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

ПРОФЕССИОНАЛЬНЫЙ СТАНДАРТ

Специалист по информационной безопасности в кредитно-финансовой сфере

Регистрационный номер

I. Общие сведения

Организация информационной безопасности в КФС (кредитных и некредитных финансовых организациях)

(наименование вида профессиональной деятельности) Код

Основная цель вида профессиональной деятельности:

Организация и обеспечение системы информационной безопасности в КФС; реализация процессов информационной безопасности при осуществлении банковских и финансовых операций; проведение контроля состояния информационной безопасности в информационной инфраструктуре организаций КФС; управление риском реализации информационных угроз

Группа занятий:

1223	Руководители подразделений по научным исследованиям и разработкам	2413	Финансовые аналитики
1330	Руководители служб и подразделений в сфере информационно-коммуникационных технологий	1346	Руководители служб и подразделений в сфере финансовой деятельности и страхования
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	2521	Дизайнеры баз данных и администраторы

	(ИКТ)		
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 прочее
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 ОКВЭД[2])	(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
A	Методологическое обеспечение информационной безопасности в организациях КФС	7	Методологическое обеспечение защиты информации организаций КФС	A/01.7	7
			Методологическое обеспечение защиты информации для операционной надежности организаций КФС	A/02.7	7
			Методологическое обеспечение управления инцидентами защиты информации и повышения ситуационной осведомленности в организациях КФС	A/03.7	7
			Методологическое обеспечение управления риском реализации информационных угроз при аутсорсинге и использовании сторонних информационных сервисов в организациях КФС	A/04.7	7
B	Реализация процессов информационной безопасности в информационной инфраструктуре организаций КФС	7	Реализация процессов защиты информации в информационной инфраструктуре организаций КФС	B/01.7	7
			Реализация процессов обеспечения защиты информации для операционной надежности организаций КФС	B/02.7	7
			Реализация процессов управления риском реализации информационных угроз при аутсорсинге и использовании сторонних информационных сервисов в организациях КФС	B/03.7	7
C	Технологическое обеспечение информационной безопасности в организациях КФС	7	Разработка состава технологических мер защиты информации при реализации основных бизнес- и технологических процессов организаций КФС	C/01.7	7
			Реализация технологических мер защиты информации при реализации основных бизнес- и технологических процессов организаций КФС	C/02.7	7

			Контроль применения технологических мер защиты информации при реализации основных бизнес- и технологических процессов организаций КФС	C/03.7	7
D	Управление инцидентами защиты информации в организациях КФС	7	Организация процессов управления инцидентами защиты информации в организациях КФС	D/01.7	7
			Организация мониторинга информационной безопасности в организациях КФС	D/02.7	7
			Организация взаимодействия организаций КФС с ФинЦЕРТ Банка России	D/03.7	7
			Организация взаимодействия организаций КФС с правоохранительными органами	D/04.7	7
			Подготовка отчетности по информационной безопасности организаций КФС	D/05.7	7
E	Контроль информационной безопасности в организациях КФС	7	Проведение внутреннего контроля защиты информации организаций в организациях КФС	E/01.7	7
			Проведение внутреннего контроля защиты информации для операционной надежности организаций КФС	E/02.7	7
			Проведение внутреннего контроля управления риском реализации информационных угроз при аутсорсинге и использовании сторонних информационных сервисов в организациях КФС	E/03.7	7
			Организация внешнего аудита информационной безопасности в организациях КФС	E/04.7	7
F	Управление риском реализации информационных угроз	7	Планирование системы управления риском реализации информационных угроз	F/01.7	7
		7	Реализация системы управления риском реализации информационных угроз	F/02.7	7
		7	Контроль системы управления риском реализации информационных угроз	F/03.7	7
		7	Совершенствование системы управления риском реализации информационных угроз	F/04.7	7

III. Характеристика обобщенных трудовых функций

3.1. Обобщенная трудовая функция

Наименование	Методологическое обеспечение информационной безопасности в организациях КФС	Код	A	Уровень квалификации	7

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 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))

3.1.2. Трудовая функция

Наименование	Методологическое обеспечение защиты информации организаций КФС	Код	A/01.7	Уровень (подуровень) квалификации	7

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

Трудовые действия	Разработка и согласование корпортивной политики по защите информации организации КФС
	Определение области применения процессов системы защиты информации для уровней информационной инфраструктуры организации КФС
	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 КФС
	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
	Определение состава ролей и права субъектов доступа, необходимых для обеспечения применения, эксплуатации, контроля эксплуатации и использования по назначению технических средств защиты информации
	Разработка и согласование планов по реализации организационных и технических мер защиты информации в организации КФС
Необходимые умения	Работать с действующей нормативно - правовой и методологической базой в области обеспечения защиты информации организаций КФС
	Анализировать и применять в организации КФС требования законодательства Российской Федерации и нормативных актов Банка России по вопросам защиты информации
	Анализировать и применять в организации КФС требования национальных и международных стандартов по защите информации
	Определять организационные меры защиты информации в рамках процессов защиты информации
	Определять технические меры защиты информации в рамках процессов защиты информации
	Разрабатывать проекты внутренних документов организации КФС, устанавливающих цели и принципы обеспечения защиты информации, определяющих методологию, правила организации и реализации процессов обеспечения защиты информации
	Разрабатывать проекты внутренних документов организации КФС, регламентирующих процессы обеспечения защиты информации
	Разрабатывать проекты внутренних документов организации КФС, регламентирующих взаимодействие с внешними организациями
	Разрабатывать проекты внутренних документов организации КФС по вопросам применения, эксплуатации, контроля эксплуатации и использования по назначению технических средств защиты информации
	Планировать работу по реализации организационных и технических мер защиты информации в организации КФС
Необходимые знания	Законодательство Российской Федерации по вопросам защиты информации в организациях КФС
	Нормативные акты Банка России по вопросам защиты информации в организациях КФС
	Основные национальные и международные документы в области стандартизации обеспечения защиты информации в организациях КФС
	Документы Банка России в области стандартизации обеспечения защиты информации в организациях КФС
	Основные цели обеспечения защиты информации в рамках бизнес-- и технологических процессов организаций КФС
	Виды защищаемой информации в рамках бизнес-- и технологических

	процессов организаций КФС
	Основы проектного и процессного управления в организациях КФС
	Состав, принципы, условия реализации процессов обеспечения защиты информации в организациях КФС
Другие характеристики	

3.1.3. Трудовая функция

Наименование	Методологическое обеспечение защиты информации для операционной надежности организаций КФС	Код	A/02.7	Уровень (подуровень) квалификации	7

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

Трудовые действия	Разработка и согласование корпортивной политики по обеспечению операционной надежности организации КФС
	Определение и установление ключевых индикаторов риска, связанных с обеспечением операционной надежности организации КФС
	Организация процессов и участие в идентификации области применения системы обеспечения для операционной надежности организации КФС на уровне персонала
	Организация процессов и участие в идентификации области применения системы обеспечения операционной надежности организации КФС при осуществлении видов деятельности по предоставлению финансовых и (или) информационных услуг
	Организация процессов и участие в идентификации области применения системы обеспечения операционной надежности организации КФС на прикладном уровне объектов информатизации
	Организация процессов и участие в идентификации области применения системы обеспечения операционной надежности организации КФС на уровне данных, хранимых, обрабатываемых и (или) передаваемых в рамках реализации бизнес- и технологических процессов
	Организация процессов и участие в идентификации области применения системы обеспечения операционной надежности организации КФС на инфраструктурном уровне объектов информатизации
	Организация процессов и участие в идентификации области применения системы обеспечения операционной надежности организации КФС на физическом уровне (уровне помещений организации КФС)
	Планирование применения мер, направленных на обеспечение операционной надежности организации КФС
	Определение состава и содержания мер, направленных на обеспечение операционной надежности организации КФС
	Определение порядка применения мер, направленных на обеспечение операционной надежности организации КФС
	Разработка и согласование планов по реализации мер, направленных на

	обеспечение операционной надежности организации КФС
Необходимые умения	Работать с действующей нормативно - правовой и методологической базой в области обеспечения операционной надежности организации КФС
	Анализировать и применять в организации КФС требования законодательства Российской Федерации и нормативных актов Банка России по вопросам обеспечения операционной надежности организации КФС
	Анализировать и применять в организации КФС требования национальных и международных стандартов по обеспечению операционной надежности организации КФС
	Определять организационные меры по обеспечению операционной надежности организации КФС
	Определять технические меры по обеспечению операционной надежности организации КФС
	Разрабатывать проекты внутренних документов организации КФС, устанавливающих цели и принципы обеспечения операционной надежности организации КФС
	Разрабатывать проекты внутренних документов организации КФС, определяющих методологию, правила организации и реализации обеспечения операционной надежности организации КФС
	Планировать работу по обеспечению операционной надежности организации КФС
Необходимые знания	Законодательство Российской Федерации по вопросам обеспечения защиты информации для операционной надежности бизнес- и технологических процессов организаций КФС
	Нормативные акты Банка России по вопросам обеспечения защиты информации для операционной надежности бизнес- и технологических процессов организаций КФС
	Состав и основное назначение ключевыхОсновные национальных национальные и международных международные документов документы в области стандартизации обеспечения защиты информации для операционной надежности бизнес- и технологических процессов организаций КФС
	Состав, назначение и основные положения Документовы Банка России в области защиты информации для стандартизации обеспечения операционной надежности бизнес- и технологических процессов организациий КФС
	Основные цели обеспечения защиты информации для обеспечения операционной надежности бизнес- и технологических процессов организации КФС
	Принципы обеспечения операционной надежности организаций КФС, обеспечения защиты информации для выполнения бизнес- и технологических процессов организации КФС
Другие характеристики	

3.1.4. Трудовая функция

Наименование	Методологическое обеспечение	Код	A/03.7	Уровень	7

управления инцидентами защиты информации и повышения ситуационной осведомленности в организациях КФС		(подуровень) квалификации	

Происхождение трудовой функции	Оригинал X	Заимствовано 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 КФС
	Определение и установление ключевых индикаторов риска, связанных с управлением инцидентами защиты информации и обеспечением ситуационной осведомленности организации КФС
	Определение структуры органов управления финансовой организации и подразделений, осуществляющих функции, связанные с управлением инцидентами защиты информации и обеспечением ситуационной осведомленности организации КФС
	Организация и участие в идентификации источников формирующие данные о инцидентах защиты информации (событиях защиты информации) организации КФС
	Организация и участие в идентификации технических данных, потенциально обладающих содержательной (семантической) информацией организации КФС
	Организация и участие в разработке системы хранения информации о событиях защиты информации и инцидентах защиты информации организации КФС
Необходимые умения	Работать с действующей нормативно - правовой и методологической базой в области управления инцидентами защиты информации и обеспечения ситуационной осведомленности организации КФС
	Анализировать и применять в организации КФС требования законодательства Российской Федерации и нормативных актов Банка России по вопросам управления инцидентами защиты информации и обеспечения ситуационной осведомленности организации КФС
	Анализировать и применять в организации КФС требования национальных и международных стандартов по вопросам управления инцидентами защиты информации и обеспечения ситуационной осведомленности организации КФС
	Определять организационные меры по обеспечению управления инцидентами защиты информации и обеспечения ситуационной осведомленности организации КФС
	Определять технические меры по обеспечению защиты информации для управления инцидентами защиты информации и обеспечения ситуационной осведомленности организации КФС
	Разрабатывать проекты внутренних документов организации КФС, устанавливающих цели и принципы управления инцидентами защиты информации и обеспечения ситуационной осведомленности организации

	КФС
	Разрабатывать проекты внутренних документов организации КФС, определяющих методологию, правила организации и реализации управления инцидентами защиты информации и обеспечения ситуационной осведомленности организации КФС
	Планировать работу по управлению инцидентами защиты информации и обеспечения ситуационной осведомленности организации КФС
Необходимые знания	Законодательство Российской Федерации по вопросам управления инцидентами защиты информации и обеспечения ситуационной осведомленности организации КФС
	Нормативные акты Банка России по вопросам управления инцидентами защиты информации и обеспечения ситуационной осведомленности организации КФС
	Основные национальные и международные документы в области стандартизации управления инцидентами защиты информации и обеспечения ситуационной осведомленности организации КФС
	Документы Банка России в области стандартизации управления инцидентами защиты информации и обеспечения ситуационной осведомленности организации КФС
	Основные цели управления инцидентами защиты информации и обеспечения ситуационной осведомленности организации КФС
	Принципы управления инцидентами защиты информации и обеспечения ситуационной осведомленности организации КФС
Другие характеристики	

3.1.5. Трудовая функция

Наименование	Методологическое обеспечение управления риском реализации информационных угроз при аутсорсинге и использовании сторонних информационных сервисов в организациях КФС	Код	A/04.7	Уровень (подуровень) квалификации	7

Происхождение трудовой функции	Оригинал X	Заимствовано 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 КФС
	Определение и установление ключевых индикаторов риска, связанных с управлением риском реализации информационных угроз при аутсорсинге и использовании сторонних информационных сервисов организации КФС
	Определение структуры органов управления организации КФС 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 КФС, переданных на аутсорсинг или выполняемых с использованием сторонних информационных сервисов, ненадлежащее выполнение которых поставщиком услуг создает условия для реализации или реализует риск информационных угроз
	Организация и участие в идентификации защищаемой информации применяемой в бизнес-- и (или) технологических процессах организации КФС, 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
	Организация и участие в оценке риска реализации информационных угроз при аутсорсинге и использовании сторонних информационных сервисов в организации КФС, а также согласование результатов оценки
	Определение ролей, связанных с выявлением и идентификацией риска реализации информационных угроз при аутсорсинге и использовании сторонних информационных сервисов организацией КФС
Необходимые умения	Работать с действующей нормативно - правовой и методологической базой в области управления риском реализации информационных угроз при аутсорсинге и использовании сторонних информационных сервисов организации КФС
	Анализировать и применять в организации КФС требования законодательства Российской Федерации и нормативных актов Банка России по вопросам управления риском реализации информационных угроз при аутсорсинге и использовании сторонних информационных сервисов организации КФС
	Анализировать и применять в организации КФС требования национальных и международных стандартов по вопросам управления риском реализации информационных угроз при аутсорсинге и использовании сторонних информационных сервисов организации КФС
	Определять организационные меры по обеспечению защиты информации для управления риском реализации информационных угроз при аутсорсинге и использовании сторонних информационных сервисов организации КФС
	Определять технические меры по обеспечению защиты информации для управления риском реализации информационных угроз при аутсорсинге и использовании сторонних информационных сервисов организации КФС
	Разрабатывать проекты внутренних документов организации КФС, устанавливающих цели и принципы управления риском реализации информационных угроз при аутсорсинге и использовании сторонних информационных сервисов организации КФС
	Разрабатывать проекты внутренних документов организации КФС, определяющих методологию, правила организации и реализации управления риском реализации информационных угроз при аутсорсинге

	и использовании сторонних информационных сервисов организации КФС
	Планировать работу по обеспечению защиты информации для управления риском реализации информационных угроз при аутсорсинге и использовании сторонних информационных сервисов организации КФС
Необходимые знания	Законодательство Российской Федерации по вопросам управления риском реализации информационных угроз при аутсорсинге и использовании сторонних информационных сервисов организации КФС
	Нормативные акты Банка России по вопросам управления риском реализации информационных угроз при аутсорсинге и использовании сторонних информационных сервисов организации КФС
	Основные национальные и международные документы в области стандартизации управления риском реализации информационных угроз при аутсорсинге и использовании сторонних информационных сервисов организации КФС
	Состав, назначение и основные положения документов Банка России в области стандартизации управления риском реализации информационных угроз при аутсорсинге и использовании сторонних информационных сервисов организации КФС
	Основные цели управления риском реализации информационных угроз при аутсорсинге и использовании сторонних информационных сервисов организации КФС
	Принципы управления риском реализации информационных угроз при аутсорсинге и использовании сторонних информационных сервисов организации КФС
Другие характеристики	

3.2. Обобщенная трудовая функция

Наименование	Реализация процессов информационной безопасности в информационной инфраструктуре организаций КФС	Код	B	Уровень квалификации	7

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	Образовательные программы высшего образования – программы специалитета, магистратуры

обучению	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))

3.2.2. Трудовая функция

Наименование	Реализация процессов защиты информации в информационной инфраструктуре организаций КФС	Код	B/01.7	Уровень (подуровень) квалификации	7

Происхождение трудовой функции	Оригинал X	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 КФС, 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 КФС
	Тестирование полноты реализации технических мер защиты информации
	Назначение работникам организации КФС 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 КФС
	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 КФС необходимой для функционирования технических мер и средств защиты информации
	Принятие регламентированных мер по восстановлению отказавших технических средств защиты информации информационной инфраструктуры организации КФС
	Сопровождение технических мер и средств защиты информации в течении всего срока их использования
	Обучение, практическая подготовка (переподготовка) работников организации КФС, ответственных за применение мер и средств защиты информации в рамках процесса защиты информации
	Повышение осведомленности (инструктаж) работников организации КФС в области реализации процесса защиты информации, применения организационных мер защиты информации, использования по назначению технических мер и средств защиты информации
	Организация защиты информации на этапах жизненного цикла автоматизированных систем и приложений
Необходимые умения	Осуществлять концептуальное, архитектурное, функциональное и техническое проектирование процессов защиты информации в информационной инфраструктуре организаций КФС, а также оформлять соответствующие проектные документы

	Организовывать реализацию проектов по вопросам защиты информации в организации кредитно-финансовой сферы
	Организовывать внедрение и применение политик (правил, процедур) по обеспечению защиты информации в организации КФС
	Принимать участие в концептуальном, архитектурном и техническом проектировании реализации процессов защиты информации в информационной инфраструктуре организаций КФС
	Разрабатывать функционально-технические требования к техническим средствам защиты информации и системам обеспечения защиты информации в организациях КФС
	Принимать участие в выборе техничеких средств защиты информации и систем обеспечения защиты информации для применения в рамках бизнес-- и технологических процессов организации КФС
	Организовывать внедрение технических средств защиты информации на объектах информатизации и систем защиты информации в информационной структуре организаций КФС
	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 КФС
	Обеспечивать защиту информации при выводе из эксплуатации компонентов информационной инфраструктуры, носителей данных
Необходимые знания	Виды защищаемой информации в рамках бизнес-- и технологических процессов организации КФС
	Цели обеспечения защиты информации в рамках бизнес-- и технологических процессов организаций КФС
	Состав, принципы, условия реализации процессов обеспечения защиты информации в организациии КФС
	Состав и функциональные возможности технических средств защиты информации и систем обеспечения защиты информации, предназначенных для применения в рамках процессов защиты информации организаций КФС
	Основные организационные и технические меры защиты информации
	Основы построения и принципы функционирования автоматизированных систем, реализация бизнес-- и технологических процессов организаций КФС, 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 КФС
	Уязвимости и связанные с ними риски нарушения защиты информации, присущие используемых организациями КФС, процессов проектирования, приобретения, эксплуатации и сопровождения эксплуатации автоматизированных систем, реализующих бизнес-- и технологические процессы организаций КФС, в том числе автоматизированных банковских систем
	Объекты информационной инфраструктуры организаций КФС, включая автоматизированные системы и их компоненты, задействованные в реализации бизнес-- и технологических процессов организаций КФС (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 КФС (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 КФС в сети Интранет и Интернет)
	Функционально-технические требования к техническим средствам защиты информации и системам обеспечения защиты информации в организациях КФС
	Условия по ограничениям, связанным с применением технических средств защиты информации и систем обеспечения защиты информации в рамках бизнес-- и технологических процессов организаций КФС
	Требования к применению техническим средствам защиты информации, сертифицированным по требованиям безопасности информации
Другие характеристики	

3.2.3. Трудовая функция

Наименование	Реализация процессов операционной надежности организаций КФС	Код	B/02.7	Уровень (подуровень) квалификации	7

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 КФС
	Организация и сопровождение процессов реализации мер на уровне бизнес-- и технологических процессов, реализуемых организацией КФС при осуществлении видов деятельности по предоставлению финансовых и (или) информационных услуг
	Организация и сопровождение процессов реализации мер на прикладном уровне объектов информатизации, используемых организацией КФС
	Организация и сопровождение процессов реализации мер на уровне данных, хранимых, обрабатываемых и (или) передаваемых в рамках реализации бизнес-- и технологических процессов организации КФС
	Организация и сопровождение процессов реализации мер на инфраструктурном уровне объектов информатизации, используемых организацией КФС
	Организация и сопровождение процессов реализации мер на физическом уровне (уровне помещений организации КФС)

	Участие в разработке и применении плана обеспечения операционной надежности организаций КФС
	Разработка и применение плана восстановления обеспечения операционной надежности организации КФС при реализации инцидентов защиты информации
Необходимые умения	Разрабатывать предложения в план обеспечения операционной надежности организаций КФС
	Разрабатывать план восстановления обеспечения операционной надежности организаций КФС при реализации инцидентов защиты информации
	Настраивать резервное копирование системных параметров, программного обеспечения и файлов, в том числе в соответствии с заданным расписанием
	Восстанавливать системные параметры, программное обеспечение и файлы из резервных копий
	Разрабатывать организационные и технические меры по реализации процессов обеспечения операционной надежности организаций КФС
Необходимые знания	Принципы управления вычислительными мощностями и пропускной способностью каналов связи организации КФС
	Архитектура построения отказоустойчивых центров обработки и (или) хранения данных
	Технологии резервирования и восстановления данных
	Инфраструктурные уровни объектов информатизации, используемые организацией КФС
Другие характеристики	

3.2.4. Трудовая функция

Наименование	Реализация процессов управления риском реализации информационных угроз при аутсорсинге и использовании сторонних информационных сервисов в организациях КФС	Код	B/03.7	Уровень (подуровень) квалификации	7

Происхождение трудовой функции	Оригинал X	Заимствовано 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 КФС

	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 КФС
	Выполнение оценки возможности поставщика услуг выполнить свои обязательства по аутсорсингу бизнес- и (или) технологических процессов организации КФС
	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 КФС на аутсорсинге, в части ресурсного обеспечения
	Организация и участие в оценке поставщика услуг, выполняющего бизнес- и (или) технологические процессы организации КФС на аутсорсинге, в части соблюдения требований к защите информации
	Организация и участие в оценке поставщика услуг, выполняющего бизнес- и (или) технологические процессы организации КФС на аутсорсинге, в части соблюдения требований к обеспечению операционной надежности
Необходимые умения	Разрабывать 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 выполнять свои обязательства по аутсорсингу бизнес- и (или) технологических процессов организации КФС
	Разрабывать предложения по мерам, направленным на снижение риска реализации информационных угроз при аутсорсинге и использовании сторонних информационных сервисов
	Классифицировать риски реализации информационных угроз при аутсорсинге и использовании сторонних информационных сервисов
	Организовывать систему мер, направленных на снижение риска реализации информационных угроз при аутсорсинге и использовании сторонних информационных сервисов
	Организовывать и участвовать в оценке поставщика услуг, выполняющего бизнес- и (или) технологические процессы организации КФС на аутсорсинге, в части ресурсного обеспечения
	Организовывать и участвовать в оценке поставщика услуг, выполняющего бизнес- и (или) технологические процессы организации КФС на аутсорсинге, в части соблюдения требований к защите информации
	Организовывать и участвовать в оценке поставщика услуг, выполняющего бизнес- и (или) технологические процессы организации КФС на аутсорсинге, в части соблюдения требований к обеспечению операционной надежности
Необходимые знания	Законодательство Российской Федерации по вопросам управления

	риском реализации информационных угроз при аутсорсинге и использовании сторонних информационных сервисов в организациях КФС
	Нормативные акты Банка России по вопросам управления риском реализации информационных угроз при аутсорсинге и использовании сторонних информационных сервисов в организациях КФС
	Основные национальные и международные документы в области стандартизации управления риском реализации информационных угроз при аутсорсинге и использовании сторонних информационных сервисов в организациях КФС
	Документы Банка России в области стандартизации управления риском реализации информационных угроз при аутсорсинге и использовании сторонних информационных сервисов в организациях КФС
	Основные цели управления риском реализации информационных угроз при аутсорсинге и использовании сторонних информационных сервисов в организациях КФС
	Основные риски реализации информационных угроз при аутсорсинге и использовании сторонних информационных сервисов в организациях КФС
	Принципы управления риском реализации информационных угроз при аутсорсинге и использовании сторонних информационных сервисов в организациях КФС
Другие характеристики	

3.3. Обобщенная трудовая функция

Наименование	Технологическое обеспечение информационной безопасности в организациях КФС	Код	C	Уровень квалификации	7

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 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	Код	C/01.7	Уровень (подуровень) квалификации	7

технологических процессов организаций КФС			

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

Трудовые действия	Изучение новых технологий, достижений науки и техники в области обеспечения информационной безопасности, аналитических материалов ведущих компаний в области информационной безопасности
	Разработка технологических мер защиты информации в рамках реализации бизнес- и технологических процессов организации КФС
	Разработка технологических мер защиты информации применительно к объектам информационной инфраструктуры организации КФС
	Разработка технологических мер защиты информации организации КФС при осуществлении переводов денежных средств
	Разработка технологических мер защиты информации организации КФС при осуществлении операций с платежными картами
	Разработка технологических мер защиты информации организации КФС при передаче финансовых сообщений формата СВИФТ (SWIFT)
Необходимые умения	Применять при разработке состава технологических мер защиты информации знания в области осуществления банковской и финансовой деятельности деятельности, знания в реализации бизнес-- и технологических процессов организаций КФС
	Применять при разработке состава технологических мер защиты информации знания по существующим практикам технологических мер защиты информации при реализации бизнес-- и технологических процессов организаций КФС
	Принимать участие в обеспечении применения технологических мер защиты информации на этапах концептуального, архитектурного и технического проектирования автоматизированных систем организации КФС
	Разрабатывать требования и технологические меры защиты информации в автоматизированных системах организации КФС
	Разрабатывать технологические меры защиты информации с учетом специфики реализации бизнес-- и технологических процессов организации КФС
Необходимые знания	Законодательство Российской Федерации, нормативно-правовые акты Российской Федерации, нормативные акты Банка России в области применения технологических мер защиты информации в процессах, связанных, в том числе, 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
	Состав и содержание технологических мер защиты информации при реализации бизнес-- и технологических процессов организаций КФС
	Примеры и принципы проектирования технологических мер защиты информации для бизнес-- и технологических процессов организации КФС
	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 КФС	Код	C/02.7	Уровень (подуровень) квалификации	7

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 КФС
	Участие в реализации технологических мер защиты информации применительно к объектам информационной инфраструктуры организации КФС
	Участие в реализации технологических мер защиты информации организации КФС при осуществлении переводов денежных средств
	Участие в реализации технологических мер защиты информации организации КФС при осуществлении операций с платежными картами
	Участие в реализации технологических мер защиты информации организации КФС 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 переводов денежных средств
	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 КФС

	Применять при реализации технологических мер защиты информации знания по существующим практикам технологических мер защиты информации при реализации бизнес-- и технологических процессов организаций КФС
	Принимать участие в реализации технологических мер защиты информации в ходе эксплуатации автоматизированных систем организации КФС
	Принимать участие в реализации технологических мер защиты информации с учетом специфики реализации бизнес- и технологических процессов организации КФС
Необходимые знания	Законодательство Российской Федерации, нормативно-правовых актов Российской Федерации, нормативных актов Банка России в области применения технологических мер защиты информации в процессах, связанных, в том числе, 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 КФС
	Основы реализации технологических мер защиты информации в автоматизированных системах организации КФС
	Состав и содержание ролей информационной безопасности в организации КФС в рамках реализации технологических мер защиты информации
Другие характеристики	Понимать финансовые продукты и технологии

3.3.3. Трудовая функция

Наименование	Контроль применения технологических мер защиты информации при реализации основных бизнес- и технологических процессов организаций КФС	Код	С/03.7	Уровень (подуровень) квалификации	7

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 КФС

	Участие в контроле применения технологических мер защиты информации применительно к объектам информационной инфраструктуры организации КФС
	Участие в контроле применения технологических мер защиты информации организации КФС при осуществлении переводов денежных средств
	Участие в контроле применения технологических мер защиты информации организации КФС при осуществлении операций с платежными картами
	Участие в контроле применения технологических мер защиты информации организации КФС при передаче финансовых сообщений формата СВИФТ (SWIFT)
	Участие в контроле применения технологических мер защиты информации в автоматизированных системах организаций КФС
Необходимые умения	Применять при контроле технологических мер защиты информации знания в области осуществления банковской и финансовой деятельности деятельности, знания в реализации бизнес- и технологических процессов организаций КФС
	Применять при контроле технологических мер защиты информации знания по существующим практикам технологических мер защиты информации при реализации бизнес- и технологических процессов организаций КФС
	Принимать участие в контроле технологических мер защиты информации при реализации бизнес- и технологических процессов организации КФС
	Принимать участие в контроле технологических мер защиты информации в ходе эксплуатации автоматизированных систем организации КФС
Необходимые знания	Законодательство Российской Федерации, нормативно-правовые акты Российской Федерации, нормативные акты Банка России в области применения технологических мер защиты информации в процессах, связанных, в том числе, 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 контроля технологических мер защиты информации при реализации бизнес- и технологических процессов организаций КФС
	Состав и содержание ролей информационной безопасности в организации КФС в рамках реализации технологических мер защиты информации
	Принципы и правила контроля реализации технологических мер защиты информации в автоматизированных системах и информационной инфраструктуре организации КФС на соответствие проектной и эксплуатационной документации
Другие характеристики	

3.4. Обобщенная трудовая функция

Наименование	Управление инцидентами защиты информации в организациях КФС	Код	D	Уровень квалификации	7

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 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 КФС	Код	D/01.7	Уровень (подуровень) квалификации	7

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

Трудовые действия	Участие в разработке плана управления инцидентами защиты информации и обеспечения ситуационной осведомленности организации КФС
	Классификации инцидентов защиты информации организации КФС
	Определение и организация стадий обработки инцидентов защиты информации организации КФС
	Определение организационной структуры группы реагирования на инциденты защиты информации организации КФС
	Определение технического обеспечения организации КФС для осуществления деятельности по управлению инцидентами защиты информации
	Выявление и реагирование на инциденты защиты информации организации КФС
	Своевременная обработка инцидентов защиты информации организации КФС
	Регламентация и выполнение деятельности по расследованию и анализу инцидентов защиты информации организации КФС
	Организация процесса сбора технических данных в случае реализации инцидентов защиты информации организации КФС

	Планирование и регламентацию процесса сбора технических данных, в случае реализации инцидентов защиты информации организации КФС
	Определение общего состава действий при сборе технических данных в случае реализации инцидентов защиты информации организации КФС
Необходимые умения	Участвовать в организации и планировании деятельности служб информационной безопасности организации КФС применительно к процессам мониторинга и управления инцидентами защиты информации
	Участвовать в концептуальном, архитектурном и техническом проектировании реализации процессов мониторинга и управления инцидентами защиты информации в информационной инфраструктуре организаций КФС
	Разрабатывать функционально-технические требования к системам сбора данных для сбора технических данных в случае реализации инцидентов защиты информации организации КФС
	Принимать участие в выборе технических средств защиты информации для применения в рамках управления инцидентами защиты информации организации КФС
	Применять и работать с техническими средствами защиты информации и системами, реализующими функции управления инцидентами защиты информации организации КФС
	Формировать требования к объектам сбора технических данных процессов управления инцидентами защиты информации для объектов информационной инфраструктуры организаций КФС 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 КФС
	Принимать участие в мероприятиях по реализации процессов управления инцидентами защиты информации, сборе и обработке сведений и технических данных об инцидентах защиты информации организации КФС
	Выявлять и реагировать на инциденты защиты информации организации КФС
	Обрабатывать инциденты защиты информации организации КФС
	Участвовать в расследовании и анализе инцидентов защиты информации организации КФС
	Организовывать и осуществлять сбор технических данных в случае реализации инцидентов защиты информации организации КФС
Необходимые знания	Законодательство Российской Федерации по вопросам управления инцидентами защиты информации и обеспечения ситуационной осведомленности организации КФС
	Нормативные акты Банка России по вопросам управления инцидентами защиты информации и обеспечения ситуационной осведомленности организации КФС
	Основные национальные и международные документы в области стандартизации управления инцидентами защиты информации и обеспечения ситуационной осведомленности организации КФС
	Документы Банка России в области стандартизации управления инцидентами защиты информации и обеспечения ситуационной осведомленности организации КФС

	Источники возникновения, классификация и технические характеристики инцидентов защиты информации объектов информационной инфраструктуры организаций КФС
	Состав уязвимостей и угроз информационной безопасности в целях сбора данных о событиях защиты информации организации КФС
	Состав, принципы, условия реализации процессов мониторинга и управления инцидентами защиты информации в организации КФС
	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 КФС
	Порядок обработки инцидентов защиты информации и обеспечения ситуационной осведомленности организации КФС
	Виды и типы инцидентов защиты информации организации КФС
	Порядок проведения расследования инцидентов защиты информации организации КФС
	Порядок сбора технических данных в случае реализации инцидентов защиты информации организации КФС
Другие характеристики	

3.4.2. Трудовая функция

Наименование	Организация мониторинга информационной безопасности в организациях КФС	Код	D/02.7	Уровень (подуровень) квалификации	7

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 КФС
	Контроль за фактическими значениями ключевых индикаторов риска, связанных с управлением инцидентами защиты информации и обеспечения ситуационной осведомленности организации КФС
	Контроль процедуры сбора и регистрации информации о реализации инцидентов защиты информации организации КФС
	Определение ролей, связанных с мониторингом системы управления инцидентами защиты информации и обеспечения ситуационной осведомленности организации КФС
	Определение и согласование процедуры стрестестирования системы управления инцидентами защиты информации и обеспечения ситуационной осведомленности организации КФС
	Организация стресс-тестирования, разработка плана управления инцидентами защиты информации и обеспечения ситуационной осведомленности организации КФС
	Определение ролей, связанных с выполнением деятельности по стресс-

	тестированию плана управления инцидентами защиты информации и обеспечения ситуационной осведомленности организации КФС
Необходимые умения	Применять и работать с техническими средствами защиты информации и системами, реализующими функции оперативного мониторинга, обнаружения вторжений и сетевых атак, направленных на организации КФС
	Работать с конфигурациями средств сбора технических данных мониторинга и настройки подсистем обработки этих данных для выявления событий и инцидентов защиты информации организации КФС
	Осуществлять контроль процедуры сбора и регистрации информации о реализации инцидентов защиты информации
	Осуществлять контроль за фактическими значениями ключевых индикаторов риска, связанных с управлением инцидентами защиты информации и обеспечения ситуационной осведомленности организации КФС
	Участвовать в проведении мероприятий по стресс-тестированию системы управления инцидентами защиты информации и обеспечения ситуационной осведомленности организации КФС
	Принимать участие в проведении оценки эффективности реализуемых процессов мониторинга и управления инцидентами защиты информации и формировании предложений по развитию и совершенствованию указанных процессов организации КФС
Необходимые знания	Законодательство Российской Федерации по вопросам мониторинга защиты информации в организациях КФС
	Нормативные акты Банка России по вопросам мониторинга защиты информации в организациях КФС
	Основные национальные и международные документы в области стандартизации мониторинга защиты информации в организациях КФС
	Документы Банка России в области стандартизации мониторинга защиты информации в организациях КФС
	Источники возникновения, классификация и технические характеристики инцидентов защиты информации объектов информационной инфраструктуры организаций КФС
	Состав уязвимостей и угроз информационной безопасности в целях сбора данных о событиях защиты информации организации КФС
	Состав, принципы, условия реализации процессов мониторинга и управления инцидентами защиты информации в организации КФС
	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 КФС
	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 КФС
Другие характеристики	

3.4.3. Трудовая функция

Наименование	Организация взаимодействия организаций КФС с ФинЦЕРТ Банка России	Код	D/03.7	Уровень (подуровень) квалификации	7

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 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
	Принимать участие в организации и осуществлению информационного обмена с ФинЦЕРТ Банка России об инцидентах, связанных с нарушением требований к обеспечению защиты информации организации КФС
	Принимать участие в мероприятиях организации КФС по взаимодействию с ФинЦЕРТ Банка России при реагировании на инциденты, связанные с нарушением требований к обеспечению защиты информации
Необходимые умения	Работать с техническими средствами и системами осуществления информационного обмена с ФинЦЕРТ Банка России об инцидентах, связанных с нарушением требований к обеспечению защиты информации организации КФС
	Требования законодательства Российской Федерации по вопросам взаимодействия организаций КФС с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на объекты информционной системы Российской Федерации
	Требования нормативные актов Банка России по вопросам

	взимодействия организаций КФС с ФинЦЕРТ Банка России
Необходимые знания	Основные требования национальных стандартов в области ввзаимодействия организаций КФС с ФинЦЕРТ Банка России
	Основные цели и процедуры организации взаимодействия организации КФС с ФинЦЕРТ Банка России
	Порядок подключения организации организаций КФС к информационному обмену с ФинЦЕРТ Банка России
Другие характеристики	

3.4.4. Трудовая функция

Наименование	Организация взаимодействия организаций КФС с правоохранительными органами	Код	D/04.7	Уровень (подуровень) квалификации	7

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

Трудовые действия	Организация процедуры взаимодействия организации КФС с правоохранительными органами РФ в части выполнения сбора, упаковки, хранения и траспортировки технических данных потенциально обладающих содержательной (семантической) информацией
	Выполнение документирования результатов выделения и анализа содержательной (семантической) информации, предполагаемых к передаче в правоохранительные органы
	Определение и применение способов непосредственного сбора технических данных потенциально обладающих содержательной (семантической) информацией
	Организация выполнения «криминалистического» копирования (создания образов) энергонезависимых технических данных потенциально обладающих содержательной (семантической) информацией
	Организация выполнения копирования содержимого оперативной памяти средств вычислительной техники и получению данных операционных систем
	Организация выполнения копирования протоколов (журналов) регистрации
	Организация выполнения копирования сетевого трафика
	Рекомендации по обеспечению безопасной упаковки, хранения и транспортировки носителей, собранных данных
	Организация применения технических средств сбора и обработки технических данных
Необходимые умения	Документировать результаты выделения и анализа содержательной (семантической) информации, предполагаемых к передаче в правоохранительные органы

	Участвовать в расследовании и анализе инцидентов защиты информации организации КФС
	Организовывать и осуществлять сбор технических данных для передачи в правоохранительные органы в случае реализации инцидентов защиты информации организации КФС
	Организовывать процедуры взаимодействия организации КФС с правоохранительными органами РФ в части выполнения сбора, упаковки, хранения и траспортировки технических данных потенциально обладающих содержательной (семантической) информацией
	Определять и применять способы непосредственного сбора технических данных потенциально обладающих содержательной (семантической) информацией
	Организовывать выполнение «криминалистического» копирования (создания образов) энергонезависимых технических данных потенциально обладающих содержательной (семантической) информацией
	Организовывать выполнение копирования содержимого оперативной памяти средств вычислительной техники и получению данных операционных систем
	Организовывать выполнение копирования протоколов (журналов) регистрации
	Организовывать выполнение копирования сетевого трафика
	Обеспечивать безопасную упаковку, хранение и транспортировку носителей, собранных данных
	Организовывать применение технических средств сбора и обработки технических данных
Необходимые знания	Законодательство Российской Федерации по вопросам взаимодействия организаций КФС с правоохранительными органами
	Нормативные акты Банка России по вопросам взимодействия организаций КФС с правоохранительными органами
	Национальные стандарты в области ввзаимодействия организаций КФС с ФинЦЕРТ Банка России правоохранительными органами
	Стандарты Банка России в области ввзаимодействия организаций КФС с правоохранительными органами
	Основные цели и процедуры организации взаимодействия организций КФС с правохранительными органами
	Основные цели и процедуры организации взаимодействия организаций КФС с правоохранительными органами
	Порядок проведения расследования инцидентов защиты информации организации КФС
	Порядок сбора технических данных в случае реализации инцидентов защиты информации организации КФС
Другие характеристики	Понимать финансовые продукты и технологии

3.4.5. Трудовая функция

Наименование	Подготовка отчетности по информационной безопасности организаций КФС	Код	D/05.7	Уровень (подуровень) квалификации	7

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 КФС
	Подготовка внутренней отчетности организации КФС в рамках деятельности по управлению инцидентами защиты информации
	Подготовка отчетности по информационной безопасности организаций КФС, предоставляемой в Банк России
	Отправка в Банк России отчетности по информационной безопасности организаций КФС
Необходимые умения	Принимать участие в подготовке отчетности по инцидентам защиты информации организации КФС
	Взаимодействовать с структурными подразделениями организации КФС при сборе данных для подготовки отчетности по информационной безопасности
	Заполнять формы отчетности по информационной безопасности организаций КФС
Необходимые знания	Законодательство Российской Федерации по вопросам подготовки отчетности по информационной безопасности организаций КФС
	Нормативные акты Банка России по вопросам подготовки отчетности по информационной безопасности организаций КФС
	Основные международные и национальные стандарты в области подготовки отчетности по информационной безопасности организаций КФС
	Стандарты Банка России в области подготовки отчетности по информационной безопасности организаций КФС
	Основные цели подготовки отчетности по информационной безопасности организаций КФС
	Основные формы отчетности по информационной безопасности организаций КФС
	Порядок подготовки и заполнения форм отчетности по информационной безопасности организаций КФС
	Порядок предоставления отчетности по информационной безопасности организации КФС в Банк России
Другие характеристики	

3.5. Обобщенная трудовая функция

Наименование	Контроль информационной безопасности в организациях КФС	Код	E	Уровень квалификации	7

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 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 КФС	Код	E/01.6	Уровень (подуровень) квалификации	6

Происхождение трудовой функции	Оригинал X	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 КФС
	Контроль за уровнем риска реализации информационных угроз организации КФС
	Организация и участие в анализе и контроле адекватности идентификации области применения системы управления риском реализации информационных угроз организации КФС
	Организация и участие в анализе и контроле адекватности идентификации области применения иных систем управления в рамках ключевых направлений обеспечения информационной безопасности организации КФС
	Проведение анализа и контроля адекватности моделей угроз безопасности информации организации КФС
	Организация и участие в анализе и контроле адекватности оценки риска реализации информационных угроз организации КФС
	Реализация системы внутренней отчетности в рамках управления риском реализации информационных угроз организации КФС
	Контроль применения способа реагирования на риск реализации информационных угроз организации КФС
	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 КФС
	Осуществлять контроль за уровнем риска реализации информационных угроз
	Формировать отчетность по результатам контроля управления риском реализации информационных угроз организации КФС
	Осуществлять контроль применения способа реагирования на риск реализации информационных угроз организации КФС
	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 КФС в части организации контрольных мероприятий
	Требованиия национальных и международных документов в области стандартизации обеспечения зашиты информации организаций КФС, регламентирующих проведение контрольных мероприятий в области защиты информации
	Основные риски реализации информационных угроз в рамках бизнес- и технологических процессов организаций КФС
	Принципы управления рисками реализации информационных угроз организаций КФС
	Состав, назначение и основные цели проведения мероприятий по контролю управлением риском реализации информационных угроз в организации КФС
	Методология проведения оперативного и периодического контроля управлением риском реализации информационных угроз в организации КФС
Другие характеристики	

3.5.2. Трудовая функция

Наименование	Проведение внутреннего контроля защиты информации в организациях КФС	Код	E/01.7	Уровень (подуровень) квалификации	7

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
	Проведение проверок знаний работников организации в части применения мер защиты информации в рамках процесса системы защиты информации
	Фиксация и оформление результатов (свидетельств) проведения мероприятий по контролю реализации процесса системы защиты информации
	Осуществелние регистрации операций по установке и (или) обновлению программного обеспечения технических средств защиты информации
	Осуществление регистрации операций по обновлению сигнатурных баз технических средств защиты информации
	Осуществление регистрации операций по изменению параметров настроек технических мер защиты информации и информационной инфраструктуры, предназначенных для размещения технических мер защиты информации
	Осуществление регистрации сбоев (отказов) технических мер защиты информации
Необходимые умения	Принимать участие в контроле реализации технических средств защиты информации и систем обеспечения защиты информации в информационной инфраструктуре организаций КФС
	Организовывать и осуществлять самооценку соответствия процессов обеспечения защиты информации положениям документов Банка России в области стандартизации обеспечения информационной безопасности организации КФС, требованиям правил платежных систем
	Определять объекты контроля защищенности из состава объектов информационной инфраструктуры организаций КФС
	Принимать участие в реализации контроля защищенности объектов информационной инфраструктуры организаций КФС
	Организовывать категорирование объектов информационной инфраструктуры организации КФС для осуществления мониторинга защиты информации
	Принимать участие в мероприятиях по операционному и периодическому контролю реализации процессов обеспечения защиты информации в организации КФС
	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 КФС
	Формировать правила анализа данных мониторинга информационной безопасности, в том числе для целей выявления событий и инцидентов защиты информации
	Формировать отчетность по результатам контроля защиты информации
	Применять навыки контроля назначенных ролей, исполнения планов повышения осведомленности в обласит защиты информации
	Формировать функциональные требования к средствам и технологиям контроля защиты информации и осуществлять выбор таких средств и технологий
	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	Законодательство Российской Федерации, нормативно-правовые акты Российской Федерации, нормативные акты Банка России в области обеспечения защиты информации, распространяющиеся на деятельность организаций КФС в части организации контрольных мероприятий
	Основные национальные и международные документы в области стандартизации обеспечения зашиты информации организаций КФС, регламентирующие проведение контрольных мероприятий в области защиты информации
	Функционально-технические требования к техническим средствам защиты информации и системам обеспечения защиты информации организаций КФС в целях их контроля
	Состав, назначение и основные цели проведения мероприятий по обеспечению контроля защищенности объектов информационной инфраструктуры организаций КФС
	Состав, назначение и основные цели проведения контрольных мероприятий по обнаружению вторжений и сетевых атак, направленных на информационную инфраструктуру организаций КФС
	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 КФС
	Принципы и правила контроля применения технических средств защиты информации и систем обеспечения защиты информации в информационной инфраструктуре организаций КФС
	Принципы и правила контроля состава объектов информационной инфраструктуры организаций КФС, включая автоматизированные системы и их компоненты, задействованные в реализации бизнес- и технологических процессов организаций КФС (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 КФС (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 КФС
	Возможности по регистрации событий для типовых компонентов информационной инфраструктуры организаций КФС
	Методология проведения оперативного и периодического контроля реализации процессов обеспечения защиты информации в организациях КФС
Другие характеристики	

3.5.3. Трудовая функция

Наименование	Проведение внутреннего контроля операционной надежности организаций КФС	Код	E/02.7	Уровень (подуровень) квалификации	7

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

Трудовые действия	Контроль за фактическими значениями ключевых индикаторов риска, связанных с обеспечением операционной надежности организаций КФС
	Сбор и регистрация информации о функционировании объектов информатизации инфраструктурного уровня, используемых организацией КФС
	Организация и участие в проведении анализа и контроля адекватности идентификации области применения системы обеспечения операционной надежности организаций КФС
	Реализация системы внутренней отчетности в рамках обеспечения операционной надежности организаций КФС

	Участие в тестировании плана восстановления деятельности организаций КФС в случае чрезвычайных ситуаций и оценка эффективности обеспечения операционной надежности организаций КФС в рамках указанного плана
	Организация и проведение тестирования плана восстановления деятельности организаций КФС при реализации инцидентов защиты информации
	Оценка эффективности плана восстановления деятельности организаций КФС при реализации инцидентов защиты информации
	Контроль применения мер, направленных на обеспечение операционной надежности организаций КФС
	Планирование и реализация программ по самооценке полноты и качества состава мер по реализации требований к процессам операционной надежности организаций КФС
Необходимые умения	Осуществлять сбор и регистрацию информации о функционировании объектов информатизации инфраструктурного уровня, используемых организацией КФС
	Осуществлять контроль применения мер, направленных на обеспечение операционной надежности организаций КФС
	Формировать отчетность по результатам контроля обеспечения операционной надежности организаций КФС
	Разрабатывать предложения в планы и программы по самооценке полноты и качества состава мер по реализации требований к процессам обеспечения операционной надежности организаций КФС
Необходимые знания	Законодательство Российской Федерации, нормативно-правовые акты Российской Федерации, нормативные акты Банка России в области обеспечения защиты информации, распространяющиеся на деятельность организаций КФС в части организации контрольных мероприятий
	Основные национальные и международные документы в области стандартизации обеспечения зашиты информации организаций КФС, регламентирующих проведение контрольных мероприятий в области защиты информации
	Основные организационные меры защиты информации для непрерывности выполнения бизнес-- и технологических процессов организаций КФС
	Основные технические меры защиты информации для непрерывности выполнения бизнес-- и технологических процессов организаций КФС
	Принципы контроля защиты информации для непрерывности выполнения бизнес-- и технологических процессов организаций КФС
	Состав, назначение и основные цели проведения мероприятий по контролю защиты информации для непрерывности выполнения бизнес-- и технологических процессов организаций КФС
	Методология проведения оперативного и периодического контроля защиты информации для непрерывности выполнения бизнес-- и технологических процессов организаций КФС
Другие характеристики	

3.5.4. Трудовая функция

Наименование	Проведение внутреннего контроля	Код	E/03.7	Уровень	7

управления риском реализации информационных угроз при аутсорсинге и использовании сторонних информационных сервисов в организациях КФС		(подуровень) квалификации	

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 КФС на аутсорсинге, в части ресурсного обеспечения
	Контроль применения мер, направленных на проведение оценки поставщика услуг, выполняющего бизнес- и (или) технологические процессы организации КФС 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 КФС 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
	Планирование и реализацию программ проведения самооценки полноты и качества реализации настоящих требований к процессам
	Определение и назначение ролей, связанных с выполнением деятельности по контролю за эффективностью управления риском реализации информационных угроз при аутсорсинге и использовании сторонних информационных сервисов
	Определение и назначение ролей, связанных с контролем системы мер, направленных на снижение риска реализации информационных угроз
Необходимые умения	Осуществлять сбор и регистрацию информации об инцидентах защиты информации в случае реализации риска информационных угроз при аутсорсинге и использовании сторонних информационных сервисов
	Осуществлять контроль применения мер, направленных на обеспечение защиты информации при аутсорсинге и использовании сторонних информационных сервисов
	Формировать отчетность по результатам контроля защиты информации при управлении риском информационных угроз при аутсорсинге и использовании сторонних информационных сервисов
	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
	Осуществлять контроль за уровнем риска реализации информационных угроз при аутсорсинге и использовании сторонних информационных сервисов
	Осуществлять контроль применения мер, направленных на проведение оценки поставщика услуг, выполняющего бизнес- и (или) технологические процессы организации КФС на аутсорсинге, в части соблюдения требований к защите информации
	Осуществлять контроль применения мер, направленных на проведение оценки поставщика услуг, выполняющего бизнес- и (или) технологические процессы организации КФС на аутсорсинге, в части соблюдения требований к обеспечению непрерывности деятельности
	Определять и назначать роли, связанные с выполнением деятельности по контролю за эффективностью управления риском реализации информационных угроз при аутсорсинге и использовании сторонних информационных сервисов
	Определять и назначать роли, связанные с контролем системы мер, направленных на снижение риска реализации информационных угроз
Необходимые знания	Законодательство Российской Федерации, нормативно-правовые акты Российской Федерации, нормативные акты Банка России в области обеспечения защиты информации, распространяющиеся на деятельность организаций КФС в части организации контрольных мероприятий
	Основные национальные и международные документы в области стандартизации обеспечения зашиты информации организаций КФС, регламентирующих проведение контрольных мероприятий в области защиты информации
	Основные организационные меры защиты информации для управления риском реализации информационных угроз при аутсорсинге и использовании сторонних информационных сервисов в организациях КФС
	Основные технические меры защиты информации для управления риском реализации информационных угроз при аутсорсинге и использовании сторонних информационных сервисов в организациях КФС
	Принципы контроля защиты информации для управления риском реализации информационных угроз при аутсорсинге и использовании сторонних информационных сервисов в организациях КФС
	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 КФС
	Методология проведения оперативного и периодического контроля защиты информации для управления риском реализации информационных угроз при аутсорсинге и использовании сторонних информационных сервисов в организациях КФС
Другие характеристики	

3.5.5. Трудовая функция

Наименование	Организация внешнего аудита информационной безопасности в организациях КФС	Код	E/04.7	Уровень (подуровень) квалификации	7

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 КФС
	Организация выбора проверяющих организаций, осуществляющих внешний аудит информационной безопасности в организации КФС
	Участие в определении правил и последовательности мероприятий при проведении внешнего аудита информационной безопасности в организации КФС
	Участие в определении перечня неоцениваемых областей оценки соответствия при проведении внешнего аудита информационной безопасности в организации КФС
	Подготовка предложений по выбору источников свидетельств при проведении оценки соответствия обеспечения информационной безопасности в организации КФС
	Участие в анализе параметров конфигураций, фактических настроек и электронных журналов регистрации технических объектов информатизации и средств защиты информации организации КФС, в том числе с использованием технических и программных средств
	Участие в анализе уязвимостей и проведения тестирования на проникновение объектов информационной инфраструктуры организации КФС
	Участие в проведении оценки соответствия обеспечения информационной безопасности в организации КФС
	Участие в определении и расчете оценок соответствия процессов (подпроцессов) системы информационной безопасности и итоговой оценки соответствия обеспечения информационной безопасности в организации КФС
	Участие в подготовке рекомендаций по совершенствованию системы информационной безопасности организации КФС и устранению выявленных нарушений
	Участие в оформлении и представлении результатов внешнего аудита информационной безопасности в организации КФС
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 КФС
	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 КФС
	Принимать участие в подготовке и предоставлении необходимых сведений при формировании свидетельств оценки соответствия информационной безопасности организации КФС
	Применять технические и программные средства в области оценки соответствия информационной безопасности организации КФС
	Принимать участие в формировании отчетных материалов результатов проведения работ по внешнему аудиту информационной безопасности в организации КФС
	Принимать участие в надзорных мероприятиях (инспекционных проверках), проводимых ФинЦЕРТ Банка России
Необходимые знания	Законодательство Российской Федерации, нормативно-правовые акты Российской Федерации, устанавливающие организационно-правовые основания (режим) деятельности организаций КФС в рамках проведения внешнего аудита информационной безопасности
	Состав, назначение и основные положения документов Банка России, регламентирующие вопросы проведения внешнего аудита информационной безопасности в организации КФС
	Состав, назначение и основные положения международных и национальных стандартов, регламентирующие вопросы проведения внешнего аудита информационной безопасности в организации КФС
	Состав, принципы, условия проведения внешнего аудита информационной безопасности в организациях КФС
	Цели, правила организации и проведения внешнего аудита внешнего аудита информационной безопасности в организациях КФС
	Назначение и основные мероприятия проведения внешнего аудита информационной безопасности в организациях КФС
	Состав, назначение и основные положения нормативно-правовых актов Российской Федерации, нормативных актов Банка России, регулирующих контроль обеспечения информационной безопасности в организациях КФС со стороны уполномоченных надзорных органов и Банка России
	Правила и правовые основания проведения контроля и осуществления взаимодействия организации КФС с надзорными подразделениями Банка России
	Цели и правила организации взаимодействия с ФинЦЕРТ Банка России в рамках проведения внешнего аудита информационной безопасности организации КФС
Другие характеристики	

3.6. Обобщенная трудовая функция

Наименование	Управление риском реализации информационных угроз	Код	F	Уровень квалификации	7

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 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[4]	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))

3.6.1. Трудовая функция

Наименование	Методологическое обеспечение управления риском реализации информационных угроз в организациях КФС	Код	A/01.7	Уровень (подуровень) квалификации	7

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

Трудовые действия	Разработка и согласование политики управления риском реализации информационных угроз в организациях КФС
	Выявление и идентификация риска реализации информационных угроз в организациях КФС
	Моделирование угроз безопасности информации в организациях КФС
	Оценка риска реализации информационных угроз в организациях КФС
	Выбор и применение способа реагирования на риск реализации информационных угроз в организациях КФС
	Разработка системы мер, направленных на снижение риска реализации информационных угроз в организациях КФС
	Планирование системы мер, направленных на снижение риска реализации информационных угроз в организациях КФС
	Планирование применения мер, направленных на предотвращение реализации (снижение степени возможности реализации инцидентов защиты информации) инцидентов защиты информации в организациях КФС
	Планирование применения мер, направленных на ограничение степени тяжести последствий реализации инцидентов защиты информации в результате реализации инцидентов защиты информации в организациях

	КФС
Необходимые умения	Работать с действующей нормативно - правовой и методологической базой в области упрвления риском реализации информационных угроз в организациях КФС
	Анализировать и применять в организации КФС требования законодательства Российской Федерации и нормативных актов Банка России по вопросам упрвления риском реализации информационных угроз в организациях КФС
	Анализировать и применять в организации КФС требования национальных и международных стандартов по вопросам упрвления риском реализации информационных угроз в организациях КФС
	Определять состав, а также сигнальные и контрольные значения ключевого индикатора риска реализации информационных угроз в организации КФС
	Осуществлять мониторинг значений ключевого индикатора риска реализации информационных угроз в организации КФС, включая мониторинг инцидентов защиты информации
	Разрабатывать модели угроз безопасности информации в организациях КФС
	Разрабатывать проекты внутренних документов организации КФС, устанавливающих цели и принципы обеспечения управления риском реализации информационных угроз
	Разрабатывать проекты внутренних документов организации КФС, определяющих методологию, правила организации и реализации состава мер по оценке риска реализации информационных угроз в организациях КФС
	Разрабатывать предложения по выбору способа реагирования на риска реализации информационных угроз в организациях КФС
	Планировать работу по раегированию на риск реализации информационных угроз в организациях КФС
	Разрабатывать проекты планов, внутренних документов организации КФС по реагированию на риск реализации информационных угроз в организациях КФС
Необходимые знания	Законодательство Российской Федерации по вопросам управления риском реализации информационных угроз в организациях КФС
	Нормативные акты Банка России по вопросам управления риском реализации информационных угроз в организациях КФС
	Основные национальные и международные документы в области стандартизации управления риском реализации информационных угроз в организациях КФС
	Документы Банка России в области стандартизации управления риском реализации информационных угроз в организациях КФС
	Основные цели управления риском реализации информационных угроз в рамках бизнес- и технологических процессов организаций КФС
	Основные риски реализации информационных угроз в рамках бизнес- и технологических процессов организаций КФС
	Принципы управления рисками реализации информационных угроз организаций КФС
Другие характеристики	

3.6.2. Трудовая функция

Наименование	Реализация системы управления риском реализации информационных угроз	Код	F/02.7	Уровень (подуровень) квалификации	7

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

Трудовые действия	Организация и сопровождение процессов реализации состава мер по защите информации в организациях КФС
	Организация и сопровождение процессов реализации состава мер по операционной надежности в организациях КФС
	Организация и сопровождение процессов реализации состава мер управлению риском реализации информационных угроз в организациях КФС
	Организация и сопровождение процессов реализации состава мер по управлению риском реализации информационных угроз при аутсорсинге и взаимодействии с поставщиками услуг
	Организация и сопровождение процессов реализации состава мер по правлению риском внутреннего нарушителя в организация КФС
	Выявление, классификация, регистрация и определение ущерба от событий риска реализации информационных угроз
	Выявление и регистрация инцидентов защиты информации, в том числе обнаружение компьютерных атак
	Выявление фактов (индикаторов) компрометации объектов информатизации
	Разработка и согласование предложений по организации необходимого и достаточного ресурсного (кадрового и финансового) обеспечения процессов системы управления риском реализации информационных угроз в организациях КФС
	Разработка, реализация планов и программ обучения и повышения осведомленности в части противодействия информационным угрозам и контроль результатов
	Разработка и реализация способов мотивации персонала организации КФС к участию в управлении риском реализации информационных угроз
	Организация и сопровождение процессов взаимодействия с клиентами организации КФС с целью повышения осведомленности клиентов в части противодействия информационным угрозам
	Организация и сопровождение процессов взаимодействия с клиентами организации КФС с целью обеспечения защиты информации при предоставлении финансовых (банковских) услуг, в том числе при осуществлении переводов денежных средств
	Ведение претензионной работы
Необходимые умения	Разрабатывать предложения по реализации состава мер по защите информации в организациях КФС

	Разрабатывать предложения по реализации состава мер по операционной надежности в организациях КФС
	Разрабатывать предложения по реализации состава мер управлению риском реализации информационных угроз в организациях КФС
	Разрабатывать предложения по управлению риском реализации информационных угроз при аутсорсинге и взаимодействии с поставщиками услуг
	Разрабатывать предложения по правлению риском внутреннего нарушителя в организация КФС
	Организовывать реализацию проектов по вопросам обработки рисков реализации информационных угроз в организации КФС
	Организовывать внедрение и применение политик (правил, процедур), направленных на предотвращение (снижение степени вероятности реализации) реализации инцидентов защиты информации
	Разрабатывать предложения по организации необходимого и достаточного ресурсного (кадрового и финансового) обеспечения процессов системы управления риском реализации информационных угроз организации КФС
	Разрабатывать планы и программы обучения и повышения осведомленности в части противодействия информационным угрозам организации КФС
	Разрабатывать способы мотивации персонала организации КФС к участию в управлении риском реализации информационных угроз
	Организовывать сопровождение процессов взаимодействия с клиентами организации КФС с целью повышения осведомленности клиентов в части противодействия информационным угрозам
	Организовывать сопровождение процессов взаимодействия с клиентами организации КФС с целью обеспечения защиты информации при предоставлении финансовых (банковских) услуг, в том числе при осуществлении переводов денежных средств
Необходимые знания	Законодательство Российской Федерации по вопросам управления риском реализации информационных угроз в организациях КФС
	Нормативные акты Банка России по вопросам управления риском реализации информационных угроз в организациях КФС
	Основные национальные и международные документы в области стандартизации управления риском реализации информационных угроз в организациях КФС
	Документы Банка России в области стандартизации управления риском реализации информационных угроз в организациях КФС
	Основные цели управления риском реализации информационных угроз в рамках бизнес- и технологических процессов организаций КФС
	Основные риски реализации информационных угроз в рамках бизнес- и технологических процессов организаций КФС
	Принципы управления рисками реализации информационных угроз организаций КФС
	Уязвимости и связанные с ними риски нарушения защиты информации, присущие используемых организациями КФС, процессов проектирования, приобретения, эксплуатации и сопровождения эксплуатации автоматизированных систем
Другие характеристики	

3.6.3. Трудовая функция

Наименование	Контроль системы управления риском реализации информационных угроз	Код	F/03.7	Уровень (подуровень) квалификации	7

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

Трудовые действия	Организация контроля за фактическими значениями контрольных показателей уровня риска реализации информационных угроз
	Проведение независимой оценки соответствия процессов защиты информации и обеспечения операционной надежности
	Тестирование готовности финансовой организации противостоять реализации информационных угроз
	Определение набора ключевых индикаторов риска реализации информационных угроз
	Организация мониторинга риска реализации информационных угроз на основе ключевых индикаторов риска реализации информационных угроз
	Оценка эффективности выполнения процессов управления риском реализации информационных угроз
	Формирование внутренней отчетности об эффективности управления риском реализации информационных угроз.
Необходимые умения	Организовать контроля за фактическими значениями контрольных показателей уровня риска реализации информационных угроз
	Контролировать фактические значения контрольных показателей уровня риска реализации информационных угроз
	Организовывать проведение независимой оценки соответствия процессов защиты информации и обеспечения операционной надежности
	Проводить независимую оценку соответствия процессов защиты информации и обеспечения операционной надежности
	Тестировать готовность финансовой организации противостоять реализации информационных угроз
	Определять набор ключевых индикаторов риска реализации информационных угроз
	Организовывать мониторинг риска реализации информационных угроз на основе ключевых индикаторов риска реализации информационных угроз
	Осуществлять мониторинг риска реализации информационных угроз на основе ключевых индикаторов риска реализации информационных угроз
	Оценивать эффективности выполнения процессов управления риском реализации информационных угроз
	Организовывать формирование внутренней отчетности об эффективности управления риском реализации информационных угроз.
	Осуществлять формирование внутренней отчетности об эффективности управления риском реализации информационных угроз.
Необходимые знания	Законодательство Российской Федерации по вопросам управления риском реализации информационных угроз в организациях КФС

	Нормативные акты Банка России по вопросам управления риском реализации информационных угроз в организациях КФС
	Основные национальные и международные документы в области стандартизации управления риском реализации информационных угроз в организациях КФС
	Документы Банка России в области стандартизации управления риском реализации информационных угроз в организациях КФС
	Основные цели управления риском реализации информационных угроз в рамках бизнес- и технологических процессов организаций КФС
	Основные риски реализации информационных угроз в рамках бизнес- и технологических процессов организаций КФС
	Принципы управления рисками реализации информационных угроз организаций КФС
	Уязвимости и связанные с ними риски нарушения защиты информации, присущие используемых организациями КФС, процессов проектирования, приобретения, эксплуатации и сопровождения эксплуатации автоматизированных систем
Другие характеристики	

3.6.4. Трудовая функция

Наименование	Совершенствование системы управления риском реализации информационных угроз	Код	F/03.7	Уровень (подуровень) квалификации	7

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

Трудовые действия	Проведение анализа необходимости совершенствования системы управления риском реализации информационных угроз
	Разработка и согласование изменений политики финансовой организации в отношении принципов и приоритетов в реализации системы управления риском реализации информационных угроз, в том числе целевых показателей реагирования на инциденты защиты информации и восстановления после их реализации
	Разработка и согласование изменений политики финансовой организации в отношении величины допустимого риска реализации информационных угроз
	Разработка и согласование изменений политики финансовой организации в отношении аутсорсинга
	Внедрение финансовой организацией новых технологий предоставления финансовых (банковских) и (или) информационных услуг
	Организация принятия решений по совершенствованию системы управления риском реализации информационных угроз

	Определение источников информации для проведения анализа необходимости совершенствования системы управления риском реализации информационных угроз
	Анализ результатов эффективности системы управления риском реализации информационных угроз в целях принятия решения о необходимости ее совершенствования
	Разработка и согласование предложений по повышению эффективности системы управления риском реализации информационных угроз в целях принятия решения о необходимости ее совершенствования
Необходимые умения	Проводить анализ необходимости совершенствования системы управления риском реализации информационных угроз
	Разрабатывать изменения политики финансовой организации в отношении принципов и приоритетов в реализации системы управления риском реализации информационных угроз, в том числе целевых показателей реагирования на инциденты защиты информации и восстановления после их реализации
	Организовывать согласование изменений политики финансовой организации в отношении принципов и приоритетов в реализации системы управления риском реализации информационных угроз, в том числе целевых показателей реагирования на инциденты защиты информации и восстановления после их реализации
	Разрабатывать изменения политики финансовой организации в отношении величины допустимого риска реализации информационных угроз
	Разрабатывать и согласовывать изменений политики финансовой организации в отношении величины допустимого риска реализации информационных угроз
	Организовывать согласование изменений политики финансовой организации в отношении аутсорсинга
	Внедрять в деятельность финансовой организации новых технологий предоставления финансовых (банковских) и (или) информационных услуг
	Организовывать принятие решений по совершенствованию системы управления риском реализации информационных угроз
	Определять источники информации для проведения анализа необходимости совершенствования системы управления риском реализации информационных угроз
	Анализировать источники информации для проведения анализа необходимости совершенствования системы управления риском реализации информационных угроз
	Анализировать результаты эффективности системы управления риском реализации информационных угроз в целях принятия решения о необходимости ее совершенствования
	Разрабатывать предложения по повышению эффективности системы управления риском реализации информационных угроз в целях принятия решения о необходимости ее совершенствования
	Организовывать согласование предложений по повышению эффективности системы управления риском реализации информационных угроз в целях принятия решения о необходимости ее совершенствования
Необходимые знания	Законодательство Российской Федерации по вопросам управления риском реализации информационных угроз в организациях КФС
	Нормативные акты Банка России по вопросам управления риском реализации информационных угроз в организациях КФС
	Основные национальные и международные документы в области стандартизации управления риском реализации информационных угроз в организациях КФС
	Документы Банка России в области стандартизации управления риском

	реализации информационных угроз в организациях КФС
	Основные цели управления риском реализации информационных угроз в рамках бизнес- и технологических процессов организаций КФС
	Основные риски реализации информационных угроз в рамках бизнес- и технологических процессов организаций КФС
	Принципы управления рисками реализации информационных угроз организаций КФС
	Уязвимости и связанные с ними риски нарушения защиты информации, присущие используемых организациями КФС, процессов проектирования, приобретения, эксплуатации и сопровождения эксплуатации автоматизированных систем
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)

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