

УТВЕРЖДЕН
приказом Министерства
труда и социальной защиты Российской
Федерации
от «___» _____ 201__ г. №___

ПРОФЕССИОНАЛЬНЫЙ СТАНДАРТ

**Специалист по информационной (кибер) безопасности
в кредитно-финансовой сфере**

Регистрационный
номер

I. Общие сведения

Организация информационной безопасности в кредитно-финансовой сфере
(кредитных и некредитных финансовых организациях)
(наименование вида профессиональной деятельности)

Код

Основная цель вида профессиональной деятельности:

Организация и обеспечение системы информационной безопасности в кредитно-финансовой сфере; реализация процессов информационной безопасности при осуществлении банковских и финансовых операций; проведение контроля состояния информационной безопасности в информационной инфраструктуре организаций кредитно-финансовой сферы

Группа занятий:

2149	Специалисты в области техники, не входящие в другие группы	2519	Разработчики и аналитики программного обеспечения и приложений, не входящие в другие группы
2153	Инженеры по телекоммуникациям	2523	Специалисты по компьютерным сетям
2422	Специалисты в области политики администрирования	2522	Системные администраторы
2434	Специалисты по сбыту информационно-коммуникационных технологий (ИКТ)	2521	Дизайнеры баз данных и администраторы
2425	Специалисты органов государственной власти	2529	Специалисты по базам данных и сетям, не входящие в другие группы
2511	Системные аналитики	2512	Разработчики программного обеспечения
2611	Юристы		

(код ОКЗ ¹)	(наименование)	(код ОКЗ)	(наименование)
-------------------------	----------------	-----------	----------------

Отнесение к видам экономической деятельности:

26.30.16	Производство оборудования средств связи, в том числе программное обеспечение, обеспечивающее выполнение установленных действий при проведении оперативно-розыскных мероприятий
26.30.19	Производство прочего коммуникационного оборудования
26.30.3	Производство запасных частей и комплектующих коммуникационного оборудования
62.01	Разработка компьютерного программного обеспечения
62.02.1	Деятельность по планированию, проектированию компьютерных систем
62.02.2	Деятельность по обследованию и экспертизе компьютерных систем
62.02.3	Деятельность по обучению пользователей
62.02.4	Деятельность по подготовке компьютерных систем к эксплуатации
62.02.9	Деятельность консультативная в области компьютерных технологий прочая
62.09	Деятельность, связанная с использованием вычислительной техники и информационных технологий, прочая
63.11.1	Деятельность по созданию и использованию баз данных и информационных ресурсов
69.10	Деятельность в области права
71.20.9	Деятельность по техническому контролю, испытаниям и анализу прочая
72.19.2	Научные исследования и разработки в области технических наук
74.90	Деятельность профессиональная, научная и техническая прочая, не включенная в другие группировки
74.90.32	Предоставление услуг по проведению оценки уязвимости объектов промышленного назначения, связи, здравоохранения и т.д.
80.20	Деятельность систем обеспечения безопасности
95.12	Ремонт коммуникационного оборудования
64.11	Деятельность Центрального банка Российской Федерации (Банка России)
71.12.6	Деятельность в области технического регулирования, стандартизации, метрологии, аккредитации, каталогизации продукции
71.12.61	Деятельность в области технического регулирования и стандартизации
71.12.62	Деятельность в области метрологии
71.12.63	Деятельность в области аккредитации
71.12.64	Государственный контроль (надзор) за соблюдением требований технических регламентов

(код ОКВЭД²)

(наименование вида экономической деятельности)

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

Обобщенные трудовые функции			Трудовые функции		
код	наименование	уровень квалификации	наименование	код	уровень (подуровень) квалификации
А	Методологическое обеспечение информационной безопасности в организациях кредитно-финансовой сферы	6	Методологическое обеспечение управления риском реализации информационных угроз в организациях кредитно-финансовой сферы	А/01.6	6
			Методологическое обеспечение защиты информации организаций кредитной-финансовой сферы	А/02.6	6
			Методологическое обеспечение защиты информации для непрерывности выполнения бизнес- и технологических процессов организаций кредитно-финансовой сферы	А/03.6	6
			Методологическое обеспечение управления инцидентами защиты информации и повышения ситуационной осведомленности в организациях кредитно-финансовой сферы	А/04.6	6
			Методологическое обеспечение управления риском реализации информационных угроз при аутсорсинге и использовании сторонних информационных сервисов в организациях кредитно-финансовой сферы	А/05.6	6
В	Реализация процессов информационной безопасности в информационной инфраструктуре организаций кредитно-финансовой сферы	6	Реализация процессов управления риском реализации информационных угроз в организациях кредитно-финансовой сферы	В/01.6	6
			Реализация процессов защиты информации в информационной инфраструктуре организаций кредитно-финансовой сферы	В/02.6	6
			Реализация процессов обеспечения защиты информации для непрерывности выполнения бизнес- и	В/03.6	6

			технологических процессов организаций кредитно-финансовой сферы		
			Реализация процессов управления риском реализации информационных угроз при аутсорсинге и использовании сторонних информационных сервисов в организациях кредитно-финансовой сферы	В/04.6	6
С	Технологическое обеспечение информационной безопасности в организациях кредитно-финансовой сферы	6	Разработка состава технологических мер защиты информации при реализации основных бизнес и технологических процессов организаций кредитно-финансовой сферы	С/01.6	6
			Реализация технологических мер защиты информации при реализации основных бизнес и технологических процессов организаций кредитно-финансовой сферы	С/02.6	6
			Контроль применения технологических мер защиты информации при реализации основных бизнес и технологических процессов организаций кредитно-финансовой сферы	С/03.6	6
D	Управление инцидентами защиты информации в организациях кредитно-финансовой сферы	6	Организация процессов управления инцидентами защиты информации в организациях кредитно-финансовой сферы	D/01.6	6
			Организация мониторинга информационной безопасности в организациях кредитно-финансовой сферы	D/02.6	6
			Организация взаимодействия организаций кредитно-финансовой сферы с ФинЦЕРТ Банка России	D/03.6	6
			Организация взаимодействия организаций кредитно-финансовой сферы с правоохранительными органами	D/04.6	6
			Подготовка отчетности по информационной безопасности организаций кредитно-финансовой сферы	D/05.6	6
E	Контроль информационной безопасности в организациях кредитно-финансовой сферы	6	Проведение внутреннего контроля управления риском реализации информационных угроз в организациях кредитно-финансовой сферы	E/01.6	6
			Проведение внутреннего контроля защиты информации организаций в организациях кредитно-финансовой сферы	E/02.6	6

			Проведение внутреннего контроля защиты информации для непрерывности выполнения бизнес- и технологических процессов организаций кредитно-финансовой сферы	Е/03.6	6
			Проведение внутреннего контроля управления риском реализации информационных угроз при аутсорсинге и использовании сторонних информационных сервисов в организациях кредитно-финансовой сферы	Е/04.6	6
			Организация внешнего аудита информационной безопасности в организациях кредитно-финансовой сферы	Е/05.6	6

III. Характеристика обобщенных трудовых функций

3.1. Обобщенная трудовая функция

Наименование	Методологическое обеспечение информационной безопасности в организациях кредитно-финансовой сферы		Код	A	Уровень квалификации	6
Происхождение обобщенной трудовой функции	Оригинал	X	Заимствовано из оригинала			
				Код оригинала	Регистрационный номер профессионального стандарта	
Возможные наименования должностей	Специалист по информационной безопасности Специалист по информационной безопасности 2 категории Специалист по информационной безопасности 1 категории Ведущий специалист по информационной безопасности Главный специалист по информационной безопасности					
Требования к образованию и обучению	Образовательные программы высшего образования – программы бакалавриата, специалитета, магистратуры Дополнительные профессиональные программы					
Требования к опыту практической работы	-					
Особые условия допуска к работе	-					

Дополнительные характеристики

Наименование документа	Код	Наименование базовой группы, должности (профессии) или специальности
ЕКС		
	-	Инженер-программист (программист)
	-	Инженер-программист по технической защите информации
	-	Инженер по защите информации
	-	Инженер-проектировщик
	-	Научный сотрудник
	-	Старший научный сотрудник
	-	Главный научный сотрудник
	-	Эксперт
	-	Администратор по обеспечению безопасности информации
-	Главный специалист по технической защите информации	

	-	Специалист по обеспечению безопасности информации в ключевых системах информационной инфраструктуры
ОКЗ	2153	Инженеры по телекоммуникациям
	2422	Специалисты в области политики администрирования
	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
	2519	Разработчики и аналитики программного обеспечения и приложений, не входящие в другие группы
	2611	Юристы
ОКСО ³	5.38.02.06	Финансы
	5.38.02.07	Банковское дело
	5.38.04.08	Финансы и кредит
	2.09.02.04	Информационные системы (по отраслям)
	2.09.02.05	Прикладная информатика (по отраслям)
	2.10.02.01	Организация и технология защиты информации
	2.10.02.02	Информационная безопасность телекоммуникационных систем
	2.10.02.03	Информационная безопасность автоматизированных систем
	2.09.03.02	Информационные системы и технологии
	2.09.03.03	Прикладная информатика
	2.09.03.04	Программная инженерия
	2.10.03.01	Информационная безопасность
	1.02.04.01	Математика и компьютерные науки
	1.02.04.02	Фундаментальная информатика и информационные технологии
	1.02.04.03	Математическое обеспечение и администрирование информационных систем
	2.09.04.02	Информационные системы и технологии
	2.09.04.03	Прикладная информатика
	2.09.04.04	Программная инженерия
	2.10.04.01	Информационная 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
	1.02.06.01	Компьютерные и информационные науки
	2.09.06.01	Информатика и вычислительная техника

	2.10.06.01	Информационная безопасность
	1.02.07.01	Компьютерные и информационные науки
	2.10.07.01	Информационная безопасность
	5.38.05.01	Экономическая безопасность
	5.38.07.02	Экономическая безопасность
	5.40.06.01	Юриспруденция

ОКПДТР	20911	Главный специалист по защите информации
	22567	Инженер по защите информации
	22824	Инженер-программист
	22870	Инженер электросвязи
	24392	Научный сотрудник (в области информатики и вычислительной техники)
	26579	Специалист по защите информации
	40064	Администратор баз данных
	40067	Администратор вычислительной сети
	40070	Администратор информационной безопасности вычислительной сети
	42843	Инженер - системный программист
	44544	Начальник исследовательской группы
	46115	Руководитель аналитической группы подразделения по комплексной защите информации
	051319	Методы и системы защиты информации, информационная безопасность
24062	Менеджер (в финансово-экономических и административных подразделениях (службах))	

3.1.1. Трудовая функция

Наименование	Методологическое обеспечение управления риском реализации информационных угроз в организациях кредитно-финансовой сферы	Код	A/01.6	Уровень (подуровень) квалификации	6
--------------	---	-----	--------	-----------------------------------	---

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

Трудовые действия	Разработка и согласование корпоративной политики по управлению риском реализации информационных угроз
	Определение и согласование контрольных показателей уровня риска реализации информационных угроз
	Разработка и согласование предложений по формированию структуры и организации управления риском реализации информационных угроз в организации кредитно-финансовой сферы

	Организация процессов и участие в идентификации области применения системы управления риском реализации информационных угроз
	Моделирование угроз безопасности информации
	Согласование результатов оценки риска реализации информационных угроз
	Разработка и согласование предложений по выбору способа реагирования на риск реализации информационных угроз
	Планирование применения мер, направленных на предотвращение (снижение степени вероятности реализации) реализации инцидентов защиты информации
	Планирование применения мер, направленных на ограничение (снижение степени тяжести потерь) потерь в результате реализации инцидентов защиты информации
Необходимые умения	Работать с действующей нормативно - правовой и методологической базой в области управления риском реализации информационных угроз в организациях кредитно-финансовой сферы
	Анализировать и применять в организации кредитно-финансовой сферы требования законодательства Российской Федерации и нормативных актов Банка России по вопросам управления риском реализации информационных угроз в организациях кредитно-финансовой сферы
	Анализировать и применять в организации кредитно-финансовой сферы требования национальных и международных стандартов по управления риском реализации информационных угроз в организациях кредитно-финансовой сферы
	Определять контрольные показатели уровня риска реализации информационных угроз в организации кредитно-финансовой сферы
	Разрабатывать модели угроз безопасности информации в организации кредитно-финансовой сферы
	Разрабатывать проекты внутренних документов организации кредитно-финансовой сферы, устанавливающих цели и принципы обеспечения управления риском реализации информационных угроз
	Разрабатывать проекты внутренних документов организации кредитно-финансовой сферы, определяющих методологию, правила организации и реализации управления риском реализации информационных угроз
	Планировать работу по реализации управления риском реализации информационных угроз в организации кредитно-финансовой сферы
Необходимые знания	Требования законодательства Российской Федерации по вопросам управления риском реализации информационных угроз в организациях кредитно-финансовой сферы
	Требования нормативных актов Банка России по вопросам управления риском реализации информационных угроз в организациях кредитно-финансовой сферы
	Состав и основное назначение ключевых национальных и международных документов в области стандартизации управления риском реализации информационных угроз в организациях кредитно-финансовой сферы
	Состав, назначение и основные положения документов Банка России в области стандартизации управления риском реализации информационных угроз в организациях кредитно-финансовой сферы

	Основные цели управления риском реализации информационных угроз в рамках бизнес и технологических процессов организаций кредитно-финансовой сферы
	Основные риски реализации информационных угроз в рамках бизнес и технологических процессов организаций кредитно-финансовой сферы
	Принципы управления рисками реализации информационных угроз организаций кредитно-финансовой сферы
Другие характеристики	

3.1.2. Трудовая функция

Наименование	Методологическое обеспечение защиты информации организаций кредитной-финансовой сферы	Код	A/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	Разработка и согласование корпоративной политики по защите информации организации кредитно-финансовой сферы				
	Определение области применения процессов системы защиты информации для уровней информационной инфраструктуры организации кредитно-финансовой сферы				
	Определение состава и содержания организационных мер защиты информации, реализуемых в рамках процессов системы защиты информации				
	Определение порядка применения организационных мер защиты информации, реализуемых в рамках процессов системы защиты информации				
	Определение состава и содержания технических мер защиты информации, выбранных организацией и реализуемых в рамках процессов системы защиты информации				
	Определение порядка применения технических мер защиты информации, реализуемых в рамках процессов системы защиты информации				
	Разработка правил размещения технических средств защиты информации в информационной инфраструктуре организации кредитно-финансовой сферы				
	Разработка параметров настроек технических средств защиты информации и информационной инфраструктуры, предназначенной для размещения технических средств защиты информации				
Разработка руководств по применению, эксплуатации, контролю эксплуатации и использованию по назначению технических средств защиты информации					

	<p>Определение состава ролей и права субъектов доступа, необходимых для обеспечения применения, эксплуатации, контроля эксплуатации и использования по назначению технических средств защиты информации</p>
	<p>Разработка и согласования планов по реализации организационных и технических мер защиты информации в организации кредитно-финансовой сферы</p>
Необходимые умения	<p>Работать с действующей нормативно - правовой и методологической базой в области обеспечения защиты информации организаций кредитно-финансовой сферы</p>
	<p>Анализировать и применять в организации кредитно-финансовой сферы требования законодательства Российской Федерации и нормативных актов Банка России по вопросам защиты информации</p>
	<p>Анализировать и применять в организации кредитно-финансовой сферы требования национальных и международных стандартов по защите информации</p>
	<p>Определять организационные меры защиты информации в рамках процессов защиты информации</p>
	<p>Определять технические меры защиты информации в рамках процессов защиты информации</p>
	<p>Разрабатывать проекты внутренних документов организации кредитно-финансовой сферы, устанавливающих цели и принципы обеспечения защиты информации, определяющих методологию, правила организации и реализации процессов обеспечения защиты информации</p>
	<p>Разрабатывать проекты внутренних документов организации кредитно-финансовой сферы, регламентирующих процессы обеспечения защиты информации</p>
	<p>Разрабатывать проекты внутренних документов организации кредитно-финансовой сферы, регламентирующих взаимодействие с внешними организациями</p>
	<p>Разрабатывать проекты внутренних документов организации кредитно-финансовой сферы по вопросам применения, эксплуатации, контроля эксплуатации и использования по назначению технических средств защиты информации</p>
	<p>Планировать работу по реализации организационных и технических мер защиты информации в организации кредитно-финансовой сферы</p>
Необходимые знания	<p>Требования законодательства Российской Федерации по вопросам защиты информации в организациях кредитно-финансовой сферы</p>
	<p>Требования нормативных актов Банка России по вопросам защиты информации в организациях кредитно-финансовой сферы</p>
	<p>Состав и основное назначение ключевых национальных и международных документов в области стандартизации обеспечения защиты информации в организациях кредитно-финансовой сферы</p>
	<p>Состав, назначение и основные положения документов Банка России в области стандартизации обеспечения защиты информации в организациях кредитно-финансовой сферы</p>
	<p>Основные цели обеспечения защиты информации в рамках бизнес и технологических процессов организаций кредитно-финансовой сферы</p>
	<p>Виды защищаемой информации в рамках бизнес и технологических процессов организаций кредитно-финансовой сферы</p>

	Основы проектного управления организаций кредитно-финансовой сферы
	Состав, принципы, условия реализации процессов обеспечения защиты информации в организациях кредитно-финансовой сферы
Другие характеристики	

3.1.3. Трудовая функция

Наименование	Методологическое обеспечение защиты информации для непрерывности выполнения бизнес- и технологических процессов организаций кредитно-финансовой сферы	Код	A/03.6	Уровень (подуровень) квалификации	6
Происхождение трудовой функции	Оригинал X	Заимствовано из оригинала			
			Код оригинала	Регистрационный номер профессионального стандарта	

Трудовые действия	Разработка и согласование корпоративной политики по обеспечению защиты информации для непрерывности выполнения бизнес- и технологических процессов организации кредитно-финансовой сферы
	Определение и установление ключевых индикаторов риска, связанных с обеспечением защиты информации для непрерывности выполнения бизнес- и технологических процессов организации кредитно-финансовой сферы
	Организация процессов и участие в идентификации области применения системы обеспечения защиты информации для непрерывности выполнения бизнес- и технологических процессов на уровне персонала организации кредитно-финансовой сферы
	Организация процессов и участие в идентификации области применения системы обеспечения защиты информации для непрерывности выполнения бизнес- и технологических процессов на уровне бизнес- и технологических процессов, реализуемых организацией кредитно-финансовой сферы при осуществлении видов деятельности по предоставлению финансовых и (или) информационных услуг
	Организация процессов и участие в идентификации области применения системы обеспечения защиты информации для непрерывности выполнения бизнес- и технологических процессов на прикладном уровне объектов информатизации, используемых организацией кредитно-финансовой сферы
	Организация процессов и участие в идентификации области применения системы обеспечения защиты информации для непрерывности выполнения бизнес- и технологических процессов на уровне данных, хранимых, обрабатываемых и (или) передаваемых в рамках реализации бизнес- и технологических процессов организации кредитно-финансовой сферы

	<p>Организация процессов и участие в идентификации области применения системы обеспечения защиты информации для непрерывности выполнения бизнес- и технологических процессов на инфраструктурном уровне объектов информатизации, используемых организацией кредитно-финансовой сферы</p> <p>Организация процессов и участие в идентификации области применения системы обеспечения защиты информации для непрерывности выполнения бизнес- и технологических процессов на физическом уровне (уровне помещений организации кредитно-финансовой сферы)</p> <p>Планирование применения мер, направленных на обеспечения защиты информации для непрерывности выполнения бизнес- и технологических процессов организации кредитно-финансовой сферы</p> <p>Определение состава и содержания мер, направленных на обеспечения защиты информации для непрерывности выполнения бизнес- и технологических процессов организации кредитно-финансовой сферы</p> <p>Определение порядка применения мер, направленных на обеспечения защиты информации для непрерывности выполнения бизнес- и технологических процессов организации кредитно-финансовой сферы</p> <p>Разработка и согласование планов по реализации мер, направленных на обеспечения защиты информации для непрерывности выполнения бизнес- и технологических процессов организации кредитно-финансовой сферы</p>
Необходимые умения	<p>Работать с действующей нормативно - правовой и методологической базой в области обеспечения защиты информации для непрерывности выполнения бизнес- и технологических процессов организации кредитно-финансовой сферы</p> <p>Анализировать и применять в организации кредитно-финансовой сферы требования законодательства Российской Федерации и нормативных актов Банка России по вопросам обеспечения защиты информации для непрерывности выполнения бизнес- и технологических процессов организации кредитно-финансовой сферы</p> <p>Анализировать и применять в организации кредитно-финансовой сферы требования национальных и международных стандартов по обеспечению защиты информации для непрерывности выполнения бизнес- и технологических процессов организации кредитно-финансовой сферы</p> <p>Определять организационные меры по обеспечению защиты информации для непрерывности выполнения бизнес- и технологических процессов организации кредитно-финансовой сферы</p> <p>Определять технические меры по обеспечению защиты информации для непрерывности выполнения бизнес- и технологических процессов организации кредитно-финансовой сферы</p> <p>Разрабатывать проекты внутренних документов организации кредитно-финансовой сферы, устанавливающих цели и принципы обеспечения защиты информации для непрерывности выполнения бизнес- и технологических процессов</p> <p>Разрабатывать проекты внутренних документов организации кредитно-финансовой сферы, определяющих методологию, правила организации и реализации обеспечения защиты информации для непрерывности выполнения бизнес- и технологических процессов</p>

	Планировать работу по обеспечению защиты информации для непрерывности выполнения бизнес- и технологических процессов организации кредитно-финансовой сферы
Необходимые знания	Требования законодательства Российской Федерации по вопросам обеспечения защиты информации для непрерывности выполнения бизнес- и технологических процессов организаций кредитно-финансовой сферы
	Требования нормативных актов Банка России по вопросам обеспечения защиты информации для непрерывности выполнения бизнес- и технологических процессов организаций кредитно-финансовой сферы
	Состав и основное назначение ключевых национальных и международных документов в области стандартизации обеспечения защиты информации для непрерывности выполнения бизнес- и технологических процессов организаций кредитно-финансовой сферы
	Состав, назначение и основные положения документов Банка России в области стандартизации обеспечения защиты информации для непрерывности выполнения бизнес- и технологических процессов организации кредитно-финансовой сферы
	Основные цели обеспечения защиты информации для непрерывности выполнения бизнес- и технологических процессов организации кредитно-финансовой сферы
	Принципы обеспечения защиты информации для непрерывности выполнения бизнес- и технологических процессов организации кредитно-финансовой сферы
Другие характеристики	

3.1.4. Трудовая функция

Наименование	Методологическое обеспечение управления инцидентами защиты информации и повышения ситуационной осведомленности в организациях кредитно-финансовой сферы	Код	A/04.6	Уровень (подуровень) квалификации	6
Происхождение трудовой функции	Оригинал <input checked="" type="checkbox"/>	Заемствовано из оригинала			
			Код оригинала	Регистрационный номер профессионального стандарта	
Трудовые действия	Определение и участие в согласовании политики управления инцидентами защиты информации и обеспечения ситуационной осведомленности организации кредитно-финансовой сферы				
	Определение и установление ключевых индикаторов риска (далее – КИР), связанных с управлением инцидентами защиты информации и обеспечением ситуационной осведомленности организации кредитно-финансовой сферы				

	<p>Определение структуры органов управления финансовой организации и подразделений, осуществляющих функции, связанные с управлением инцидентами защиты информации и обеспечением ситуационной осведомленности организации кредитно-финансовой сферы</p>
	<p>Организация и участие в идентификации источников формирующие данные о инцидентах защиты информации (событиях защиты информации) организации кредитно-финансовой сферы</p>
	<p>Организация и участие в идентификации технических данных, потенциально обладающих содержательной (семантической) информацией организации кредитно-финансовой сферы</p>
	<p>Организация и участие в разработке системы хранения информации о событиях защиты информации и инцидентах защиты информации организации кредитно-финансовой сферы</p>
Необходимые умения	<p>Работать с действующей нормативно - правовой и методологической базой в области управления инцидентами защиты информации и обеспечения ситуационной осведомленности организации кредитно-финансовой сферы</p>
	<p>Анализировать и применять в организации кредитно-финансовой сферы требования законодательства Российской Федерации и нормативных актов Банка России по вопросам управления инцидентами защиты информации и обеспечения ситуационной осведомленности организации кредитно-финансовой сферы</p>
	<p>Анализировать и применять в организации кредитно-финансовой сферы требования национальных и международных стандартов по вопросам управления инцидентами защиты информации и обеспечения ситуационной осведомленности организации кредитно-финансовой сферы</p>
	<p>Определять организационные меры по обеспечению управления инцидентами защиты информации и обеспечения ситуационной осведомленности организации кредитно-финансовой сферы</p>
	<p>Определять технические меры по обеспечению защиты информации для управления инцидентами защиты информации и обеспечения ситуационной осведомленности организации кредитно-финансовой сферы</p>
	<p>Разрабатывать проекты внутренних документов организации кредитно-финансовой сферы, устанавливающих цели и принципы управления инцидентами защиты информации и обеспечения ситуационной осведомленности организации кредитно-финансовой сферы</p>
	<p>Разрабатывать проекты внутренних документов организации кредитно-финансовой сферы, определяющих методологию, правила организации и реализации управления инцидентами защиты информации и обеспечения ситуационной осведомленности организации кредитно-финансовой сферы</p>
	<p>Планировать работу по управлению инцидентами защиты информации и обеспечения ситуационной осведомленности организации кредитно-финансовой сферы</p>
Необходимые знания	<p>Требования законодательства Российской Федерации по вопросам управления инцидентами защиты информации и обеспечения ситуационной осведомленности организации кредитно-финансовой сферы</p>

	Требования нормативных актов Банка России по вопросам управления инцидентами защиты информации и обеспечения ситуационной осведомленности организации кредитно-финансовой сферы
	Состав и основное назначение ключевых национальных и международных документов в области стандартизации управления инцидентами защиты информации и обеспечения ситуационной осведомленности организации кредитно-финансовой сферы
	Состав, назначение и основные положения документов Банка России в области стандартизации управления инцидентами защиты информации и обеспечения ситуационной осведомленности организации кредитно-финансовой сферы
	Основные цели управления инцидентами защиты информации и обеспечения ситуационной осведомленности организации кредитно-финансовой сферы
	Принципы управления инцидентами защиты информации и обеспечения ситуационной осведомленности организации кредитно-финансовой сферы
Другие характеристики	

3.1.5. Трудовая функция

Наименование	Методологическое обеспечение управления риском реализации информационных угроз при аутсорсинге и использовании сторонних информационных сервисов в организациях кредитно-финансовой сферы	Код	A/05.6	Уровень (подуровень) квалификации	6
Происхождение трудовой функции	Оригинал <input checked="" type="checkbox"/>	Займствовано из оригинала			
			Код оригинала	Регистрационный номер профессионального стандарта	
Трудовые действия	Определение и участие в согласовании политики управления риском реализации информационных угроз при аутсорсинге и использовании сторонних информационных сервисов организации кредитно-финансовой сферы				
	Определение и установление ключевых индикаторов риска (далее – КИР), связанных с управлением риском реализации информационных угроз при аутсорсинге и использовании сторонних информационных сервисов организации кредитно-финансовой сферы				
	Определение структуры органов управления организации кредитно-финансовой сферы и подразделений, осуществляющих функции, связанные с управлением риском реализации информационных угроз при аутсорсинге и использовании сторонних информационных сервисов				
	Организация и участие в идентификации бизнес и (или) технологических процессов организации кредитно-финансовой сферы,				

	<p>переданных на аутсорсинг или выполняемых с использованием сторонних информационных сервисов, ненадлежащее выполнение которых поставщиком услуг создает условия для реализации или реализует риск информационных угроз</p>
	<p>Организация и участие в идентификации защищаемой информации применяемой в бизнес и (или) технологических процессах организации кредитно-финансовой сферы, переданных на аутсорсинг или выполняемых с использованием сторонних информационных сервисов, несанкционированный доступ к которой, раскрытие (распространение), несанкционированное (неавторизованное) изменение, уничтожение (потеря) и (или) хищение создают условия для возникновения убытков финансовой организации, ее клиентов или контрагентов, в том числе условия для совершения финансовых операций от имени клиентов</p>
	<p>Организация и участие в оценке риска реализации информационных угроз при аутсорсинге и использовании сторонних информационных сервисов в организации кредитно-финансовой сферы, а также согласование результатов оценки.</p>
	<p>Определение ролей, связанных с выявлением и идентификацией риска реализации информационных угроз при аутсорсинге и использовании сторонних информационных сервисов организацией кредитно-финансовой сферы</p>
Необходимые умения	<p>Работать с действующей нормативно - правовой и методологической базой в области управления риском реализации информационных угроз при аутсорсинге и использовании сторонних информационных сервисов организации кредитно-финансовой сферы</p>
	<p>Анализировать и применять в организации кредитно-финансовой сферы требования законодательства Российской Федерации и нормативных актов Банка России по вопросам управления риском реализации информационных угроз при аутсорсинге и использовании сторонних информационных сервисов организации кредитно-финансовой сферы</p>
	<p>Анализировать и применять в организации кредитно-финансовой сферы требования национальных и международных стандартов по вопросам управления риском реализации информационных угроз при аутсорсинге и использовании сторонних информационных сервисов организации кредитно-финансовой сферы</p>
	<p>Определять организационные меры по обеспечению защиты информации для управления риском реализации информационных угроз при аутсорсинге и использовании сторонних информационных сервисов организации кредитно-финансовой сферы</p>
	<p>Определять технические меры по обеспечению защиты информации для управления риском реализации информационных угроз при аутсорсинге и использовании сторонних информационных сервисов организации кредитно-финансовой сферы</p>
	<p>Разрабатывать проекты внутренних документов организации кредитно-финансовой сферы, устанавливающих цели и принципы управления риском реализации информационных угроз при аутсорсинге и использовании сторонних информационных сервисов организации кредитно-финансовой сферы</p>
	<p>Разрабатывать проекты внутренних документов организации кредитно-финансовой сферы, определяющих методологию, правила организации и реализации управления риском реализации информационных угроз</p>

	при аутсорсинге и использовании сторонних информационных сервисов организации кредитно-финансовой сферы
	Планировать работу по обеспечению защиты информации для управления риском реализации информационных угроз при аутсорсинге и использовании сторонних информационных сервисов организации кредитно-финансовой сферы
Необходимые знания	Требования законодательства Российской Федерации по вопросам управления риском реализации информационных угроз при аутсорсинге и использовании сторонних информационных сервисов организации кредитно-финансовой сферы
	Требования нормативных актов Банка России по вопросам управления риском реализации информационных угроз при аутсорсинге и использовании сторонних информационных сервисов организации кредитно-финансовой сферы
	Состав и основное назначение ключевых национальных и международных документов в области стандартизации управления риском реализации информационных угроз при аутсорсинге и использовании сторонних информационных сервисов организации кредитно-финансовой сферы
	Состав, назначение и основные положения документов Банка России в области стандартизации управления риском реализации информационных угроз при аутсорсинге и использовании сторонних информационных сервисов организации кредитно-финансовой сферы
	Основные цели управления риском реализации информационных угроз при аутсорсинге и использовании сторонних информационных сервисов организации кредитно-финансовой сферы
	Принципы управления риском реализации информационных угроз при аутсорсинге и использовании сторонних информационных сервисов организации кредитно-финансовой сферы
Другие характеристики	

3.2. Обобщенная трудовая функция

Наименование	Реализация процессов информационной безопасности в информационной инфраструктуре организаций кредитно-финансовой сферы	Код	В	Уровень квалификации	6
Происхождение обобщенной трудовой функции	Оригинал <input checked="" type="checkbox"/>	Заимствовано из оригинала			
		Код оригинала		Регистрационный номер профессионального стандарта	
Возможные наименования должностей	Специалист по информационной безопасности Специалист по информационной безопасности 2 категории Специалист по информационной безопасности 1 категории				

	Ведущий специалист по информационной безопасности Главный специалист по информационной безопасности
Требования к образованию и обучению	Образовательные программы высшего образования – программы бакалавриата, специалитета, магистратуры Дополнительные профессиональные программы
Требования к опыту практической работы	-
Особые условия допуска к работе	-

Дополнительные характеристики

Наименование документа	Код	Наименование базовой группы, должности (профессии) или специальности
ЕКС	-	Инженер-программист (программист)
	-	Инженер-программист по технической защите информации
	-	Инженер по защите информации
	-	Инженер-проектировщик
	-	Научный сотрудник
	-	Старший научный сотрудник
	-	Главный научный сотрудник
	-	Эксперт
	-	Администратор по обеспечению безопасности информации
	-	Главный специалист по технической защите информации
	-	Специалист по обеспечению безопасности информации в ключевых системах информационной инфраструктуры
	ОКЗ	2153
2422		Специалисты в области политики администрирования
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
2519		Разработчики и аналитики программного обеспечения и приложений, не входящие в другие группы
2611	Юристы	
ОКСО	5.38.02.06	Финансы
	5.38.02.07	Банковское дело
	5.38.04.08	Финансы и кредит
	2.09.02.04	Информационные системы (по отраслям)

	2.09.02.05	Прикладная информатика (по отраслям)
	2.10.02.01	Организация и технология защиты информации
	2.10.02.02	Информационная безопасность телекоммуникационных систем
	2.10.02.03	Информационная безопасность автоматизированных систем
	2.09.03.02	Информационные системы и технологии
	2.09.03.03	Прикладная информатика
	2.09.03.04	Программная инженерия
	2.10.03.01	Информационная безопасность
	1.02.04.01	Математика и компьютерные науки
	1.02.04.02	Фундаментальная информатика и информационные технологии
	1.02.04.03	Математическое обеспечение и администрирование информационных систем
	2.09.04.02	Информационные системы и технологии
	2.09.04.03	Прикладная информатика
	2.09.04.04	Программная инженерия
	2.10.04.01	Информационная 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
	1.02.06.01	Компьютерные и информационные науки
	2.09.06.01	Информатика и вычислительная техника
	2.10.06.01	Информационная безопасность
	1.02.07.01	Компьютерные и информационные науки
	2.10.07.01	Информационная безопасность
	5.38.05.01	Экономическая безопасность
	5.38.07.02	Экономическая безопасность
	5.40.06.01	Юриспруденция

ОКПДТР	20911	Главный специалист по защите информации
	22567	Инженер по защите информации
	22824	Инженер-программист
	22870	Инженер электросвязи
	24392	Научный сотрудник (в области информатики и вычислительной техники)
	26579	Специалист по защите информации
	40064	Администратор баз данных
	40067	Администратор вычислительной сети
	40070	Администратор информационной безопасности вычислительной сети
	42843	Инженер - системный программист
	44544	Начальник исследовательской группы
	46115	Руководитель аналитической группы подразделения

		по комплексной защите информации
	051319	Методы и системы защиты информации, информационная безопасность
	24062	Менеджер (в финансово-экономических и административных подразделениях (службах))

3.2.1. Трудовая функция

Наименование	Реализация процессов управления риском реализации информационных угроз в организациях кредитно-финансовой сферы	Код	V/01.6	Уровень (подуровень) квалификации	6
--------------	---	-----	--------	-----------------------------------	---

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

Трудовые действия	Организация и сопровождение процессов реализации мер, направленных на предотвращение (снижение степени вероятности реализации) реализации инцидентов защиты информации
	Организация и сопровождение процессов реализации мер, направленных на ограничение (снижение степени тяжести потерь) потерь в результате реализации инцидентов защиты информации
	Оценка необходимого и достаточного ресурсного (кадрового и финансового) обеспечения процессов системы управления риском реализации информационных угроз, а также иных систем управления в рамках ключевых направлений обеспечения информационной безопасности
	Разработка и согласование предложений по организации необходимого и достаточного ресурсного (кадрового и финансового) обеспечения процессов системы управления риском реализации информационных угроз, а также иных систем в рамках ключевых направлений (доменов)
	Оценка необходимого и достаточного ресурсного (кадрового и финансового) обеспечения функционирования службы информационной безопасности
	Разработка и согласование предложений по организации необходимого и достаточного ресурсного (кадрового и финансового) обеспечения функционирования службы информационной безопасности
	Управление риском реализации информационных угроз при назначении и распределении ролей, в том числе в целях обеспечения доверия к персоналу
	Разработка, реализация планов и программ обучения и повышения осведомленности в части противодействия информационным угрозам и контроль результатов
	Разработка способов мотивации персонала организации кредитно-финансовой сферы к участию в управлении риском реализации информационных угроз

	<p>Организация и сопровождение процессов взаимодействия с клиентами организации кредитно-финансовой сферы с целью повышения осведомленности клиентов в части противодействия информационным угрозам</p> <p>Организация и сопровождение процессов взаимодействия с клиентами организации кредитно-финансовой сферы с целью обеспечения защиты информации при предоставлении финансовых (банковских) услуг, в том числе при осуществлении переводов денежных средств</p>
Необходимые умения	<p>Организовывать реализацию проектов по вопросам обработки рисков реализации информационных угроз в организации кредитно-финансовой сферы</p> <p>Организовывать внедрение и применение политик (правил, процедур), направленных на предотвращение (снижение степени вероятности реализации) реализации инцидентов защиты информации</p> <p>Разрабатывать предложения по организации необходимого и достаточного ресурсного (кадрового и финансового) обеспечения процессов системы управления риском реализации информационных угроз организации кредитно-финансовой сферы</p> <p>Разрабатывать предложения по организации необходимого и достаточного ресурсного (кадрового и финансового) обеспечения функционирования службы информационной безопасности организации кредитно-финансовой сферы</p> <p>Осуществлять управление риском реализации информационных угроз при назначении и распределении ролей в организации кредитно-финансовой сферы</p> <p>Разрабатывать планы и программы обучения и повышения осведомленности в части противодействия информационным угрозам организации кредитно-финансовой сферы</p> <p>Разрабатывать способы мотивации персонала организации кредитно-финансовой сферы к участию в управлении риском реализации информационных угроз</p> <p>Разрабатывать систему мер и мероприятий для контроля уязвимостей и связанных с ними рисков нарушения информационной безопасности на стадиях создания автоматизированных систем организации кредитно-финансовой сферы</p>
Необходимые знания	<p>Требования законодательства Российской Федерации по вопросам управления риском реализации информационных угроз в организациях кредитно-финансовой сферы</p> <p>Требования нормативных актов Банка России по вопросам управления риском реализации информационных угроз в организациях кредитно-финансовой сферы</p> <p>Требования национальных и международных документов в области стандартизации управления риском реализации информационных угроз в организациях кредитно-финансовой сферы</p> <p>Требования документов Банка России в области стандартизации управления риском реализации информационных угроз в организациях кредитно-финансовой сферы</p> <p>Основные цели управления риском реализации информационных угроз в рамках бизнес и технологических процессов организаций кредитно-финансовой сферы</p>

	Основные риски реализации информационных угроз в рамках бизнес и технологических процессов организаций кредитно-финансовой сферы
	Принципы управления рисками реализации информационных угроз организаций кредитно-финансовой сферы
	Уязвимости и связанные с ними риски нарушения защиты информации, присущие используемых организациями кредитно-финансовой сферы, процессов проектирования, приобретения, эксплуатации и сопровождения эксплуатации автоматизированных систем
Другие характеристики	

3.2.2. Трудовая функция

Наименование	Реализация процессов защиты информации в информационной инфраструктуре организаций кредитно-финансовой сферы	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	Учет объектов и ресурсов доступа, входящих в область применения процесса системы защиты информации, для всех уровней информационной инфраструктуры организации кредитно-финансовой сферы, в том числе объектов доступа, расположенных в публичных (общедоступных) местах (в том числе банкоматов, платежных терминалов)
	Размещение и настройка (конфигурирование) технических мер защиты информации в информационной инфраструктуре организации кредитно-финансовой сферы
	Тестирование полноты реализации технических мер защиты информации
	Назначение работникам организации кредитно-финансовой сферы ролей, связанных с применением мер защиты информации, и установление обязанности и ответственности за их выполнение
	Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной инфраструктуры организации кредитно-финансовой сферы
	Эксплуатация и использование по назначению технических средств защиты информации
	Применение организационных мер защиты информации
	Централизованное управление техническими средствами и мерами защиты информации
Организация резервирования информационной инфраструктуры, организации кредитно-финансовой сферы необходимой для функционирования технических мер и средств защиты информации	

	<p>Принятие регламентированных мер по восстановлению отказавших технических средств защиты информации информационной инфраструктуры организации кредитно-финансовой сферы</p> <p>Сопровождение технических мер и средств защиты информации в течении всего срока их использования</p> <p>Обучение, практическая подготовка (переподготовка) работников организации кредитно-финансовой сферы, ответственных за применение мер и средств защиты информации в рамках процесса защиты информации</p> <p>Повышение осведомленности (инструктаж) работников организации кредитно-финансовой сферы в области реализации процесса защиты информации, применения организационных мер защиты информации, использования по назначению технических мер и средств защиты информации</p> <p>Организация защиты информации на этапах жизненного цикла автоматизированных систем и приложений</p>
Необходимые умения	<p>Осуществлять концептуальное, архитектурное, функциональное и техническое проектирование процессов защиты информации в информационной инфраструктуре организаций кредитно-финансовой сферы, а также оформлять соответствующие проектные документы</p> <p>Организовывать реализацию проектов по вопросам защиты информации в организации уредитно-финансовой сферы</p> <p>Организовывать внедрение и применение политик (правил, процедур) по обеспечению защиты информации в организации кредитно-финансовой сферы</p> <p>Принимать участие в концептуальном, архитектурном и техническом проектировании реализации процессов защиты информации в информационной инфраструктуре организаций кредитно-финансовой сферы</p> <p>Разрабатывать функционально-технические требования к техническим средствам защиты информации и системам обеспечения защиты информации в организациях кредитно-финансовой сферы</p> <p>Принимать участие в выборе технических средств защиты информации и систем обеспечения защиты информации для применения в рамках бизнес и технологических процессов организации кредитно-финансовой сферы</p> <p>Организовывать внедрение технических средств защиты информации на объектах информатизации и систем защиты информации в информационной структуре организаций кредитно-финансовой сферы</p> <p>Организовать и обеспечивать защиту информации в ходе эксплуатации технических средств защиты информации и систем обеспечения защиты информации на объектах информационной инфраструктуры, бизнес и технологических процессов организации кредитно-финансовой сферы</p> <p>Обеспечивать защиту информации при выводе из эксплуатации компонентов информационной инфраструктуры, носителей данных</p>
Необходимые знания	<p>Виды защищаемой информации в рамках бизнес и технологических процессов организации кредитно-финансовой сферы</p> <p>Основные цели обеспечения защиты информации в рамках бизнес и технологических процессов организаций кредитно-финансовой сферы</p> <p>Состав, принципы, условия реализации процессов обеспечения защиты информации в организации кредитно-финансовой сферы</p>

	Состав и основные функциональные возможности технических средств защиты информации и систем обеспечения защиты информации, предназначенных для применения в рамках процессов защиты информации организаций кредитно-финансовой сферы
	Основные организационные и технические меры защиты информации
	Основы построения и принципы функционирования автоматизированных систем, реализация бизнес и технологических процессов организаций кредитно-финансовой сферы, в том числе автоматизированных банковских систем
	Основы выполнения, принципы, задачи и правила оформления концептуального, архитектурного и технического проектирования реализации процессов защиты информации в информационной инфраструктуре организаций кредитно-финансовой сферы
	Уязвимости и связанные с ними риски нарушения защиты информации, присущие используемым организациями кредитно-финансовой сферы, процессов проектирования, приобретения, эксплуатации и сопровождения эксплуатации автоматизированных систем, реализующих бизнес и технологические процессы организаций кредитно-финансовой сферы, в том числе автоматизированных банковских систем
	Объекты информационной инфраструктуры организаций кредитно-финансовой сферы, включая автоматизированные системы и их компоненты, задействованные в реализации бизнес и технологических процессов организаций кредитно-финансовой сферы (автоматизированные рабочие места пользователей и эксплуатационного персонала, серверное и сетевое оборудование, системы хранения данных, аппаратные модули безопасности (HSM), устройства печати и копирования информации, объекты доступа, расположенные в публичных (общедоступных) местах (в том числе банкоматы, платежные терминалы)
	Ресурсы доступа информационной инфраструктуры организаций кредитно-финансовой сферы (автоматизированные системы, базы данных, сетевые файловые ресурсы, виртуальные машины, предназначенные для размещения серверных компонентов автоматизированных систем, ресурсы доступа, относящиеся к сервисам электронной почты, а также к WEB-сервисам организации кредитно-финансовой сферы в сети Интранет и Интернет)
	Функционально-технические требования к техническим средствам защиты информации и системам обеспечения защиты информации в организациях кредитно-финансовой сферы
	Условия по ограничениям, связанным с применением технических средств защиты информации и систем обеспечения защиты информации в рамках бизнес и технологических процессов организаций кредитно-финансовой сферы
	Требования к применению техническим средствам защиты информации, сертифицированным по требованиям безопасности информации
Другие характеристики	

3.2.3. Трудовая функция

Наименование	Реализация процессов обеспечения защиты информации для непрерывности выполнения бизнес- и технологических процессов организаций кредитно-финансовой сферы	Код	В/03.6	Уровень (подуровень) квалификации	6
--------------	---	-----	--------	-----------------------------------	---

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

Трудовые действия	Организация и сопровождение процессов реализации мер на уровне персонала организации кредитно-финансовой сферы
	Организация и сопровождение процессов реализации мер на уровне бизнес- и технологических процессов, реализуемых организацией кредитно-финансовой сферы при осуществлении видов деятельности по предоставлению финансовых и (или) информационных услуг
	Организация и сопровождение процессов реализации мер на прикладном уровне объектов информатизации, используемых организацией кредитно-финансовой сферы
	Организация и сопровождение процессов реализации мер на уровне данных, хранимых, обрабатываемых и (или) передаваемых в рамках реализации бизнес- и технологических процессов организации кредитно-финансовой сферы
	Организация и сопровождение процессов реализации мер на инфраструктурном уровне объектов информатизации, используемых организацией кредитно-финансовой сферы
	Организация и сопровождение процессов реализации мер на физическом уровне (уровне помещений организации кредитно-финансовой сферы)
	Участие в разработке и применения плана обеспечения непрерывности и восстановление деятельности в случае чрезвычайных ситуаций) в рамках обеспечения защиты информации для непрерывности выполнения бизнес- и технологических процессов организации кредитно-финансовой сферы
	Разработка и применение плана восстановления непрерывности выполнения бизнес- и технологических процессов организации кредитно-финансовой сферы при реализации инцидентов защиты информации
Необходимые умения	Разрабатывать предложения в план обеспечения непрерывности и восстановление деятельности в случае чрезвычайных ситуаций) в рамках обеспечения защиты информации для непрерывности выполнения бизнес- и технологических процессов организации кредитно-финансовой сферы
	Разрабатывать план восстановления непрерывности выполнения бизнес- и технологических процессов организации кредитно-финансовой сферы при реализации инцидентов защиты информации

	<p>Настраивать резервное копирование системных параметров, программного обеспечения и файлов, в том числе в соответствии с заданным расписанием</p> <p>Восстанавливать системные параметры, программное обеспечение и файлы из резервных копий</p> <p>Разрабатывать организационные и технические меры по реализации процессов обеспечения защиты информации для непрерывности выполнения бизнес- и технологических процессов организаций кредитно-финансовой сферы</p>
Необходимые знания	<p>Принципы управления вычислительными мощностями и пропускной способностью каналов связи организации кредитно-финансовой сферы</p> <p>Архитектура построения отказоустойчивых центров обработки и (или) хранения данных</p> <p>Технологии резервирования и восстановления данных</p> <p>Инфраструктурные уровни объектов информатизации, используемые организацией кредитно-финансовой сферы</p>
Другие характеристики	

3.2.4. Трудовая функция

Наименование	Реализация процессов управления риском реализации информационных угроз при аутсорсинге и использовании сторонних информационных сервисов в организациях кредитно-финансовой сферы	Код	В/04.6	Уровень (подуровень) квалификации	6
--------------	---	-----	--------	-----------------------------------	---

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

Трудовые действия	Подготовка предложений в план управления риском реализации информационных угроз при аутсорсинге и использовании сторонних информационных сервисов
	Классификация риска реализации информационных угроз при аутсорсинге и использовании сторонних информационных сервисов
	Определение и согласование зоны ответственности руководства финансовой организации при аутсорсинге и использовании сторонних информационных сервисов для выполнения бизнес и (или) технологических процессов организации кредитно-финансовой сферы
	Разработка и согласование необходимого состава (содержания) соглашения (контракта, пакета договорных документов) при аутсорсинге и использовании сторонних информационных сервисов для выполнения бизнес и (или) технологических процессов организации кредитно-финансовой сферы

	Выполнение оценки возможности поставщика услуг выполнить свои обязательства по аутсорсингу бизнес и (или) технологических процессов организации кредитно-финансовой сферы
	Организация системы мер, направленных на снижение риска реализации информационных угроз при аутсорсинге и использовании сторонних информационных сервисов
	Организация и участие в оценке поставщика услуг, выполняющего бизнес и (или) технологические процессы организации кредитно-финансовой сферы на аутсорсинге, в части ресурсного обеспечения
	Организация и участие в оценке поставщика услуг, выполняющего бизнес и (или) технологические процессы организации кредитно-финансовой сферы на аутсорсинге, в части соблюдения требований к защите информации
	Организация и участие в оценке поставщика услуг, выполняющего бизнес и (или) технологические процессы организации кредитно-финансовой сферы на аутсорсинге, в части соблюдения требований к обеспечению непрерывности деятельности
Необходимые умения	Разрабатывать предложения в план управления риском реализации информационных угроз при аутсорсинге и использовании сторонних информационных сервисов
	Разрабатывать предложения по снижению риска реализации информационных угроз в соглашение (контракт, пакет договорных документов) при аутсорсинге и использовании сторонних информационных сервисов для выполнения бизнес и (или) технологических процессов финансовой организации
	Оценивать возможности поставщика услуг выполнить свои обязательства по аутсорсингу бизнес и (или) технологических процессов организации кредитно-финансовой сферы
	Разрабатывать предложения по мерам, направленным на снижение риска реализации информационных угроз при аутсорсинге и использовании сторонних информационных сервисов
Необходимые знания	Требования законодательства Российской Федерации по вопросам управления риском реализации информационных угроз при аутсорсинге и использовании сторонних информационных сервисов в организациях кредитно-финансовой сферы
	Требования нормативных актов Банка России по вопросам управления риском реализации информационных угроз при аутсорсинге и использовании сторонних информационных сервисов в организациях кредитно-финансовой сферы
	Требования национальных и международных документов в области стандартизации управления риском реализации информационных угроз при аутсорсинге и использовании сторонних информационных сервисов в организациях кредитно-финансовой сферы
	Требования документов Банка России в области стандартизации управления риском реализации информационных угроз при аутсорсинге и использовании сторонних информационных сервисов в организациях кредитно-финансовой сферы
	Основные цели управления риском реализации информационных угроз при аутсорсинге и использовании сторонних информационных сервисов в организациях кредитно-финансовой сферы

	Основные риски реализации информационных угроз при аутсорсинге и использовании сторонних информационных сервисов в организациях кредитно-финансовой сферы
	Принципы управления риском реализации информационных угроз при аутсорсинге и использовании сторонних информационных сервисов в организациях кредитно-финансовой сферы
Другие характеристики	

3.3. Обобщенная трудовая функция

Наименование	Технологическое обеспечение информационной безопасности в организациях кредитно-финансовой сферы	Код	С	Уровень квалификации	6
Происхождение обобщенной трудовой функции	Оригинал <input checked="" type="checkbox"/>	Заимствовано из оригинала			
		Код оригинала		Регистрационный номер профессионального стандарта	
Возможные наименования должностей	Специалист по информационной безопасности Специалист по информационной безопасности 2 категории Специалист по информационной безопасности 1 категории Ведущий специалист по информационной безопасности Главный специалист по информационной безопасности				
Требования к образованию и обучению	Образовательные программы высшего образования – программы бакалавриата, специалитета, магистратуры Дополнительные профессиональные программы				
Требования к опыту практической работы	-				
Особые условия допуска к работе	-				

Дополнительные характеристики

Наименование документа	Код	Наименование базовой группы, должности (профессии) или специальности
ЕКС		
	-	Инженер-программист (программист)
	-	Инженер-программист по технической защите информации
	-	Инженер по защите информации
	-	Инженер-проектировщик
	-	Научный сотрудник
	-	Старший научный сотрудник

	-	Главный научный сотрудник
	-	Эксперт
	-	Администратор по обеспечению безопасности информации
	-	Главный специалист по технической защите информации
	-	Специалист по обеспечению безопасности информации в ключевых системах информационной инфраструктуры
ОКЗ	2153	Инженеры по телекоммуникациям
	2422	Специалисты в области политики администрирования
	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
	2519	Разработчики и аналитики программного обеспечения и приложений, не входящие в другие группы
	2611	Юристы
ОКСО	5.38.02.06	Финансы
	5.38.02.07	Банковское дело
	5.38.04.08	Финансы и кредит
	2.09.02.04	Информационные системы (по отраслям)
	2.09.02.05	Прикладная информатика (по отраслям)
	2.10.02.01	Организация и технология защиты информации
	2.10.02.02	Информационная безопасность телекоммуникационных систем
	2.10.02.03	Информационная безопасность автоматизированных систем
	2.09.03.02	Информационные системы и технологии
	2.09.03.03	Прикладная информатика
	2.09.03.04	Программная инженерия
	2.10.03.01	Информационная безопасность
	1.02.04.01	Математика и компьютерные науки
	1.02.04.02	Фундаментальная информатика и информационные технологии
	1.02.04.03	Математическое обеспечение и администрирование информационных систем
	2.09.04.02	Информационные системы и технологии
	2.09.04.03	Прикладная информатика
	2.09.04.04	Программная инженерия
	2.10.04.01	Информационная 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
	1.02.06.01	Компьютерные и информационные науки
	2.09.06.01	Информатика и вычислительная техника
	2.10.06.01	Информационная безопасность
	1.02.07.01	Компьютерные и информационные науки
	2.10.07.01	Информационная безопасность
	5.38.05.01	Экономическая безопасность
	5.38.07.02	Экономическая безопасность
	5.40.06.01	Юриспруденция

ОКПДТР	20911	Главный специалист по защите информации
	22567	Инженер по защите информации
	22824	Инженер-программист
	22870	Инженер электросвязи
	24392	Научный сотрудник (в области информатики и вычислительной техники)
	26579	Специалист по защите информации
	40064	Администратор баз данных
	40067	Администратор вычислительной сети
	40070	Администратор информационной безопасности вычислительной сети
	42843	Инженер - системный программист
	44544	Начальник исследовательской группы
	46115	Руководитель аналитической группы подразделения по комплексной защите информации
	051319	Методы и системы защиты информации, информационная безопасность
	24062	Менеджер (в финансово-экономических и административных подразделениях (службах))

3.3.1. Трудовая функция

Наименование	Разработка состава технологических мер защиты информации при реализации основных бизнес и технологических процессов организаций кредитно-финансовой сферы	Код	C/01.6	Уровень (подуровень) квалификации	6
--------------	---	-----	--------	-----------------------------------	---

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

Трудовые действия	<p>Изучение новых технологий, достижений науки и техники в области обеспечения информационной безопасности, аналитических материалов ведущих компаний в области информационной безопасности</p> <p>Разработка технологических мер защиты информации в рамках реализации бизнес и технологических процессов организации кредитно-финансовой сферы</p> <p>Разработка технологических мер защиты информации применительно к объектам информационной инфраструктуры организации кредитно-финансовой сферы</p> <p>Разработка технологических мер защиты информации организации кредитно-финансовой сферы при осуществлении переводов денежных средств</p> <p>Разработка технологических мер защиты информации организации кредитно-финансовой сферы при осуществлении операций с платежными картами</p> <p>Разработка технологических мер защиты информации организации кредитно-финансовой сферы при передаче финансовых сообщений формата СВИФТ (SWIFT)</p>
Необходимые умения	<p>Применять при разработке состава технологических мер защиты информации знания в области осуществления банковской и финансовой деятельности, знания в реализации бизнес и технологических процессов организаций кредитно-финансовой сферы</p> <p>Применять при разработке состава технологических мер защиты информации знания по существующим практикам технологических мер защиты информации при реализации бизнес и технологических процессов организаций кредитно-финансовой сферы</p> <p>Принимать участие в обеспечении применения технологических мер защиты информации на этапах концептуального, архитектурного и технического проектирования автоматизированных систем организации кредитно-финансовой сферы</p> <p>Разрабатывать требования и технологические меры защиты информации в автоматизированных системах организации кредитно-финансовой сферы</p> <p>Разрабатывать технологические меры защиты информации с учетом специфики реализации бизнес и технологических процессов организации кредитно-финансовой сферы</p>
Необходимые знания	<p>Требования законодательства Российской Федерации, нормативно-правовых актов Российской Федерации, нормативных актов Банка России в области применения технологических мер защиты информации в процессах, связанных с:</p> <ul style="list-style-type: none"> - осуществлением переводов денежных средств в системах дистанционного банковского обслуживания; - осуществлением переводов денежных средств с использованием платежных карт; - реализацией операционных функций, передачей и обработкой электронных сообщений, в том числе в рамках переводов денежных средств, осуществления платежного клиринга и проведения иных форм безналичных расчетов; - наличным денежным обращением и кассовым обслуживанием

	Состав и содержание технологических мер защиты информации при реализации бизнес и технологических процессов организаций кредитно-финансовой сферы
	Примеры и принципы проектирования технологических мер защиты информации для бизнес и технологических процессов организации кредитно-финансовой сферы
	Терминология в области обеспечения информационной безопасности в части технологических мер защиты информации
Другие характеристики	

3.3.2. Трудовая функция

Наименование	Реализация технологических мер защиты информации при реализации основных бизнес и технологических процессов организаций кредитно-финансовой сферы	Код	C/02.6	Уровень (подуровень) квалификации	6
--------------	---	-----	--------	-----------------------------------	---

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

Трудовые действия	Участие в реализации технологических мер защиты информации в рамках реализации бизнес и технологических процессов организации кредитно-финансовой сферы
	Участие в реализации технологических мер защиты информации применительно к объектам информационной инфраструктуры организации кредитно-финансовой сферы
	Участие в реализации технологических мер защиты информации организации кредитно-финансовой сферы при осуществлении переводов денежных средств
	Участие в реализации технологических мер защиты информации организации кредитно-финансовой сферы при осуществлении операций с платежными картами
	Участие в реализации технологических мер защиты информации организации кредитно-финансовой сферы при передаче финансовых сообщений формата СВИФТ (SWIFT)
	Участие в организации и осуществлении взаимодействия с Национальной системой платежных карт
	Участие в организации и осуществлении взаимодействия с платежной системой Банка России
	Участие в организации и осуществлении взаимодействия с системой быстрых
	Участие в организации и осуществлении взаимодействия с системой передачи финансовых сообщений

Необходимые умения	Применять при реализации технологических мер защиты информации знания в области осуществления банковской и финансовой деятельности, знания в реализации бизнес и технологических процессов организаций кредитно-финансовой сферы
	Применять при реализации технологических мер защиты информации знания по существующим практикам технологических мер защиты информации при реализации бизнес и технологических процессов организаций кредитно-финансовой сферы
	Принимать участие в реализации технологических мер защиты информации в ходе эксплуатации автоматизированных систем организации кредитно-финансовой сферы
	Принимать участие в реализации технологических мер защиты информации с учетом специфики реализации бизнес и технологических процессов организации кредитно-финансовой сферы
Необходимые знания	Требования законодательства Российской Федерации, нормативно-правовых актов Российской Федерации, нормативных актов Банка России в области применения технологических мер защиты информации в процессах, связанных с: - осуществлением переводов денежных средств в системах дистанционного банковского обслуживания; - осуществлением переводов денежных средств с использованием платежных карт; - реализацией операционных функций, передачей и обработкой электронных сообщений, в том числе в рамках переводов денежных средств, осуществления платежного клиринга и проведения иных форм безналичных расчетов; - наличным денежным обращением и кассовым обслуживанием
	Основные цели реализации технологических мер защиты информации при реализации бизнес и технологических процессов организаций кредитно-финансовой сферы
	Основы реализации технологических мер защиты информации в автоматизированных системах организации кредитно-финансовой сферы
	Состав и содержание ролей информационной безопасности в организации кредитно-финансовой сферы в рамках реализации технологических мер защиты информации
Другие характеристики	

3.3.3. Трудовая функция

Наименование	Контроль применения технологических мер защиты информации при реализации основных бизнес и технологических процессов организаций кредитно-финансовой сферы	Код	C/03.6	Уровень (подуровень) квалификации	6
Происхождение трудовой функции	Оригинал X	Заимствовано из оригинала			

	Код оригинала	Регистрационный номер профессионального стандарта
Трудовые действия	Участие в контроле применения технологических мер защиты информации в рамках реализации бизнес и технологических процессов организации кредитно-финансовой сферы	
	Участие в контроле применения технологических мер защиты информации применительно к объектам информационной инфраструктуры организации кредитно-финансовой сферы	
	Участие в контроле применения технологических мер защиты информации организации кредитно-финансовой сферы при осуществлении переводов денежных средств	
	Участие в контроле применения технологических мер защиты информации организации кредитно-финансовой сферы при осуществлении операций с платежными картами	
	Участие в контроле применения технологических мер защиты информации организации кредитно-финансовой сферы при передаче финансовых сообщений формата СВИФТ (SWIFT)	
	Участие в контроле применения технологических мер защиты информации в автоматизированных системах организации кредитно-финансовой сферы	
Необходимые умения	Применять при контроле технологических мер защиты информации знания в области осуществления банковской и финансовой деятельности, знания в реализации бизнес и технологических процессов организаций кредитно-финансовой сферы	
	Применять при контроле технологических мер защиты информации знания по существующим практикам технологических мер защиты информации при реализации бизнес и технологических процессов организаций кредитно-финансовой сферы	
	Принимать участие в контроле технологических мер защиты информации при реализации бизнес и технологических процессов организации кредитно-финансовой сферы	
	Принимать участие в контроле технологических мер защиты информации в ходе эксплуатации автоматизированных систем организации кредитно-финансовой сферы	
Необходимые знания	<p>Требования законодательства Российской Федерации, нормативно-правовых актов Российской Федерации, нормативных актов Банка России в области применения технологических мер защиты информации в процессах, связанных с:</p> <ul style="list-style-type: none"> - осуществлением переводов денежных средств в системах дистанционного банковского обслуживания; - осуществлением переводов денежных средств с использованием платежных карт; - реализацией операционных функций, передачей и обработкой электронных сообщений, в том числе в рамках переводов денежных средств, осуществления платежного клиринга и проведения иных форм безналичных расчетов; - наличным денежным обращением и кассовым обслуживанием 	

	Основные цели контроля технологических мер защиты информации при реализации бизнес и технологических процессов организаций кредитно-финансовой сферы
	Состав и содержание ролей информационной безопасности в организации кредитно-финансовой сферы в рамках реализации технологических мер защиты информации
	Принципы и правила контроля реализации технологических мер защиты информации в автоматизированных системах и информационной инфраструктуре организации кредитно-финансовой сферы на соответствие проектной и эксплуатационной документации
Другие характеристики	

3.4. Обобщенная трудовая функция

Наименование	Управление инцидентами защиты информации в организациях кредитно-финансовой сферы	Код	D	Уровень квалификации	6
Происхождение обобщенной трудовой функции	Оригинал	X	Заимствовано из оригинала		
				Код оригинала	Регистрационный номер профессионального стандарта
Возможные наименования должностей	Специалист по информационной безопасности Специалист по информационной безопасности 2 категории Специалист по информационной безопасности 1 категории Ведущий специалист по информационной безопасности Главный специалист по информационной безопасности				
Требования к образованию и обучению	Образовательные программы высшего образования – программы бакалавриата, специалитета, магистратуры Дополнительные профессиональные программы				
Требования к опыту практической работы	-				
Особые условия допуска к работе	-				

Дополнительные характеристики

Наименование документа	Код	Наименование базовой группы, должности (профессии) или специальности
ЕКС	-	Инженер-программист (программист)
	-	Инженер-программист по технической защите информации
	-	Инженер по защите информации

	-	Инженер-проектировщик
	-	Научный сотрудник
	-	Старший научный сотрудник
	-	Главный научный сотрудник
	-	Эксперт
	-	Администратор по обеспечению безопасности информации
	-	Главный специалист по технической защите информации
	-	Специалист по обеспечению безопасности информации в ключевых системах информационной инфраструктуры
ОКЗ	2153	Инженеры по телекоммуникациям
	2422	Специалисты в области политики администрирования
	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
	2519	Разработчики и аналитики программного обеспечения и приложений, не входящие в другие группы
	2611	Юристы
ОКСО	5.38.02.06	Финансы
	5.38.02.07	Банковское дело
	5.38.04.08	Финансы и кредит
	2.09.02.04	Информационные системы (по отраслям)
	2.09.02.05	Прикладная информатика (по отраслям)
	2.10.02.01	Организация и технология защиты информации
	2.10.02.02	Информационная безопасность телекоммуникационных систем
	2.10.02.03	Информационная безопасность автоматизированных систем
	2.09.03.02	Информационные системы и технологии
	2.09.03.03	Прикладная информатика
	2.09.03.04	Программная инженерия
	2.10.03.01	Информационная безопасность
	1.02.04.01	Математика и компьютерные науки
	1.02.04.02	Фундаментальная информатика и информационные технологии
	1.02.04.03	Математическое обеспечение и администрирование информационных систем
	2.09.04.02	Информационные системы и технологии
	2.09.04.03	Прикладная информатика
	2.09.04.04	Программная инженерия
	2.10.04.01	Информационная 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
	1.02.06.01	Компьютерные и информационные науки
	2.09.06.01	Информатика и вычислительная техника
	2.10.06.01	Информационная безопасность
	1.02.07.01	Компьютерные и информационные науки
	2.10.07.01	Информационная безопасность
	5.38.05.01	Экономическая безопасность
	5.38.07.02	Экономическая безопасность
	5.40.06.01	Юриспруденция

ОКПДТР	20911	Главный специалист по защите информации
	22567	Инженер по защите информации
	22824	Инженер-программист
	22870	Инженер электросвязи
	24392	Научный сотрудник (в области информатики и вычислительной техники)
	26579	Специалист по защите информации
	40064	Администратор баз данных
	40067	Администратор вычислительной сети
	40070	Администратор информационной безопасности вычислительной сети
	42843	Инженер - системный программист
	44544	Начальник исследовательской группы
	46115	Руководитель аналитической группы подразделения по комплексной защите информации
	051319	Методы и системы защиты информации, информационная безопасность
	24062	Менеджер (в финансово-экономических и административных подразделениях (службах))

3.4.1. Трудовая функция

Наименование	Организация процессов управления инцидентами защиты информации в организациях кредитно-финансовой сферы	Код	D/01.6	Уровень (подуровень) квалификации	6
--------------	---	-----	--------	-----------------------------------	---

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

Трудовые действия	<p>Участие в разработке плана управления инцидентами защиты информации и обеспечения ситуационной осведомленности организации кредитно-финансовой сферы</p> <p>Классификации инцидентов защиты информации организации кредитно-финансовой сферы</p> <p>Определение и организация стадий обработки инцидентов защиты информации организации кредитно-финансовой сферы</p> <p>Определение организационной структуры группы реагирования на инциденты защиты информации организации кредитно-финансовой сферы</p> <p>Определение технического обеспечения организации кредитно-финансовой сферы для осуществления деятельности по управлению инцидентами защиты информации</p> <p>Выявление и реагирование на инциденты защиты информации организации кредитно-финансовой сферы</p> <p>Своевременная обработка инцидентов защиты информации организации кредитно-финансовой сферы</p> <p>Регламентация и выполнение деятельности по расследованию и анализу инцидентов защиты информации организации кредитно-финансовой сферы</p> <p>Организация процесса сбора технических данных в случае реализации инцидентов защиты информации организации кредитно-финансовой сферы</p> <p>Планирование и регламентацию процесса сбора технических данных, в случае реализации инцидентов защиты информации организации кредитно-финансовой сферы</p> <p>Определение общего состава действий при сборе технических данных в случае реализации инцидентов защиты информации организации кредитно-финансовой сферы</p>
Необходимые умения	<p>Участвовать в организации и планировании деятельности служб информационной безопасности организации кредитно-финансовой сферы применительно к процессам мониторинга и управления инцидентами защиты информации</p> <p>Участвовать в концептуальном, архитектурном и техническом проектировании реализации процессов мониторинга и управления инцидентами защиты информации в информационной инфраструктуре организаций кредитно-финансовой сферы</p> <p>Разрабатывать функционально-технические требования к системам сбора данных для сбора технических данных в случае реализации инцидентов защиты информации организации кредитно-финансовой сферы</p> <p>Принимать участие в выборе технических средств защиты информации для применения в рамках управления инцидентами защиты информации организации кредитно-финансовой сферы</p> <p>Применять и работать с техническими средствами защиты информации и системами, реализующими функции управления инцидентами защиты информации организации кредитно-финансовой сферы</p> <p>Формировать требования к объектам сбора технических данных процессов управления инцидентами защиты информации для объектов информационной инфраструктуры организаций кредитно-финансовой сферы</p>

	сферы в соответствии с организацией бизнес и технологических процессов
	Принимать участие в настройке средств (агентов, интерфейсов) сбора технических данных и настройке подсистем, в обработке этих данных для выявления событий и инцидентов защиты информации организации кредитно-финансовой сферы
	Принимать участие в мероприятиях по реализации процессов управления инцидентами защиты информации, сборе и обработке сведений и технических данных об инцидентах защиты информации организации кредитно-финансовой сферы
	Выявлять и реагировать на инциденты защиты информации организации кредитно-финансовой сферы
	Обрабатывать инциденты защиты информации организации кредитно-финансовой сферы
	Участвовать в расследовании и анализе инцидентов защиты информации организации кредитно-финансовой сферы
	Организовывать и осуществлять сбор технических данных в случае реализации инцидентов защиты информации организации кредитно-финансовой сферы
Необходимые знания	Требования законодательства Российской Федерации по вопросам управления инцидентами защиты информации и обеспечения ситуационной осведомленности организации кредитно-финансовой сферы
	Требования нормативных актов Банка России по вопросам управления инцидентами защиты информации и обеспечения ситуационной осведомленности организации кредитно-финансовой сферы
	Требования национальных и международных документов в области стандартизации управления инцидентами защиты информации и обеспечения ситуационной осведомленности организации кредитно-финансовой сферы
	Требования документов Банка России в области стандартизации управления инцидентами защиты информации и обеспечения ситуационной осведомленности организации кредитно-финансовой сферы
	Источники возникновения, классификация и технические характеристики инцидентов защиты информации объектов информационной инфраструктуры организаций кредитно-финансовой сферы
	Состав уязвимостей и угроз информационной безопасности в целях сбора данных о событиях защиты информации организации кредитно-финансовой сферы
	Состав, принципы, условия реализации процессов мониторинга и управления инцидентами защиты информации в организации кредитно-финансовой сферы
	Состав и основные функциональные возможности технических средств защиты информации и систем мониторинга информационной безопасности, предназначенных для применения в рамках процессов управления инцидентами защиты информации в организации кредитно-финансовой сферы

	Порядок обработки инцидентов защиты информации и обеспечения ситуационной осведомленности организации кредитно-финансовой сферы
	Виды и типы инцидентов защиты информации организации кредитно-финансовой сферы
	Порядок проведения расследования инцидентов защиты информации организации кредитно-финансовой сферы
	Порядок сбора технических данных в случае реализации инцидентов защиты информации организации кредитно-финансовой сферы
Другие характеристики	

3.4.2. Трудовая функция

Наименование	Организация мониторинга информационной безопасности в организациях кредитно-финансовой сферы	Код	D/02.6	Уровень (подуровень) квалификации	6
--------------	--	-----	--------	-----------------------------------	---

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

Трудовые действия	Мониторинг системы управления инцидентами защиты информации и обеспечения ситуационной осведомленности организации кредитно-финансовой сферы
	Контроль за фактическими значениями ключевых индикаторов риска, связанных с управлением инцидентами защиты информации и обеспечения ситуационной осведомленности организации кредитно-финансовой сферы
	Контроль процедуры сбора и регистрации информации о реализации инцидентов защиты информации организации кредитно-финансовой сферы
	Определение ролей, связанных с мониторингом системы управления инцидентами защиты информации и обеспечения ситуационной осведомленности организации кредитно-финансовой сферы
	Определение и согласование процедуры стрестестирования системы управления инцидентами защиты информации и обеспечения ситуационной осведомленности организации кредитно-финансовой сферы
	Организация стрестестирования, разработка плана управления инцидентами защиты информации и обеспечения ситуационной осведомленности организации кредитно-финансовой сферы
	Определение ролей, связанных с выполнением деятельности по стрестестированию плана управления инцидентами защиты информации и обеспечения ситуационной осведомленности организации кредитно-финансовой сферы

Необходимые умения	<p>Применять и работать с техническими средствами защиты информации и системами, реализующими функции оперативного мониторинга, обнаружения вторжений и сетевых атак, направленных на организации кредитно-финансовой сферы</p>
	<p>Работать с конфигурациями средств сбора технических данных мониторинга и настройки подсистем обработки этих данных для выявления событий и инцидентов защиты информации организации кредитно-финансовой сферы</p>
	<p>Осуществлять контроль процедуры сбора и регистрации информации о реализации инцидентов защиты информации</p>
	<p>Осуществлять контроль за фактическими значениями ключевых индикаторов риска, связанных с управлением инцидентами защиты информации и обеспечения ситуационной осведомленности организации кредитно-финансовой сферы</p>
	<p>Участвовать в проведении мероприятий по стрестестированию системы управления инцидентами защиты информации и обеспечения ситуационной осведомленности организации кредитно-финансовой сферы</p>
	<p>Принимать участие в проведении оценки эффективности реализуемых процессов мониторинга и управления инцидентами защиты информации и формировании предложений по развитию и совершенствованию указанных процессов организации кредитно-финансовой сферы</p>
Необходимые знания	<p>Требования законодательства Российской Федерации по вопросам мониторинга защиты информации в организациях кредитно-финансовой сферы</p>
	<p>Требования нормативных актов Банка России по вопросам мониторинга защиты информации в организациях кредитно-финансовой сферы</p>
	<p>Требования национальных и международных документов в области стандартизации мониторинга защиты информации в организациях кредитно-финансовой сферы</p>
	<p>Требования документов Банка России в области стандартизации мониторинга защиты информации в организациях кредитно-финансовой сферы</p>
	<p>Источники возникновения, классификация и технические характеристики инцидентов защиты информации объектов информационной инфраструктуры организаций кредитно-финансовой сферы</p>
	<p>Состав уязвимостей и угроз информационной безопасности в целях сбора данных о событиях защиты информации организации кредитно-финансовой сферы</p>
	<p>Состав, принципы, условия реализации процессов мониторинга и управления инцидентами защиты информации в организации кредитно-финансовой сферы</p>
	<p>Состав и основные функциональные возможности технических средств защиты информации и систем мониторинга информационной безопасности, предназначенных для применения в рамках процессов управления инцидентами защиты информации в организации кредитно-финансовой сферы</p>
	<p>Состав и основные функциональные возможности технических средств защиты информации и систем мониторинга информационной</p>

	безопасности, предназначенных для применения в рамках процессов управления инцидентами защиты информации в организации кредитно-финансовой сферы
Другие характеристики	

3.4.3. Трудовая функция

Наименование	Организация взаимодействия организаций кредитно-финансовой сферы с ФинЦЕРТ Банка России	Код	D/03.6	Уровень (подуровень) квалификации	6
--------------	---	-----	--------	-----------------------------------	---

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

Трудовые действия	Определение и утверждение процедуры взаимодействия с ФинЦЕРТ Банка России по вопросам информирования об инцидентах, связанных с нарушением требований к обеспечению защиты информации
	Организация процедуры сбора и предоставления информации для выполнения информирования ФинЦЕРТ Банка России об инцидентах, связанных с нарушением требований к обеспечению защиты информации, с учетом сроков их представления в ФинЦЕРТ Банка России
	Организация процедуры сбора и предоставления информации для выполнения информирования ФинЦЕРТ Банка России в случае проверки конкретного получателя средств, а также в части приостановления (невозможности приостановления) зачисления денежных средств на банковский счет получателя средств или увеличения остатка электронных денежных средств получателя средств
	Организация процедуры сбора и предоставления информации для выполнения информирования ФинЦЕРТ Банка России об установлении (или снятии) на банковские (корреспондентские) счета (субсчета) ограничения в виде запрета на списание денежных средств при выявлении инцидентов, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств
	Организация процедуры учета и применения распространяемой ФинЦЕРТ Банка России информации об инцидентах, связанных с нарушением требований к обеспечению защиты информации
	Организация процедуры сбора и предоставления информации для выполнения информирования ФинЦЕРТ Банка России о планируемых мероприятиях по раскрытию информации о выявленных инцидентах, связанных с нарушением требований к обеспечению защиты информации, с учетом сроков их представления в ФинЦЕРТ Банка России

	Контроль применения установленных условий представления в ФинЦЕРТ Банка России данных о выявленных инцидентах, связанных с нарушением требований к обеспечению защиты информации
	Контроль применения технологии подготовки и направления электронных сообщений при информационном обмене с Банком России
Необходимые умения	Принимать участие в организации и осуществлению информационного обмена с ФинЦЕРТ Банка России об инцидентах, связанных с нарушением требований к обеспечению защиты информации организации кредитно-финансовой сферы
	Принимать участие в мероприятиях организации кредитно-финансовой сферы по взаимодействию с ФинЦЕРТ Банка России при реагировании на инциденты, связанные с нарушением требований к обеспечению защиты информации
	Работать с техническими средствами и системами осуществления информационного обмена с ФинЦЕРТ Банка России об инцидентах, связанных с нарушением требований к обеспечению защиты информации организации кредитно-финансовой сферы
Необходимые знания	Требования законодательства Российской Федерации по вопросам взаимодействия организаций кредитно-финансовой сферы с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на объекты информционной системы Российской Федерации
	Требования нормативных актов Банка России по вопросам взаимодействия организаций кредитно-финансовой сферы с ФинЦЕРТ Банка России
	Требования национальных стандартов в области взаимодействия организаций кредитно-финансовой сферы с ФинЦЕРТ Банка России
	Основные цели и процедуры организации взаимодействия организации кредитно-финансовой сферы с ФинЦЕРТ Банка России
	Порядок подключения организации кредитно-финансовой сферы к информационному обмену с ФинЦЕРТ Банка России
Другие характеристики	

3.4.4. Трудовая функция

Наименование	Организация взаимодействия организаций кредитно-финансовой сферы с правоохранительными органами	Код	D/04.6	Уровень (подуровень) квалификации	6
Происхождение трудовой функции	Оригинал <input checked="" type="checkbox"/>	Заимствовано из оригинала			
			Код оригинала	Регистрационный номер профессионального стандарта	
Трудовые действия	Организация процедуры взаимодействия организации кредитно-финансовой сферы с правоохранительными органами РФ в части				

	<p>выполнения сбора, упаковки, хранения и транспортировки технических данных потенциально обладающих содержательной (семантической) информацией</p> <p>Выполнение документирования результатов выделения и анализа содержательной (семантической) информации, предполагаемых к передаче в правоохранительные органы</p> <p>Определение и применение способов непосредственного сбора технических данных потенциально обладающих содержательной (семантической) информацией</p> <p>Организация выполнения «криминалистического» копирования (создания образов) энергонезависимых технических данных потенциально обладающих содержательной (семантической) информацией</p> <p>Организация выполнения копирования содержимого оперативной памяти средств вычислительной техники и получению данных операционных систем</p> <p>Организация выполнения выполнению копирования протоколов (журналов) регистрации</p> <p>Организация выполнения копирования сетевого трафика</p> <p>Рекомендации по обеспечению безопасной упаковки, хранения и транспортировки носителей, собранных данных</p> <p>Организация применения технических средств сбора и обработки технических данных</p>
Необходимые умения	<p>Документировать результаты выделения и анализа содержательной (семантической) информации, предполагаемых к передаче в правоохранительные органы</p> <p>Участвовать в расследовании и анализе инцидентов защиты информации организации кредитно-финансовой сферы</p> <p>Организовывать и осуществлять сбор технических данных для передачи в правоохранительные органы в случае реализации инцидентов защиты информации организации кредитно-финансовой сферы</p>
Необходимые знания	<p>Требования законодательства Российской Федерации по вопросам взаимодействия организаций кредитно-финансовой сферы с правоохранительными органами</p> <p>Требования нормативных актов Банка России по вопросам взаимодействия организаций кредитно-финансовой сферы с правоохранительными органами</p> <p>Требования национальных стандартов в области взаимодействия организаций кредитно-финансовой сферы с ФинЦЕРТ Банка России правоохранительными органами</p> <p>Требования стандартов Банка России в области взаимодействия организаций кредитно-финансовой сферы с правоохранительными органами</p> <p>Основные цели и процедуры организации взаимодействия организаций кредитно-финансовой сферы с правоохранительными органами</p> <p>Основные цели и процедуры организации взаимодействия организаций кредитно-финансовой сферы с правоохранительными органами</p> <p>Порядок проведения расследования инцидентов защиты информации организации кредитно-финансовой сферы</p> <p>Порядок сбора технических данных в случае реализации инцидентов защиты информации организации кредитно-финансовой сферы</p>

Другие характеристики	
-----------------------	--

3.4.5. Трудовая функция

Наименование	Подготовка отчетности по информационной безопасности организаций кредитно-финансовой сферы	Код	D/05.6	Уровень (подуровень) квалификации	6
--------------	--	-----	--------	-----------------------------------	---

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

Трудовые действия	Сбор данных для подготовки отчетности по информационной безопасности организаций кредитно-финансовой сферы
	Подготовка внутренней отчетности организации кредитно-финансовой сферы в рамках деятельности по управлению инцидентами защиты информации
	Подготовка отчетности по информационной безопасности организаций кредитно-финансовой сферы, предоставляемой в Банк России
	Отправка в Банк России отчетности по информационной безопасности организаций кредитно-финансовой сферы
Необходимые умения	Принимать участие в подготовке отчетности по инцидентам защиты информации организации кредитно-финансовой сферы
	Взаимодействовать с структурными подразделениями организации кредитно-финансовой сферы при сборе данных для подготовки отчетности по информационной безопасности
	Заполнять формы отчетности по информационной безопасности организаций кредитно-финансовой сферы
Необходимые знания	Требования законодательства Российской Федерации по вопросам подготовки отчетности по информационной безопасности организаций кредитно-финансовой сферы
	Требования нормативных актов Банка России по вопросам подготовки отчетности по информационной безопасности организаций кредитно-финансовой сферы
	Требования международных и национальных стандартов в области подготовки отчетности по информационной безопасности организаций кредитно-финансовой сферы
	Требования стандартов Банка России в области подготовки отчетности по информационной безопасности организаций кредитно-финансовой сферы
	Основные цели подготовки отчетности по информационной безопасности организаций кредитно-финансовой сферы
	Основные формы отчетности по информационной безопасности организаций кредитно-финансовой сферы

	Порядок подготовки и заполнения форм отчетности по информационной безопасности организаций кредитно-финансовой сферы
	Порядок предоставления отчетности по информационной безопасности организации кредитно-финансовой сферы в Банк России
Другие характеристики	

3.5. Обобщенная трудовая функция

Наименование	Контроль информационной безопасности в организациях кредитно-финансовой сферы	Код	Е	Уровень квалификации	6
Происхождение обобщенной трудовой функции	Оригинал <input checked="" type="checkbox"/>	Заимствовано из оригинала			
		Код оригинала		Регистрационный номер профессионального стандарта	
Возможные наименования должностей	Специалист по информационной безопасности Специалист по информационной безопасности 2 категории Специалист по информационной безопасности 1 категории Ведущий специалист по информационной безопасности Главный специалист по информационной безопасности				
Требования к образованию и обучению	Образовательные программы высшего образования – программы бакалавриата, специалитета, магистратуры Дополнительные профессиональные программы				
Требования к опыту практической работы	-				
Особые условия допуска к работе	-				

Дополнительные характеристики

Наименование документа	Код	Наименование базовой группы, должности (профессии) или специальности
ЕКС		
	-	Инженер-программист (программист)
	-	Инженер-программист по технической защите информации
	-	Инженер по защите информации
	-	Инженер-проектировщик
	-	Научный сотрудник
	-	Старший научный сотрудник
	-	Главный научный сотрудник
	-	Эксперт

	-	Администратор по обеспечению безопасности информации
	-	Главный специалист по технической защите информации
	-	Специалист по обеспечению безопасности информации в ключевых системах информационной инфраструктуры
ОКЗ	2153	Инженеры по телекоммуникациям
	2422	Специалисты в области политики администрирования
	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
	2519	Разработчики и аналитики программного обеспечения и приложений, не входящие в другие группы
	2611	Юристы
ОКСО	5.38.02.06	Финансы
	5.38.02.07	Банковское дело
	5.38.04.08	Финансы и кредит
	2.09.02.04	Информационные системы (по отраслям)
	2.09.02.05	Прикладная информатика (по отраслям)
	2.10.02.01	Организация и технология защиты информации
	2.10.02.02	Информационная безопасность телекоммуникационных систем
	2.10.02.03	Информационная безопасность автоматизированных систем
	2.09.03.02	Информационные системы и технологии
	2.09.03.03	Прикладная информатика
	2.09.03.04	Программная инженерия
	2.10.03.01	Информационная безопасность
	1.02.04.01	Математика и компьютерные науки
	1.02.04.02	Фундаментальная информатика и информационные технологии
	1.02.04.03	Математическое обеспечение и администрирование информационных систем
	2.09.04.02	Информационные системы и технологии
	2.09.04.03	Прикладная информатика
	2.09.04.04	Программная инженерия
	2.10.04.01	Информационная 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
	1.02.06.01	Компьютерные и информационные науки
	2.09.06.01	Информатика и вычислительная техника
	2.10.06.01	Информационная безопасность
	1.02.07.01	Компьютерные и информационные науки
	2.10.07.01	Информационная безопасность
	5.38.05.01	Экономическая безопасность
	5.38.07.02	Экономическая безопасность
	5.40.06.01	Юриспруденция

ОКПДТР	20911	Главный специалист по защите информации
	22567	Инженер по защите информации
	22824	Инженер-программист
	22870	Инженер электросвязи
	24392	Научный сотрудник (в области информатики и вычислительной техники)
	26579	Специалист по защите информации
	40064	Администратор баз данных
	40067	Администратор вычислительной сети
	40070	Администратор информационной безопасности вычислительной сети
	42843	Инженер - системный программист
	44544	Начальник исследовательской группы
	46115	Руководитель аналитической группы подразделения по комплексной защите информации
	051319	Методы и системы защиты информации, информационная безопасность
	24062	Менеджер (в финансово-экономических и административных подразделениях (службах))

3.5.1. Трудовая функция

Наименование	Проведение внутреннего контроля управлением риском реализации информационных угроз в организациях кредитно-финансовой сферы	Код	E/01.6	Уровень (подуровень) квалификации	6
Происхождение трудовой функции	Оригинал <input checked="" type="checkbox"/>	Заимствовано из оригинала		Код оригинала	Регистрационный номер профессионального стандарта
Трудовые действия	Сбор и регистрация информации об инцидентах защиты информации в целях мониторинга уровня риска реализации информационных угроз организации кредитно-финансовой сферы				

	Контроль за уровнем риска реализации информационных угроз организации кредитно-финансовой сферы
	Организация и участие в анализе и контроле адекватности идентификации области применения системы управления риском реализации информационных угроз организации кредитно-финансовой сферы
	Организация и участие в анализе и контроле адекватности идентификации области применения иных систем управления в рамках ключевых направлений обеспечения информационной безопасности организации кредитно-финансовой сферы
	Проведение анализа и контроля адекватности моделей угроз безопасности информации организации кредитно-финансовой сферы
	Организация и участие в анализе и контроле адекватности оценки риска реализации информационных угроз организации кредитно-финансовой сферы
	Реализация системы внутренней отчетности в рамках управления риском реализации информационных угроз организации кредитно-финансовой сферы
	Контроль применения способа реагирования на риск реализации информационных угроз организации кредитно-финансовой сферы
	Контроль применения мер, направленных на предотвращение (снижение степени вероятности реализации) реализации инцидентов защиты информации
	Контроль применения мер, направленных на ограничение (снижение степени тяжести потерь) потерь в результате реализации инцидентов защиты информации
Необходимые умения	Осуществлять сбор и регистрацию информации об инцидентах защиты информации в целях мониторинга уровня риска реализации информационных угроз организации кредитно-финансовой сферы
	Осуществлять контроль за уровнем риска реализации информационных угроз
	Формировать отчетность по результатам контроля управления риском реализации информационных угроз организации кредитно-финансовой сферы
	Осуществлять контроль применения способа реагирования на риск реализации информационных угроз организации кредитно-финансовой сферы
	Осуществлять контроль применения мер, направленных на предотвращение (снижение степени вероятности реализации) реализации инцидентов защиты информации
	Осуществлять контроль применения мер, направленных на ограничение (снижение степени тяжести потерь) потерь в результате реализации инцидентов защиты информации
Необходимые знания	Требования законодательства Российской Федерации, нормативно-правовых актов Российской Федерации, нормативных актов Банка России в области обеспечения защиты информации, распространяющиеся на деятельность организаций кредитно-финансовой сферы в части организации контрольных мероприятий
	Требования национальных и международных документов в области стандартизации обеспечения защиты информации организаций

	кредитно-финансовой сферы, регламентирующих проведение контрольных мероприятий в области защиты информации
	Основные риски реализации информационных угроз в рамках бизнес и технологических процессов организаций кредитно-финансовой сферы
	Принципы управления рисками реализации информационных угроз организаций кредитно-финансовой сферы
	Состав, назначение и основные цели проведения мероприятий по контролю управлением риском реализации информационных угроз в организации кредитно-финансовой сферы
	Методология проведения оперативного и периодического контроля управлением риском реализации информационных угроз в организации кредитно-финансовой сферы
Другие характеристики	

3.5.2. Трудовая функция

Наименование	Проведение внутреннего контроля защиты информации организаций в организациях кредитно-финансовой сферы	Код	Е/02.6	Уровень (подуровень) квалификации	6
--------------	--	-----	--------	-----------------------------------	---

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

Трудовые действия	Контроль фактического состава объектов и ресурсов доступа, входящих в область применения процесса системы защиты информации, на соответствие учетным данным
	Контроль фактического размещения технических мер защиты информации в информационной инфраструктуре
	Контроль фактических параметров настроек технических мер защиты информации и компонентов информационной инфраструктуры, предназначенных для размещения технических мер защиты информации
	Контроль назначения ролей, связанных с эксплуатацией и использованием по назначению технических мер защиты информации
	Контроль выполнения руководств по эксплуатации и использованию по назначению технических мер защиты информации
	Периодический контроль (тестирование) полноты реализации технических мер защиты информации
	Контроль применения организационных мер защиты информации
	Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование

	<p>Проведение проверок знаний работников организации в части применения мер защиты информации в рамках процесса системы защиты информации</p> <p>Фиксация и оформление результатов (свидетельств) проведения мероприятий по контролю реализации процесса системы защиты информации</p> <p>Осуществление регистрации операций по установке и (или) обновлению программного обеспечения технических средств защиты информации</p> <p>Осуществление регистрации операций по обновлению сигнатурных баз технических средств защиты информации</p> <p>Осуществление регистрации операций по изменению параметров настроек технических мер защиты информации и информационной инфраструктуры, предназначенных для размещения технических мер защиты информации</p> <p>Осуществление регистрации сбоев (отказов) технических мер защиты информации</p>
Необходимые умения	<p>Принимать участие в контроле реализации технических средств защиты информации и систем обеспечения защиты информации в информационной инфраструктуре организаций кредитно-финансовой сферы</p> <p>Организовывать и осуществлять самооценку соответствия процессов обеспечения защиты информации положениям документов Банка России в области стандартизации обеспечения информационной безопасности организации кредитно-финансовой сферы, требованиям правил платежных систем</p> <p>Определять объекты контроля защищенности из состава объектов информационной инфраструктуры организаций кредитно-финансовой сферы</p> <p>Принимать участие в реализации контроля защищенности объектов информационной инфраструктуры организаций кредитно-финансовой сферы</p> <p>Организовывать категорирование объектов информационной инфраструктуры организации кредитно-финансовой сферы для осуществления мониторинга защиты информации</p> <p>Принимать участие в мероприятиях по операционному и периодическому контролю реализации процессов обеспечения защиты информации в организации кредитно-финансовой сферы</p> <p>Применять и принимать участие в выборе технических средств защиты информации, средств мониторинга информационной безопасности и системы обеспечения защиты информации, реализующие функции оперативного мониторинга, обнаружения вторжений и сетевых атак, направленных на организации кредитно-финансовой сферы</p> <p>Формировать правила анализа данных мониторинга информационной безопасности, в том числе для целей выявления событий и инцидентов защиты информации</p> <p>Формировать отчетность по результатам контроля защиты информации</p> <p>Применять навыки контроля назначенных ролей, исполнения планов повышения осведомленности в области защиты информации</p> <p>Формировать функциональные требования к средствам и технологиям контроля защиты информации и осуществлять выбор таких средств и технологий</p>

	Организовывать и (или) осуществлять контроль внедрения средств и технологий оперативного и периодического контроля защиты информации
	Принимать участие в проектировании и регламентации оперативного и периодического контроля реализации процессов обеспечения защиты информации
	Организовать и (или) непосредственно осуществлять анализ данных (информации) мониторинга информационной безопасности и формировать правила анализа
Необходимые знания	Требования законодательства Российской Федерации, нормативно-правовых актов Российской Федерации, нормативных актов Банка России в области обеспечения защиты информации, распространяющиеся на деятельность организаций кредитно-финансовой сферы в части организации контрольных мероприятий
	Требования национальных и международных документов в области стандартизации обеспечения защиты информации организаций кредитно-финансовой сферы, регламентирующих проведение контрольных мероприятий в области защиты информации
	Функционально-технические требования к техническим средствам защиты информации и системам обеспечения защиты информации организаций кредитно-финансовой сферы в целях их контроля
	Состав, назначение и основные цели проведения мероприятий по обеспечению контроля защищенности объектов информационной инфраструктуры организаций кредитно-финансовой сферы
	Состав, назначение и основные цели проведения контрольных мероприятий по обнаружению вторжений и сетевых атак, направленных на информационную инфраструктуру организаций кредитно-финансовой сферы
	Цели и правила организации контрольных мероприятий по оперативному мониторингу, сбору и обработке сведений и иных технических данных об инцидентах защиты информации
	Состав, назначение и основные цели операционного и периодического контроля реализации процессов обеспечения защиты информации в организациях кредитно-финансовой сферы
	Принципы и правила контроля применения технических средств защиты информации и систем обеспечения защиты информации в информационной инфраструктуре организаций кредитно-финансовой сферы
	Принципы и правила контроля состава объектов информационной инфраструктуры организаций кредитно-финансовой сферы, включая автоматизированные системы и их компоненты, задействованные в реализации бизнес и технологических процессов организаций кредитно-финансовой сферы (автоматизированные рабочие места пользователей и эксплуатационного персонала, серверное и сетевое оборудование, системы хранения данных, аппаратные модули безопасности (HSM), устройства печати и копирования информации, объекты доступа, расположенные в публичных (общедоступных) местах (в том числе банкоматы, платежные терминалы)
	Принципы и правила контроля состава ресурсов доступа информационной инфраструктуры организаций кредитно-финансовой сферы (автоматизированные системы, базы данных, сетевые файловые

	ресурсы, виртуальные машины, предназначенные для размещения серверных компонентов АС, ресурсы доступа, относящиеся к сервисам электронной почты, а также к WEB-сервисам организации КФС в сети Интранет и Интернет)
	Основы действующей системы аттестации объектов информатизации; виды и содержание отчетности по результатам контроля защиты информации
	Состав и основные функциональные возможности технических средств защиты информации, средств мониторинга информационной безопасности и систем обеспечения защиты информации, реализующих функции оперативного мониторинга, обнаружения вторжений и сетевых атак, направленных на организации кредитно-финансовой сферы
	Возможности по регистрации событий для типовых компонентов информационной инфраструктуры организаций кредитно-финансовой сферы
	Методология проведения оперативного и периодического контроля реализации процессов обеспечения защиты информации в организациях кредитно-финансовой сферы
Другие характеристики	

3.5.3. Трудовая функция

Наименование	Проведение внутреннего контроля защиты информации для непрерывности выполнения бизнес- и технологических процессов организаций кредитно-финансовой сферы	Код	Е/03.6	Уровень (подуровень) квалификации	6
Происхождение трудовой функции	Оригинал <input checked="" type="checkbox"/>	Заемствовано из оригинала			
			Код оригинала	Регистрационный номер профессионального стандарта	
Трудовые действия	Контроль за фактическими значениями ключевых индикаторов риска, связанных с обеспечением защиты информации для непрерывности выполнения бизнес- и технологических процессов				
	Сбор и регистрацию информации о функционировании объектов информатизации инфраструктурного уровня, используемых организацией кредитно-финансовой сферы				
	Организация и участие в проведении анализа и контроля адекватности идентификации области применения системы обеспечения защиты информации для непрерывности выполнения бизнес- и технологических процессов организации кредитно-финансовой сферы				
	Реализация системы внутренней отчетности в рамках обеспечения защиты информации для непрерывности выполнения бизнес- и технологических процессов организации кредитно-финансовой сферы				

	<p>Участие в тестировании плана обеспечения непрерывности и восстановление деятельности в случае чрезвычайных ситуаций и оценка эффективности обеспечения защиты информации для непрерывности выполнения бизнес- и технологических процессов организации кредитно-финансовой сферы, реализуемого в рамках указанного плана.</p> <p>Организация и проведение тестирования плана восстановления непрерывности выполнения бизнес- и технологических процессов организации кредитно-финансовой сферы при реализации инцидентов защиты информации</p> <p>Оценка эффективности плана восстановления непрерывности выполнения бизнес- и технологических процессов организации кредитно-финансовой сферы при реализации инцидентов защиты информации</p> <p>Контроль применения мер, направленных на обеспечение защиты информации для непрерывности выполнения бизнес- и технологических процессов организации кредитно-финансовой сферы</p> <p>Планирование и реализация программ по самооценке полноты и качества состава мер по реализации требований к процессам обеспечения защиты информации для непрерывности выполнения бизнес- и технологических процессов организации кредитно-финансовой сферы</p>
Необходимые умения	<p>Осуществлять сбор и регистрацию информации о функционировании объектов информатизации инфраструктурного уровня, используемых организацией кредитно-финансовой сферы</p> <p>Осуществлять контроль применения мер, направленных на обеспечение защиты информации для непрерывности выполнения бизнес- и технологических процессов организации кредитно-финансовой сферы</p> <p>Формировать отчетность по результатам контроля защиты информации для непрерывности выполнения бизнес- и технологических процессов организации кредитно-финансовой сферы</p> <p>Разрабатывать предложения в планы и программы по самооценке полноты и качества состава мер по реализации требований к процессам обеспечения защиты информации для непрерывности выполнения бизнес- и технологических процессов организации кредитно-финансовой сферы</p>
Необходимые знания	<p>Требования законодательства Российской Федерации, нормативно-правовых актов Российской Федерации, нормативных актов Банка России в области обеспечения защиты информации, распространяющиеся на деятельность организаций кредитно-финансовой сферы в части организации контрольных мероприятий</p> <p>Требования национальных и международных документов в области стандартизации обеспечения защиты информации организаций кредитно-финансовой сферы, регламентирующих проведение контрольных мероприятий в области защиты информации</p> <p>Основные организационные меры защиты информации для непрерывности выполнения бизнес- и технологических процессов организаций кредитно-финансовой сферы</p> <p>Основные технические меры защиты информации для непрерывности выполнения бизнес- и технологических процессов организаций кредитно-финансовой сферы</p>

	Принципы контроля защиты информации для непрерывности выполнения бизнес- и технологических процессов организаций кредитно-финансовой сферы
	Состав, назначение и основные цели проведения мероприятий по контролю защиты информации для непрерывности выполнения бизнес- и технологических процессов организаций кредитно-финансовой сферы
	Методология проведения оперативного и периодического контроля защиты информации для непрерывности выполнения бизнес- и технологических процессов организаций кредитно-финансовой сферы
Другие характеристики	

3.5.4. Трудовая функция

Наименование	Проведение внутреннего контроля управления риском реализации информационных угроз при аутсорсинге и использовании сторонних информационных сервисов в организациях кредитно-финансовой сферы	Код	E/04.6	Уровень (подуровень) квалификации	6
--------------	--	-----	--------	-----------------------------------	---

Происхождение
трудовой функции

Оригинал	X	Заимствовано из оригинала		
			Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Контроль за уровнем риска реализации информационных угроз при аутсорсинге и использовании сторонних информационных сервисов
	Организация сбора и регистрации информации об инцидентах защиты информации в случае реализации риска информационных угроз при аутсорсинге и использовании сторонних информационных сервисов
	Контроль применения мер, направленных на проведение оценки поставщика услуг, выполняющего бизнес и (или) технологические процессы организации кредитно-финансовой сферы на аутсорсинге, в части ресурсного обеспечения
	Контроль применения мер, направленных на проведение оценки поставщика услуг, выполняющего бизнес и (или) технологические процессы организации кредитно-финансовой сферы на аутсорсинге, в части соблюдения требований к защите информации
	Контроль применения мер, направленных на проведение оценки поставщика услуг, выполняющего бизнес и (или) технологические процессы организации кредитно-финансовой сферы на аутсорсинге, в части соблюдения требований к обеспечению непрерывности деятельности
	Реализацию системы внутренней отчетности в рамках внутреннего контроля управления риском реализации информационных угроз при аутсорсинге и использовании сторонних информационных сервисов

	<p>Планирование и реализацию программ проведения самооценки полноты и качества реализации настоящих требований к процессам</p> <p>Определение и назначение ролей, связанных с выполнением деятельности по контролю за эффективностью управления риском реализации информационных угроз при аутсорсинге и использовании сторонних информационных сервисов</p> <p>Определение и назначение ролей, связанных с контролем системы мер, направленных на снижение риска реализации информационных угроз</p>
Необходимые умения	<p>Осуществлять сбор и регистрацию информации об инцидентах защиты информации в случае реализации риска информационных угроз при аутсорсинге и использовании сторонних информационных сервисов</p> <p>Осуществлять контроль применения мер, направленных на обеспечение защиты информации при аутсорсинге и использовании сторонних информационных сервисов</p> <p>Формировать отчетность по результатам контроля защиты информации при управлении риском информационных угроз при аутсорсинге и использовании сторонних информационных сервисов</p> <p>Разрабатывать предложения в планы и программы по самооценке полноты и качества состава мер по реализации требований к процессам обеспечения защиты информации при управлении риском информационных угроз при аутсорсинге и использовании сторонних информационных сервисов</p>
Необходимые знания	<p>Требования законодательства Российской Федерации, нормативно-правовых актов Российской Федерации, нормативных актов Банка России в области обеспечения защиты информации, распространяющиеся на деятельность организаций кредитно-финансовой сферы в части организации контрольных мероприятий</p> <p>Требования национальных и международных документов в области стандартизации обеспечения защиты информации организаций кредитно-финансовой сферы, регламентирующих проведение контрольных мероприятий в области защиты информации</p> <p>Основные организационные меры защиты информации для управления риском реализации информационных угроз при аутсорсинге и использовании сторонних информационных сервисов в организациях кредитно-финансовой сферы</p> <p>Основные технические меры защиты информации для управления риском реализации информационных угроз при аутсорсинге и использовании сторонних информационных сервисов в организациях кредитно-финансовой сферы</p> <p>Принципы контроля защиты информации для управления риском реализации информационных угроз при аутсорсинге и использовании сторонних информационных сервисов в организациях кредитно-финансовой сферы</p> <p>Состав, назначение и основные цели проведения мероприятий по контролю защиты информации для управления риском реализации информационных угроз при аутсорсинге и использовании сторонних информационных сервисов в организациях кредитно-финансовой сферы</p> <p>Методология проведения оперативного и периодического контроля защиты информации для управления риском реализации информационных угроз при аутсорсинге и использовании сторонних информационных сервисов в организациях кредитно-финансовой сферы</p>

Другие характеристики	
-----------------------	--

3.5.5. Трудовая функция

Наименование	Организация внешнего аудита информационной безопасности в организациях кредитно-финансовой сферы		Код	E/05.6	Уровень (подуровень) квалификации	6
Происхождение трудовой функции	Оригинал	X	Заимствовано из оригинала			
				Код оригинала	Регистрационный номер профессионального стандарта	
Трудовые действия	Организация деятельности по проведению внешнего аудита информационной безопасности в организации кредитно-финансовой сферы					
	Организация выбора проверяющих организаций, осуществляющих внешний аудит информационной безопасности в организации кредитно-финансовой сферы					
	Участие в определении правил и последовательности мероприятий при проведении внешнего аудита информационной безопасности в организации кредитно-финансовой сферы					
	Участие в определении перечня неоцениваемых областей оценки соответствия при проведении внешнего аудита информационной безопасности в организации кредитно-финансовой сферы					
	Подготовка предложений по выбору источников свидетельств при проведении оценки соответствия обеспечения информационной безопасности в организации кредитно-финансовой сферы					
	Участие в анализе параметров конфигураций, фактических настроек и электронных журналов регистрации технических объектов информатизации и средств защиты информации организации кредитно-финансовой сферы, в том числе с использованием технических и программных средств					
	Участие в анализе уязвимостей и проведения тестирования на проникновение объектов информационной инфраструктуры организации кредитно-финансовой сферы					
	Участие в проведении оценки соответствия обеспечения информационной безопасности в организации кредитно-финансовой сферы					
	Участие в определении и расчете оценок соответствия процессов (подпроцессов) системы информационной безопасности и итоговой оценки соответствия обеспечения информационной безопасности в организации кредитно-финансовой сферы					
	Участие в подготовке рекомендаций по совершенствованию системы информационной безопасности организации кредитно-финансовой сферы и устранению выявленных нарушений					

	Участие в оформлении и представлении результатов внешнего аудита информационной безопасности в организации кредитно-финансовой сферы
Необходимые умения	Принимать участие в разработке проектов документов, регламентирующих взаимодействие с внешними организациями
	Использовать нормативные правовые акты, методические документы, международные и национальные стандарты в области обеспечения информационной безопасности и оценки соответствия
	Принимать необходимое участие в мероприятиях по организации, планированию, проведению и сопровождению внешнего аудита информационной безопасности в организации кредитно-финансовой сферы
	Принимать участие в формировании требований к работам организаций и специалистов, осуществляющих внешний аудит информационной безопасности на этапах заключения договоров
	Принимать участие в сопровождении работ специалистов, осуществляющих внешний аудит информационной безопасности, в том числе на объектах информационной инфраструктуры и в подразделениях организации кредитно-финансовой сферы
	Принимать участие в подготовке и предоставлении необходимых сведений при формировании свидетельств оценки соответствия информационной безопасности организации кредитно-финансовой сферы
	Применять технические и программные средства в области оценки соответствия информационной безопасности организации кредитно-финансовой сферы
	Принимать участие в формировании отчетных материалов результатов проведения работ по внешнему аудиту информационной безопасности в организации кредитно-финансовой сферы
	Принимать участие в надзорных мероприятиях (инспекционных проверках), проводимых ФинЦЕРТ Банка России
Необходимые знания	Требования законодательства Российской Федерации, нормативно-правовых актов Российской Федерации, устанавливающие организационно-правовые основания (режим) деятельности организаций кредитно-финансовой сферы в рамках проведения внешнего аудита информационной безопасности
	Состав, назначение и основные положения документов Банка России, регламентирующие вопросы проведения внешнего аудита информационной безопасности в организации кредитно-финансовой сферы
	Состав, назначение и основные положения международных и национальных стандартов, регламентирующие вопросы проведения внешнего аудита информационной безопасности в организации кредитно-финансовой сферы
	Состав, принципы, условия проведения внешнего аудита информационной безопасности в организациях кредитно-финансовой сферы
	Цели, правила организации и проведения внешнего аудита информационной безопасности в организациях кредитно-финансовой сферы

	Назначение и основные мероприятия проведения внешнего аудита информационной безопасности в организациях кредитно-финансовой сферы
	Состав, назначение и основные положения нормативно-правовых актов Российской Федерации, нормативных актов Банка России, регулирующих контроль обеспечения информационной безопасности в организациях кредитно-финансовой сферы со стороны уполномоченных надзорных органов и Банка России
	Правила и правовые основания проведения контроля и осуществления взаимодействия организации кредитно-финансовой сферы с надзорными подразделениями Банка России
	Цели и правила организации взаимодействия с ФинЦЕРТ Банка России в рамках проведения внешнего аудита информационной безопасности организации кредитно-финансовой сферы
Другие характеристики	

IV. Сведения об организациях – разработчиках профессионального стандарта

4.1. Ответственная организация-разработчик

4.2. Наименования организаций-разработчиков

¹"ОК 010-2014 (МСКЗ-08). Общероссийский классификатор занятий" (принят и введен в действие Приказом Росстандарта от 12.12.2014 N 2020-ст)

² Общероссийский классификатор видов экономической деятельности

³ "ОК 009-2016. Общероссийский классификатор специальностей по образованию"
(принят и введен в действие Приказом Росстандарта от 08.12.2016 N 2007-ст)