



МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ

**ЗАРЕГИСТРИРОВАНО**

Регистрационный № 71784

от "22" декабря 2022 г.

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

**ПРИКАЗ**

28 ноября 2022 г.

Москва

№ 739н

**Об утверждении профессионального стандарта  
«Специалист по информационной безопасности в кредитно-финансовой сфере»**

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), п р и к а з ы в а ю:

1. Утвердить прилагаемый профессиональный стандарт «Специалист по информационной безопасности в кредитно-финансовой сфере».

2. Установить, что настоящий приказ вступает в силу с 1 сентября 2023 г. и действует до 1 сентября 2029 г.

Министр

А.О. Котяков

УТВЕРЖДЕН  
приказом Министерства  
труда и социальной защиты  
Российской Федерации  
от «28» ноября 2022 г. № 439Н

# ПРОФЕССИОНАЛЬНЫЙ СТАНДАРТ

**Специалист по информационной безопасности в кредитно-финансовой сфере**

1593

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.....	6
3.1. Обобщенная трудовая функция «Обеспечение функционирования систем и средств защиты информации в организациях кредитно-финансовой сферы».....	6
3.2. Обобщенная трудовая функция «Управление инцидентами информационной безопасности в организациях кредитно-финансовой сферы» .....	11
3.3. Обобщенная трудовая функция «Аналитическое и организационное сопровождение деятельности по управлению рисками информационной безопасности в организациях кредитно-финансовой сферы» .....	17
3.4. Обобщенная трудовая функция «Методологическое обеспечение процессов информационной безопасности в организациях кредитно-финансовой сферы» .....	31
3.5. Обобщенная трудовая функция «Контроль обеспечения информационной безопасности и обеспечение операционной надежности (киберустойчивости) в организациях кредитно-финансовой сферы» .....	40
3.6. Обобщенная трудовая функция «Организация процессов обеспечения информационной безопасности в организациях кредитно-финансовой сферы» .....	45
IV. Сведения об организациях – разработчиках профессионального стандарта.....	54

## I. Общие сведения

Обеспечение информационной безопасности в организациях кредитно-финансовой сферы (далее – КФС)

(наименование вида профессиональной деятельности)

06.053

код

Основная цель вида профессиональной деятельности:

Управление рисками информационной безопасности, обеспечение защиты информации, операционной надежности (киберустойчивости) в организациях КФС

Группа занятий:

1330	Руководители служб и подразделений в сфере информационно-коммуникационных технологий	2529	Специалисты по базам данных и сетям, не входящие в другие группы
(код ОКЗ <sup>1</sup> )	(наименование)	(код ОКЗ)	(наименование)

Отнесение к видам экономической деятельности:

74.90.99	Деятельность в области защиты информации прочая
62.02.9	Деятельность консультативная в области компьютерных технологий прочая
66	Деятельность вспомогательная в сфере финансовых услуг и страхования
(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	Обеспечение функционирования систем и средств защиты информации в организациях КФС	6	Проведение работ по установке, настройке и техническому обслуживанию систем и средств защиты информации в организациях КФС	A/01.6	6
			Администрирование систем и средств защиты информации в организациях КФС	A/02.6	
			Реализация процессов обеспечения операционной надежности (киберустойчивости) в организациях КФС	A/03.6	
В	Управление инцидентами информационной безопасности в организациях КФС	7	Выявление и регистрация инцидентов информационной безопасности, в том числе обнаружение компьютерных атак, в организациях КФС	B/01.7	7
			Реагирование на инциденты информационной безопасности в организациях КФС	B/02.7	
			Восстановление функционирования бизнес-процессов и технологических процессов и объектов информатизации после реализации инцидентов информационной безопасности в организациях КФС	B/03.7	
С	Аналитическое и организационное сопровождение деятельности по управлению рисками информационной безопасности в организациях КФС	7	Определение угроз информационной безопасности в организациях КФС	C/01.7	7
			Выявление, идентификация и оценка рисков информационной безопасности в организациях КФС	C/02.7	
			Сбор и регистрация информации о выявленных рисках информационной безопасности в организациях КФС	C/03.7	
			Разработка мероприятий, направленных на уменьшение негативного влияния рисков информационной безопасности в организациях КФС	C/04.7	
			Мониторинг рисков информационной безопасности и контроль показателей уровня рисков информационной безопасности в организациях КФС	C/05.7	

			Обеспечение информационной безопасности значимых объектов критической информационной инфраструктуры в организациях КФС	C/06.7	7
			Организация защиты информации, в том числе защиты персональных данных, в организациях КФС	C/07.7	7
			Обеспечение операционной надежности (киберустойчивости) в организациях КФС	C/08.7	7
D	Методологическое обеспечение процессов информационной безопасности в организациях КФС	7	Разработка политики в области обеспечения информационной безопасности, по вопросам управления рисками информационной безопасности, обеспечения операционной надежности (киберустойчивости) и защиты информации в организациях КФС	D/01.7	7
			Разработка методологии обеспечения защиты информации и операционной надежности (киберустойчивости) в организациях КФС	D/02.7	7
			Разработка методологии управления рисками информационной безопасности в организациях КФС	D/03.7	7
			Разработка методологии выявления инцидентов информационной безопасности, реагирования на них и восстановления после их реализации в организациях КФС	D/04.7	7
E	Контроль обеспечения информационной безопасности и обеспечение операционной надежности (киберустойчивости) в организациях КФС	7	Проведение контрольных проверок работоспособности и оценка эффективности применяемых программно-аппаратных средств защиты информации в организациях КФС	E/01.7	7
			Контроль процессов защиты информации и обеспечения операционной надежности (киберустойчивости) в организациях КФС	E/02.7	7
			Реализация программ повышения осведомленности организаций КФС по вопросам защиты информации и обеспечения операционной надежности (киберустойчивости) в организациях КФС	E/03.7	7
F	Организация процессов обеспечения информационной безопасности в организациях КФС	8	Организация управления рисками информационной безопасности на высшем управленческом уровне в организациях КФС	F/01.8	8
			Организация обеспечения защиты информации и операционной надежности (киберустойчивости) на высшем управленческом уровне в организациях КФС	F/02.8	8

			Контроль процедур управления рисками информационной безопасности и обеспечения защиты информации и операционной надежности (киберустойчивости) на высшем управленческом уровне в организациях КФС	F/03.8	8
			Совершенствование системы управления рисками информационной безопасности, обеспечение защиты информации и операционной надежности (киберустойчивости) на высшем управленческом уровне в организациях КФС	F/04.8	8

### III. Характеристика обобщенных трудовых функций

#### 3.1. Обобщенная трудовая функция

Наименование	Обеспечение функционирования систем и средств защиты информации в организациях КФС	Код	А	Уровень квалификации	6
--------------	--	-----	---	----------------------	---

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

Возможные наименования должностей, профессий	<p>Инженер по защите информации</p> <p>Специалист по защите информации I категории</p> <p>Специалист по защите информации II категории</p> <p>Специалист по защите информации</p> <p>Инженер-программист по технической защите информации I категории</p> <p>Инженер-программист по технической защите информации II категории</p> <p>Инженер-программист по технической защите информации</p> <p>Инженер-программист I категории</p> <p>Инженер-программист II категории</p> <p>Инженер-программист III категории</p> <p>Инженер-программист</p>
--	---

Требования к образованию и обучению	Высшее образование – бакалавриат в области информационной безопасности
Требования к опыту практической работы	Для должностей с категорией – опыт работы в должности с более низкой (предшествующей) категорией не менее одного года
Особые условия допуска к работе	-
Другие характеристики	-

#### Дополнительные характеристики

Наименование документа	Код	Наименование базовой группы, должности (профессии) или специальности
ОКЗ	2529	Специалисты по базам данных и сетям, не входящие в другие группы
ЕКС <sup>3</sup>	-	Администратор по обеспечению безопасности информации
	-	Инженер по защите информации
	-	Специалист по защите информации
	-	Инженер-программист по технической защите информации
ОКПДТР <sup>4</sup>	22567	Инженер по защите информации
	26579	Специалист по защите информации
ОКСО <sup>5</sup>	2.10.03.01	Информационная безопасность

## 3.1.1. Трудовая функция

Наименование	Проведение работ по установке, настройке и техническому обслуживанию систем и средств защиты информации в организациях КФС	Код	A/01.6	Уровень (подуровень) квалификации	6
--------------	--	-----	--------	-----------------------------------	---

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

Трудовые действия	Установка и монтаж систем и средств защиты информации, в том числе средств криптографической защиты информации (далее – СКЗИ), в организациях КФС
	Настройка программных (программно-аппаратных) средств защиты информации, в том числе СКЗИ, в организациях КФС
	Испытания систем и средств защиты информации в организациях КФС
	Обнаружение и исправление ошибок в конфигурации программных средств защиты информации в организациях КФС
	Техническое обслуживание систем и средств защиты информации, в том числе СКЗИ, в организациях КФС
	Обнаружение и устранение неисправностей в работе программно-аппаратных (технических) средств защиты информации в организациях КФС
Необходимые умения	Производить установку и монтаж систем и средств защиты информации, в том числе СКЗИ, в соответствии с инструкциями по эксплуатации и эксплуатационно-техническими документами
	Производить настройку программных (программно-аппаратных) средств защиты информации, в том числе СКЗИ, в соответствии с инструкциями по эксплуатации и эксплуатационно-техническими документами
	Проводить испытания систем и средств защиты информации в соответствии с инструкциями по эксплуатации и эксплуатационно-техническими документами
	Производить обнаружение и исправление ошибок в конфигурации программных средств защиты информации
	Производить техническое обслуживание систем и средств защиты информации в соответствии с инструкциями по эксплуатации и эксплуатационно-технической документацией
	Производить устранение выявленных неисправностей программно-аппаратных (технических) средств защиты информации и при необходимости организовывать их ремонт
Необходимые знания	Законодательство Российской Федерации, нормативные правовые акты, национальные, межгосударственные и международные стандарты в области защиты информации
	Руководящие и методические документы уполномоченных федеральных органов исполнительной власти, нормативные акты Банка России в области защиты информации
	Современные информационные технологии (операционные системы, базы данных, вычислительные сети)
	Угрозы безопасности информации в автоматизированных системах



	Методы и средства защиты информации, в том числе СКЗИ, в автоматизированных системах
	Организационно-распорядительные документы по защите информации в автоматизированных системах в организациях КФС
	Технические описания и инструкции (руководства) по эксплуатации систем и средств защиты информации, в том числе СКЗИ, в автоматизированных системах
	Порядок организации технического обслуживания систем и средств защиты информации в соответствии с инструкциями и эксплуатационно-технической документацией
	Порядок устранения неисправностей и организации ремонта программно-аппаратных (технических) средств защиты информации
Другие характеристики	-

### 3.1.2. Трудовая функция

Наименование	Администрирование систем и средств защиты информации в организациях КФС	Код	A/02.6	Уровень (подуровень) квалификации	6
--------------	---	-----	--------	-----------------------------------	---

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

Трудовые действия	Определение состава и порядка применения программно-аппаратных средств защиты информации в организациях КФС
	Конфигурирование программно-аппаратных средств защиты информации в операционных системах в организациях КФС
	Контроль корректности функционирования программно-аппаратных средств защиты информации в операционных системах в организациях КФС
	Управление правами пользователей автоматизированной системы в организациях КФС
	Обеспечение безопасности информации с учетом требования эффективного функционирования автоматизированной системы в организациях КФС
	Управление антивирусной защитой операционных систем в соответствии с действующими требованиями в организациях КФС
	Контроль соблюдения требований к защите информации при установке программного обеспечения, включая антивирусное программное обеспечение, в организациях КФС
Необходимые умения	Планировать политику безопасности компонентов (операционных систем, баз данных, компьютерных сетей, программных систем) автоматизированной системы в организациях КФС
	Оценивать угрозы безопасности информации в организациях КФС
	Устанавливать и настраивать операционные системы, системы управления базами данных, компьютерные сети и прикладное программное обеспечение с учетом требований по обеспечению защиты информации

	<p>Противодействовать угрозам безопасности информации с использованием встроенных средств защиты информации операционных систем</p> <p>Выбирать режимы работы программно-аппаратных средств защиты информации в операционных системах</p> <p>Настраивать антивирусные средства защиты информации в операционных системах</p> <p>Устанавливать обновления программного обеспечения и средств антивирусной защиты</p> <p>Проводить мониторинг функционирования программно-аппаратных средств защиты информации</p> <p>Оценивать оптимальность выбора программно-аппаратных средств защиты информации и их режимов функционирования в операционных системах</p>
Необходимые знания	<p>Законодательство Российской Федерации, нормативные правовые акты, национальные, межгосударственные и международные стандарты в области защиты информации</p> <p>Руководящие и методические документы уполномоченных федеральных органов исполнительной власти, нормативные акты Банка России в области защиты информации</p> <p>Принципы формирования политики информационной безопасности в автоматизированных системах в организациях КФС</p> <p>Принципы построения и функционирования современных операционных систем, систем управления базами данных и компьютерных сетей</p> <p>Программно-аппаратные средства обеспечения безопасности информации в типовых операционных системах, системах управления базами данных, компьютерных сетях</p> <p>Основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности информации в автоматизированных системах</p> <p>Принципы организации и структура подсистем защиты современных операционных систем, систем управления базами данных и компьютерных сетей</p> <p>Порядок реализации методов и средств антивирусной защиты в операционных системах</p> <p>Принципы работы и правила эксплуатации программно-аппаратных средств защиты информации</p> <p>Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации и обеспечению безопасности критической информационной инфраструктуры</p> <p>Основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические, технические) в организациях КФС</p>
Другие характеристики	-

## 3.1.3. Трудовая функция

Наименование	Реализация процессов обеспечения операционной надежности (киберустойчивости) в организациях КФС	Код	A/03.6	Уровень (подуровень) квалификации	6
--------------	---	-----	--------	-----------------------------------	---

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

Трудовые действия	Реализация и совершенствование процессов обеспечения операционной надежности (киберустойчивости) в организациях КФС
	Формирование отчетности о защите информации и об обеспечении операционной надежности (кибербезопасности) в организации КФС
	Обеспечение необходимого уровня зрелости (полноты и качества) процессов обеспечения операционной надежности (киберустойчивости) в организациях КФС
Необходимые умения	Анализировать и применять методологическую базу, требования законодательства Российской Федерации, нормативных актов Банка России, международных и национальных стандартов в области обеспечения операционной надежности (киберустойчивости) в организациях КФС
	Разрабатывать предложения по совершенствованию методологии обеспечения операционной надежности (киберустойчивости) в организациях КФС
	Применять организационные и технические меры обеспечения операционной надежности (киберустойчивости) в организациях КФС
	Вносить предложения об изменении контрольных показателей уровня рисков информационной безопасности в организациях КФС
	Анализировать техническую документацию на объектах информатизации в организациях КФС
Необходимые знания	Законодательство Российской Федерации, нормативные правовые акты, национальные, межгосударственные и международные стандарты в области защиты информации, реализации и контроля процессов обеспечения операционной надежности (киберустойчивости) в организациях КФС
	Руководящие и методические документы уполномоченных федеральных органов исполнительной власти, нормативные акты Банка России в области защиты информации, реализации и контроля процессов обеспечения операционной надежности (киберустойчивости) в организациях КФС
	Принципы обеспечения операционной надежности (киберустойчивости) в организациях КФС
	Базовый состав организационных, технологических и технических мер обеспечения операционной надежности (киберустойчивости) в организациях КФС
	Подходы к сегментации вычислительных сетей в организациях КФС
	Специфика платежных процессов в организациях КФС
	Основы обеспечения безопасности объектов информатизации прикладного уровня в организациях КФС

	Подходы к подтверждению реализации функций безопасности и контроля (наличия) уязвимостей объектов информатизации прикладного уровня в организациях КФС
Другие характеристики	-

### 3.2. Обобщенная трудовая функция

Наименование	Управление инцидентами информационной безопасности в организациях КФС	Код	В	Уровень квалификации	7
--------------	---	-----	---	----------------------	---

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

Возможные наименования должностей, профессий	Специалист по информационной безопасности Ведущий специалист по защите информации
--	--

Требования к образованию и обучению	Высшее образование – специалитет или магистратура в области информационной безопасности
Требования к опыту практической работы	-
Особые условия допуска к работе	-
Другие характеристики	-

#### Дополнительные характеристики

Наименование документа	Код	Наименование базовой группы, должности (профессии) или специальности
ОКЗ	2529	Специалисты по базам данных и сетям, не входящие в другие группы
ЕКС	-	Администратор по обеспечению безопасности информации
	-	Инженер по защите информации
	-	Инженер-программист по технической защите информации
	-	Специалист по обеспечению безопасности информации в ключевых системах информационной инфраструктуры
ОКПДТР	22567	Инженер по защите информации
	26579	Специалист по защите информации
ОКСО	2.10.04.01	Информационная безопасность
	2.10.05.01	Компьютерная безопасность
	2.10.05.02	Информационная безопасность телекоммуникационных систем
	2.10.05.03	Информационная безопасность автоматизированных систем

	2.10.05.04	Информационно-аналитические системы безопасности
	2.10.05.05	Безопасность информационных технологий в правоохранительной сфере
	2.10.05.06	Криптография
	2.10.05.07	Противодействие техническим разведкам

### 3.2.1. Трудовая функция

Наименование	Выявление и регистрация инцидентов информационной безопасности, в том числе обнаружение компьютерных атак, в организациях КФС	Код	В/01.7	Уровень (подуровень) квалификации	7
--------------	---	-----	--------	-----------------------------------	---

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

Трудовые действия	Оперативный мониторинг и выявление событий информационной безопасности, в том числе обнаружение компьютерных атак, в организациях КФС
	Сбор данных для регистрации событий информационной безопасности, в том числе компьютерных атак, в организациях КФС
	Обеспечение функционирования механизмов и инициативного информирования подразделений, ответственных за управление рисками информационной безопасности, работников организаций КФС о событиях информационной безопасности в организациях КФС
	Организация и выполнение деятельности по получению и использованию сведений об актуальных индикаторах компрометации объектов информатизации в организациях КФС
	Автоматизация процедур выявления наличия индикаторов компрометации в организациях КФС
	Сбор и регистрация информации об инцидентах информационной безопасности в организациях КФС
Необходимые умения	Анализировать и применять методологическую базу, требования законодательства Российской Федерации, нормативных актов Банка России, международных и национальных стандартов в области защиты информации, обеспечения информационной безопасности, управления рисками информационной безопасности в организациях КФС, а также обнаружения, предупреждения и ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры организаций КФС, и реагирования на компьютерные инциденты
	Настраивать средства (агенты, интерфейсы) сбора технических данных для выявления событий информационной безопасности в организациях КФС, в том числе для обнаружения компьютерных атак
	Осуществлять работу с техническими средствами защиты информации и системами, реализующими функции управления инцидентами информационной безопасности в организациях КФС