые знания	Нормативно-правовые акты и методические документы уполномоченных федеральных органов исполнительной власти, связанные с обеспечением технической защиты информации
	Методы и средства получения, обработки и передачи информации в современных 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
	Программно-математические методы защиты информации
	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	
Другие характеристики	Наличие опыта работы не менее 5 лет по применению и анализу эффективности средств защиты информации компьютерных систем

### 3.4.3. Трудовая функция

Наименование	Разработка, отладка и тестирование средств защиты информации компьютерных систем и сетей	Код	D/0 3.8	Уровень (подуровень) квалификации	8
--------------	--	-----	------------	-----------------------------------	---

Происхождение трудовой функции	Оригинал	X	Заемствовано из оригинала		
				Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Разработка средств защиты информации в соответствии с техническим заданием
-------------------	--

	Разработка и исследование специальных технических и 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 технических средств защиты информации
Необходимые умения	Использовать приемы защитного программирования
	Использовать приемы защиты от типовых атак компьютерных систем
	Создавать программный код на выбранном языке с использованием среды программирования и средств СУБД
	Применять методы и приемы отладки
	Применять методы и средства тестирования
Необходимые знания	Методические и нормативные материалы по вопросам, связанным с обеспечением технической защиты информации
	Методы и средства получения, обработки и передачи информации в современных операционных системах, системах управления базами данных и компьютерных сетях
	Методы и средства защиты информации в компьютерных сетях, операционных системах и системах управления базами данных
	Программно-математические методы защиты информации
	Виды атак и механизмы их реализации в компьютерных системах
	Принципы построения систем защиты информации компьютерных систем
	Методологии и технологии разработки программного и аппаратного обеспечения
Другие характеристики	Наличие опыта работы не менее 5 лет по применению и анализу эффективности средств защиты информации компьютерных систем

#### 3.4.4. Трудовая функция

Наименование	Сопровождение разработки средств защиты информации компьютерных систем и сетей	Код	D/0 4.8	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, обеспечение их соответствия действующим нормативным и методическим документам
	Создание рекомендаций и предложений по совершенствованию и повышению эффективности защиты информации
	Составление и оформлении разделов научно-технических отчетов
	Определение потребности в технических средствах защиты и контроля, составление заявок на их приобретение с необходимыми обоснованиями и расчетами к ним
	Подготовка предложений по заключению соглашений и договоров с другими учреждениями, организациями и предприятиями,

	предоставляющими услуги в области технических средств защиты информации
	Выполнение аттестации программ и алгоритмов на предмет соответствия требованиям защиты информации
	Выполнение контрольных проверок работоспособности и эффективности систем и технических средств защиты информации
	Анализ существующих методов и средств, применяемых для контроля и защиты информации, и разработка предложения по их совершенствованию и повышению эффективности этой защиты
	Подготовка проектов нормативных и методических материалов, регламентирующих работу по защите информации, а также положений, инструкций и других организационно-распорядительных документов
	Методическое руководство и контроль над работой по оценке технико-экономического уровня разрабатываемых мер по защите информации
	Контроль над выполнением требований нормативно-технической документации, за соблюдением установленного порядка выполнения работ, а также действующего законодательства при решении вопросов, касающихся защиты информации
	Организация проведения специальных исследований и контрольных проверок по выявлению демаскирующих признаков и возможных каналов утечки информации, в том числе по техническим каналам
Необходимые умения	Разрабатывать модели угроз и модели нарушителя безопасности компьютерных систем
	Разрабатывать частные политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками
	Применять отечественные и зарубежные стандарты в области защиты информации
	Применять действующую законодательную базу в области обеспечения защиты информации
Необходимые знания	Нормативно-правовые акты и методические документы уполномоченных федеральных органов исполнительной власти, связанные с обеспечением технической защиты информации
	Методы и средства получения, обработки и передачи информации
	Методы выявления каналов возможной 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 технических средств передачи, обработки, отображения и хранения информации
	Методы и средства защиты информации в компьютерных сетях, операционных системах и системах управления базами данных
	Программно-математические методы защиты информации
	Теоретико-числовые методы и алгоритмы, применяемые в средствах защиты информации
	Виды атак и механизмы их реализации в компьютерных системах
	Принципы построения систем защиты информации компьютерных систем
	Формальные модели управления доступом
Типовые криптографические протоколы и стандарты	

Другие характеристики	Наличие опыта работы не менее 5 лет по применению и анализу эффективности средств защиты информации компьютерных систем
-----------------------	---

#### IV. Сведения об организациях-разработчиках профессионального стандарта

##### 4.1. Ответственная организация – разработчик

Закрытое акционерное общество «Ассоциация специалистов информационных систем», город Санкт-Петербург
(наименование организации)
Генеральный директор Солодянников Александр Владимирович (должность и ФИО руководителя)

##### 4.2. Наименования организаций – разработчиков

1	Межрегиональная общественная организация «Ассоциация защиты информации», город Москва
2	Федеральное учебно-методическое объединение по укрупненной группе специальностей и направлений подготовки «Информационная безопасность»
3	Федеральное государственное казенное образовательное учреждение высшего профессионального образования «Академия Федеральной службы безопасности Российской Федерации» (Академия ФСБ России), город Москва

<sup>1</sup> Общероссийский классификатор занятий.

<sup>2</sup> Общероссийский классификатор видов экономической деятельности ОКВЭД ОК 029-2014 (утв. Приказом Росстандарта от 31.01.2014 №14-ст).

<sup>3</sup> Закон Российской Федерации от 21 июля 1993 г. № 5485-1 «О государственной тайне», Инструкция №3-1 Утверждена Постановлением Правительства РФ №1 от 5.01.2004 г.

<sup>4</sup> Приказ Минтруда России от 24.07.2013 N 328н "Об утверждении Правил по охране труда при эксплуатации электроустановок"

<sup>5</sup> Единый квалификационный справочник должностей руководителей, специалистов и служащих.

<sup>6</sup> Общероссийский классификатор профессий рабочих, должностей служащих и тарифных разрядов.

<sup>7</sup> Общероссийский классификатор специальностей по образованию.

<sup>8</sup> Общероссийский классификатор специальностей высшей научной квалификации.