УТВЕРЖДЕН
приказом Министерства
труда и социальной защиты
Российской Федерации
от 28 ноября 2022 № 739н

ПРОФЕССИОНАЛЬНЫЙ СТАНДАРТ

Специалист по информационной безопасности в кредитно-финансовой сфере

1593
Регистрационный номер

Содержание

I. Общие сведения

Обеспечение информационной безопасности в организациях кредитно-финансовой сферы (далее – КФС)	06.053
(наименование вида профессиональной деятельности)	Код

Основная цель вида профессиональной деятельности:

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

Группа занятий:

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

Отнесение к видам экономической деятельности:

62.02.9	Деятельность консультативная в области компьютерных технологий прочая
66	Деятельность вспомогательная в сфере финансовых услуг и страхования
(код ОКВЭД)	(наименование вида экономической деятельности)

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

Обобщенные трудовые функции			Трудовые функции		
код	наименование	уровень квалификации	наименование	код	уровень (подуровень) квалификации
A	Обеспечение функционирования систем и средств защиты информации в организациях КФС	6	Проведение работ по установке, настройке и техническому обслуживанию систем и средств защиты информации в организациях КФС	A/01.6	6
			Администрирование систем и средств защиты информации в организациях КФС	A/02.6	6
			Реализация процессов обеспечения операционной надежности (киберустойчивости) в организациях КФС	A/03.6	6
B	Управление инцидентами информационной безопасности в организациях КФС	7	Выявление и регистрация инцидентов информационной безопасности, в том числе обнаружение компьютерных атак, в организациях КФС	B/01.7	7
			Реагирование на инциденты информационной безопасности в организациях КФС	B/02.7	7
			Восстановление функционирования бизнес-процессов и технологических процессов и объектов информатизации после реализации инцидентов информационной безопасности в организациях КФС	B/03.7	7
C	Аналитическое и организационное сопровождение деятельности по управлению рисками информационной безопасности в организациях КФС	7	Сбор и регистрация информации о выявленных рисках информационной безопасности в организациях КФС	C/03.7	7
			Разработка мероприятий, направленных на уменьшение негативного влияния рисков информационной безопасности в организациях КФС	C/04.7	7
			Определение угроз информационной безопасности в организациях КФС	C/01.7	7
			Выявление, идентификация и оценка рисков информационной безопасности в организациях КФС	C/02.7	7
			Мониторинг рисков информационной безопасности и контроль	C/05.7	7

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

	информационной безопасности в организациях КФС		безопасности на высшем управленческом уровне в организациях КФС		
			Организация обеспечения защиты информации и операционной надежности (киберустойчивости) на высшем управленческом уровне в организациях КФС	F/02.8	8
			Контроль процедур управления рисками информационной безопасности и обеспечения защиты информации и операционной надежности (киберустойчивости) на высшем управленческом уровне в организациях КФС	F/03.8	8
			Совершенствование системы управления рисками информационной безопасности, обеспечение защиты информации и операционной надежности (киберустойчивости) на высшем управленческом уровне в организациях КФС	F/04.8	8

III. Характеристика обобщенных трудовых функций

3.1. Обобщенная трудовая функция «Обеспечение функционирования систем и средств защиты информации в организациях КФС»

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

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

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

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

Дополнительные характеристики

Наименование документа	Код	Наименование базовой группы, должности (профессии) или специальности
ОКЗ	2529.	Специалисты по базам данных и сетям, не входящие в другие группы
ЕТКС или ЕКС		Администратор по обеспечению безопасности информации
		Инженер по защите информации
		Специалист по защите информации
		Инженер-программист по технической защите информации
ОКПДТР	22567	Инженер по защите информации
	26579	Специалист по защите информации
ОКСО 2016	2.10.03.01	Информационная безопасность

3.1.1. Трудовая функция

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

Происхождение обобщенной трудовой функции	Оригинал X	Заимствовано из оригинала		1593
			Код оригинала	Регистрационный номер профессионального стандарта

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

	области защиты информации
	Современные информационные технологии (операционные системы, базы данных, вычислительные сети)
	Угрозы безопасности информации в автоматизированных системах
	Методы и средства защиты информации, в том числе СКЗИ, в автоматизированных системах
	Организационно-распорядительные документы по защите информации в автоматизированных системах в организациях КФС
	Технические описания и инструкции (руководства) по эксплуатации систем и средств защиты информации, в том числе СКЗИ, в автоматизированных системах
	Порядок организации технического обслуживания систем и средств защиты информации в соответствии с инструкциями и эксплуатационно-технической документацией
	Порядок устранения неисправностей и организации ремонта программно-аппаратных (технических) средств защиты информации
Особые условия допуска к работе	-
Другие характеристики	-

3.1.2. Трудовая функция

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

Происхождение обобщенной трудовой функции	Оригинал	X	Заимствовано из оригинала		1593
				Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Определение состава и порядка применения программно-аппаратных средств защиты информации в организациях КФС
	Конфигурирование программно-аппаратных средств защиты информации в операционных системах в организациях КФС
	Контроль корректности функционирования программно-аппаратных средств защиты информации в операционных системах в организациях КФС
	Управление правами пользователей автоматизированной системы в организациях КФС
	Обеспечение безопасности информации с учетом требования эффективного функционирования автоматизированной системы в организациях КФС
	Управление антивирусной защитой операционных систем в соответствии с действующими требованиями в организациях КФС
	Контроль соблюдения требований к защите информации при установке программного обеспечения, включая антивирусное программное обеспечение, в организациях КФС

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

	криптографические, технические) в организациях КФС
Особые условия допуска к работе	-
Другие характеристики	-

3.1.3. Трудовая функция

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

Происхождение обобщенной трудовой функции	Оригинал	X	Заимствовано из оригинала		1593
				Код оригинала	Регистрационный номер профессионального стандарта

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

	Принципы обеспечения операционной надежности (киберустойчивости) в организациях КФС
	Базовый состав организационных, технологических и технических мер обеспечения операционной надежности (киберустойчивости) в организациях КФС
	Подходы к сегментации вычислительных сетей в организациях КФС
	Специфика платежных процессов в организациях КФС
	Основы обеспечения безопасности объектов информатизации прикладного уровня в организациях КФС
	Подходы к подтверждению реализации функций безопасности и контроля (наличия) уязвимостей объектов информатизации прикладного уровня в организациях КФС
Особые условия допуска к работе	-
Другие характеристики	-

3.2. Обобщенная трудовая функция «Управление инцидентами информационной безопасности в организациях КФС»

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

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

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

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

Дополнительные характеристики

Наименование документа	Код	Наименование базовой группы, должности (профессии) или специальности
ОКЗ	2529.	Специалисты по базам данных и сетям, не входящие в другие группы
ЕТКС или ЕКС		Администратор по обеспечению безопасности информации
		Инженер по защите информации
		Инженер-программист по технической защите

		информации
		Специалист по обеспечению безопасности информации в ключевых системах информационной инфраструктуры
ОКПДТР	22567	Инженер по защите информации
	26579	Специалист по защите информации
ОКСО 2016	2.10.04.01	Информационная безопасность
	2.10.05.01	Компьютерная безопасность
	2.10.05.02	Информационная безопасность телекоммуникационных систем
	2.10.05.03	Информационная безопасность автоматизированных систем
	2.10.05.04	Информационно-аналитические системы безопасности
	2.10.05.05	Безопасность информационных технологий в правоохранительной сфере
	2.10.05.06	Криптография
	2.10.05.07	Противодействие техническим разведкам

3.2.1. Трудовая функция

Наименование	Выявление и регистрация инцидентов информационной безопасности, в том числе обнаружение компьютерных атак, в организациях КФС	Код	B/01.7	Уровень квалификации	7

Происхождение обобщенной трудовой функции	Оригинал X	Заимствовано из оригинала		1593
			Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Оперативный мониторинг и выявление событий информационной безопасности, в том числе обнаружение компьютерных атак, в организациях КФС
	Сбор данных для регистрации событий информационной безопасности, в том числе компьютерных атак, в организациях КФС
	Обеспечение функционирования механизмов и инициативного информирования подразделений, ответственных за управление рисками информационной безопасности, работников организаций КФС о событиях информационной безопасности в организациях КФС
	Организация и выполнение деятельности по получению и использованию сведений об актуальных индикаторах компрометации объектов информатизации в организациях КФС
	Автоматизация процедур выявления наличия индикаторов компрометации в организациях КФС
	Сбор и регистрация информации об инцидентах информационной безопасности в организациях КФС
Необходимые умения	Анализировать и применять методологическую базу, требования законодательства Российской Федерации, нормативных актов Банка

	России, международных и национальных стандартов в области защиты информации, обеспечения информационной безопасности, управления рисками информационной безопасности в организациях КФС, а также обнаружения, предупреждения и ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры организаций КФС, и реагирования на компьютерные инциденты
	Настраивать средства (агенты, интерфейсы) сбора технических данных для выявления событий информационной безопасности в организациях КФС, в том числе для обнаружения компьютерных атак
	Осуществлять работу с техническими средствами защиты информации и системами, реализующими функции управления инцидентами информационной безопасности в организациях КФС
	Анализировать технические данные, свидетельствующие о возникновении событий информационной безопасности в организациях КФС, в том числе об обнаружении компьютерных атак
	Формировать отчетность о выявленных событиях и инцидентах информационной безопасности в организациях КФС
Необходимые знания	Законодательство Российской Федерации, нормативные правовые акты, национальные, межгосударственные и международные стандарты в области защиты информации, обеспечения информационной безопасности, управления рисками информационной безопасности в организациях КФС
	Законодательство Российской Федерации, нормативные правовые акты, национальные, межгосударственные и международные стандарты в области защиты информации, обеспечения информационной безопасности, управления рисками информационной безопасности в организациях КФС, а также обнаружения, предупреждения и ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры и реагирования на компьютерные инциденты
	Руководящие и методические документы уполномоченных федеральных органов исполнительной власти, нормативные акты Банка России в области защиты информации, обеспечения информационной безопасности, управления рисками информационной безопасности в организациях КФС, а также обнаружения, предупреждения и ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры, реагирования на компьютерные инциденты
	Основные уязвимости и угрозы нарушения защиты информации, характерные для организаций КФС
	Базовый состав и функциональные возможности технических средств сбора технических данных для выявления событий информационной безопасности, в том числе обнаружения компьютерных атак, в организациях КФС
	Принципы построения систем обеспечения защиты информации и операционной надежности (киберустойчивости) в организациях КФС
	Подходы к настройке средств сбора технических данных для выявления событий и инцидентов информационной безопасности в организациях КФС, в том числе обнаружения компьютерных атак

	Специфика платежных процессов в организациях КФС
	Типичные события и инциденты информационной безопасности в организациях КФС
	Подходы к описанию сценариев реализации инцидентов информационной безопасности в организациях КФС
Особые условия допуска к работе	-
Другие характеристики	-

3.2.2. Трудовая функция

Наименование	Реагирование на инциденты информационной безопасности в организациях КФС	Код	B/02.7	Уровень квалификации	7

Происхождение обобщенной трудовой функции	Оригинал	X	Заимствовано из оригинала		1593
				Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Реализация порядка реагирования на инциденты информационной безопасности в организациях КФС
	Сбор информации об инцидентах информационной безопасности в организациях КФС, их классификация и оценка критичности
	Выполнение действий по реагированию на инциденты информационной безопасности в соответствии с едиными правилами и процедурами реагирования на такие инциденты в организациях КФС
	Разработка единых правил и процедур реагирования на инциденты информационной безопасности в организациях КФС
	Осуществление взаимодействия с подразделениями организации КФС, Банком России, федеральными органами исполнительной власти и иными уполномоченными организациями в рамках реагирования на инциденты информационной безопасности, в том числе обнаружения, предупреждения и ликвидации последствий компьютерных атак в организации КФС, а также с внешними заинтересованными организациями
	Информирование Банка России об инцидентах информационной безопасности в организациях КФС в установленном порядке
Необходимые умения	Анализировать и применять методологическую базу, требования законодательства Российской Федерации, нормативных актов Банка России, международных и национальных стандартов в области управления рисками информационной безопасности, обеспечения защиты информации и операционной надежности (киберустойчивости) в организациях КФС
	Настраивать средства (агенты, интерфейсы) сбора технических данных для выявления событий информационной безопасности в организациях КФС
	Осуществлять работу с техническими средствами защиты информации и

	системами, реализующими функции управления инцидентами информационной безопасности организаций КФС
	Анализировать технические данные, свидетельствующие о возникновении событий информационной безопасности в организациях КФС
	Формировать отчетность о выявленных событиях и инцидентах информационной безопасности в организациях КФС
	Применять меры, направленные на снижение тяжести последствий реализации инцидентов информационной безопасности в организациях КФС
	Применять методологию оценки потенциала влияния (критичности) инцидента информационной безопасности организаций КФС
Необходимые знания	Законодательство Российской Федерации, нормативные акты Банка России, международные и национальные стандарты в области обеспечения информационной безопасности, управления рисками информационной безопасности в организациях КФС
	Законодательство Российской Федерации, нормативные правовые акты, национальные, межгосударственные и международные стандарты в области защиты информации, обеспечения информационной безопасности, управления рисками информационной безопасности в организациях КФС
	Руководящие и методические документы уполномоченных федеральных органов исполнительной власти, нормативные акты Банка России в области защиты информации, обеспечения информационной безопасности, управления рисками информационной безопасности в организациях КФС, а также в области обнаружения, предупреждения и ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры, реагирования на компьютерные инциденты
	Основные уязвимости и угрозы нарушения защиты информации, характерные для организаций КФС
	Базовый состав и функциональные возможности технических средств сбора технических данных для выявления событий информационной безопасности в организациях КФС
	Принципы построения систем обеспечения защиты информации и операционной надежности (киберустойчивости) в организациях КФС
	Подходы к настройке средств сбора технических данных для выявления событий и инцидентов информационной безопасности в организациях КФС
	Типичные события и инциденты информационной безопасности в организациях КФС
	Специфика платежных процессов в организациях КФС
	Принципы работы с техническими средствами защиты информации, реализующими функции управления инцидентами информационной безопасности в организациях КФС
	Подходы к описанию сценариев реализации инцидентов информационной безопасности в организациях КФС
Особые условия допуска к работе	-
Другие характеристики	-

3.2.3. Трудовая функция

Наименование	Восстановление функционирования бизнес-процессов и технологических процессов и объектов информатизации после реализации инцидентов информационной безопасности в организациях КФС	Код	B/03.7	Уровень квалификации	7

Происхождение обобщенной трудовой функции	Оригинал	X	Заимствовано из оригинала		1593
				Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Реализация порядка восстановления функционирования бизнес-процессов и технологических процессов и объектов информатизации после реализации инцидентов информационной безопасности в организациях КФС
	Выполнение действий по восстановлению функционирования бизнес-процессов и технологических процессов и объектов информатизации после инцидентов информационной безопасности в соответствии с едиными правилами и процедурами после реализации таких инцидентов в организациях КФС
	Разработка единых правил и процедур восстановления функционирования бизнес-процессов и технологических процессов и объектов информатизации после реализации инцидентов информационной безопасности в организациях КФС
	Определение критериев и проведение оценки завершения восстановления функционирования бизнес-процессов и технологических процессов и объектов информатизации, условий закрытия инцидента информационной безопасности в организациях КФС
	Сбор и фиксация технических данных (свидетельств) в рамках восстановления функционирования бизнес-процессов и технологических процессов и объектов информатизации после реализации инцидентов информационной безопасности в организациях КФС
	Осуществление взаимодействия с подразделениями организации КФС, Банком России, федеральными органами исполнительной власти, иными уполномоченными организациями в рамках восстановления функционирования бизнес-процессов и технологических процессов и объектов информатизации после реализации инцидентов информационной безопасности в организациях КФС, а также с внешними заинтересованными организациями
	Информирование Банка России о статусе обработки инцидента информационной безопасности в организациях КФС
Необходимые умения	Анализировать и применять методологическую базу, требования законодательства Российской Федерации, нормативных актов Банка России, международных и национальных стандартов в области управления рисками информационной безопасности, обеспечения защиты информации и операционной надежности (киберустойчивости) в

	организациях КФС
	Осуществлять работу с техническими средствами защиты информации и системами, реализующими функции управления инцидентами информационной безопасности в организациях КФС
	Анализировать технические данные, свидетельствующие о возникновении событий информационной безопасности в организациях КФС
	Формировать отчетность в рамках восстановления функционирования бизнес-процессов и технологических процессов и объектов информатизации после реализации инцидентов информационной безопасности в организациях КФС
	Работать с техническими средствами защиты информации, реализующими функции управления инцидентами информационной безопасности в организациях КФС
	Применять меры, направленные на снижение тяжести последствий реализации инцидентов информационной безопасности в организациях КФС
Необходимые знания	Законодательство Российской Федерации, нормативные правовые акты, национальные, межгосударственные и международные стандарты в области защиты информации, обеспечения информационной безопасности, управления рисками информационной безопасности в организациях КФС
	Руководящие и методические документы уполномоченных федеральных органов исполнительной власти, нормативные акты Банка России в области защиты информации, обеспечения информационной безопасности, управления рисками информационной безопасности в организациях КФС, а также в области обнаружения, предупреждения и ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры, реагирования на компьютерные инциденты
	Основные уязвимости и угрозы нарушения защиты информации, характерные для организаций КФС
	Базовый состав и функциональные возможности технических средств сбора технических данных для выявления событий информационной безопасности в организациях КФС
	Принципы построения систем обеспечения защиты информации и операционной надежности (киберустойчивости) в организациях КФС
	Типичные события и инциденты информационной безопасности в организациях КФС
	Принципы работы с техническими средствами защиты информации, реализующими функции управления инцидентами информационной безопасности в организациях КФС
	Подходы к описанию сценариев реализации инцидентов информационной безопасности в организациях КФС
Особые условия допуска к работе	-
Другие характеристики	-

3.3. Обобщенная трудовая функция «Аналитическое и организационное сопровождение деятельности по управлению рисками информационной безопасности в организациях КФС»

Наименование	Аналитическое и организационное сопровождение деятельности по управлению рисками 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, профессий	Главный специалист по информационной безопасности Ведущий специалист по информационной безопасности Руководитель структурного подразделения

Требования к образованию и обучению	Высшее профильное образование – магистратура или специалитет в области информационной безопасности или Высшее образование (непрофильное) – магистратура или специалитет и дополнительное профессиональное образование (профессиональная переподготовка) в области информационной безопасности
Требования к опыту практической работы	Не менее двух лет в области информационной безопасности в организациях КФС
Особые условия допуска к работе	Наличие допуска к государственной тайне (при необходимости)
Другие характеристики	-

Дополнительные характеристики

Наименование документа	Код	Наименование базовой группы, должности (профессии) или специальности
ОКЗ	2529.	Специалисты по базам данных и сетям, не входящие в другие группы
ЕТКС или ЕКС		Главный специалист по технической защите информации
ОКПДТР	20911	Главный специалист по защите информации
ОКСО 2016	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
	2.09.04.01	Информатика и вычислительная техника
	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
	2.10.05.01	Компьютерная безопасность
	2.10.05.02	Информационная безопасность

		телекоммуникационных систем
	2.10.05.03	Информационная безопасность автоматизированных систем
	2.10.05.04	Информационно-аналитические системы безопасности
	2.10.05.05	Безопасность информационных технологий в правоохранительной сфере
	2.10.05.06	Криптография
	2.10.05.07	Противодействие техническим разведкам

3.3.1. Трудовая функция

Наименование	Сбор и регистрация информации о выявленных рисках информационной безопасности в организациях КФС	Код	C/03.7	Уровень квалификации	7

Происхождение обобщенной трудовой функции	Оригинал X	Заимствовано из оригинала		1593
			Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Выявление и классификация событий рисков информационной безопасности в организациях КФС
	Ведение базы данных о событиях рисков и регистрация событий рисков информационной безопасности в организациях КФС
	Определение потерь от реализации событий рисков информационной безопасности в организациях КФС
	Организация сбора информации о событиях рисков информационной безопасности в организациях КФС
	Проведение анализа причин и последствий реализации инцидентов информационной безопасности в организациях КФС
Необходимые умения	Анализировать и применять методологическую базу, требования законодательства Российской Федерации, нормативных актов Банка России, международных и национальных стандартов в области управления рисками информационной безопасности, обеспечения защиты информации и операционной надежности (киберустойчивости) в организациях КФС
	Разрабатывать проекты внутренних документов (локальные акты, организационно-распорядительные документы и методические материалы) организации КФС по вопросам рисков информационной безопасности в организациях КФС
	Обеспечивать ведение базы данных о событиях рисков информационной безопасности в организациях КФС
	Применять методологию проведения оценки потерь от реализации рисков информационной безопасности в организациях КФС
	Организовывать процесс сбора информации о событиях рисков информационной безопасности организаций КФС от структурных подразделений (владельцев рисков) организаций КФС, в том числе о результатах претензионной работы

	Анализировать технические данные, свидетельствующие о возникновении событий и инцидентов информационной безопасности в организациях КФС
Необходимые знания	Законодательство Российской Федерации, нормативные правовые акты, национальные, межгосударственные и международные стандарты в области защиты информации, обеспечения информационной безопасности, управления рисками информационной безопасности в организациях КФС
	Руководящие и методические документы уполномоченных федеральных органов исполнительной власти, нормативные акты Банка России в области защиты информации, обеспечения информационной безопасности, управления рисками информационной безопасности в организациях КФС
	Принципы управления рисками информационной безопасности, обеспечения информационной безопасности в организациях КФС
	Специфика платежных процессов в организациях КФС
	Принципы построения архитектуры информационной безопасности
	Основные источники рисков информационной безопасности в рамках бизнес-процессов и технологических процессов организаций КФС
	Классификация событий рисков информационной безопасности организаций КФС
	Основы организации и ведения баз данных
Особые условия допуска к работе	-
Другие характеристики	-

3.3.2. Трудовая функция

Наименование	Разработка мероприятий, направленных на уменьшение негативного влияния рисков информационной безопасности в организациях КФС	Код	C/04.7	Уровень квалификации	7

Происхождение обобщенной трудовой функции	Оригинал	X	Заимствовано из оригинала		1593
				Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Определение способов реагирования на риски информационной безопасности в организациях КФС
	Организация и выполнение работ по разработке плана реагирования на риски информационной безопасности в организациях КФС
	Определение контрольных и сигнальных значений показателей в рамках плана реагирования на риски информационной безопасности организаций КФС в соответствии с допустимым уровнем рисков информационной безопасности организаций КФС (риск-аппетитом финансовой организации)

	Определение технологических мер защиты информации, обрабатываемой в рамках технологических операций при выполнении бизнес-процессов и технологических процессов в организациях КФС
	Определение организационных и технических мер защиты информации и обеспечения операционной надежности (киберустойчивости) в организациях КФС
	Разработка мероприятий, направленных на ограничение степени тяжести последствий в результате инцидентов, связанных с реализаций информационных угроз в организациях КФС
Необходимые умения	Анализировать и применять методологическую базу, требования законодательства Российской Федерации, нормативных актов Банка России, международных и национальных стандартов в области управления рисками информационной безопасности, обеспечения защиты информации и операционной надежности (киберустойчивости) в организациях КФС
	Разрабатывать предложения по организации необходимого и достаточного ресурсного (кадрового и финансового) обеспечения процессов системы управления рисками информационной безопасности в организациях КФС
	Осуществлять выбор организационных и технических мер защиты информации и обеспечения операционной надежности (киберустойчивости) в организациях КФС
	Осуществлять выбор технологических мер ащиты информации, обрабатываемой в рамках технологических операций при выполнении бизнес-процессов и технологических процессов в организациях КФС
	Осуществлять планирование деятельности организаций КФС по реагированию на риски информационной безопасности
	Планировать процессы подтверждения реализации функций безопасности и контроля (наличия) уязвимостей объектов информатизации прикладного уровня в организациях КФС
Необходимые знания	Законодательство Российской Федерации, нормативные правовые акты, национальные, межгосударственные и международные стандарты в области защиты информации, обеспечения информационной безопасности, управления рисками информационной безопасности в организациях КФС
	Руководящие и методические документы уполномоченных федеральных органов исполнительной власти, нормативные акты Банка России в области защиты информации, обеспечения информационной безопасности, управления рисками информационной безопасности в организациях КФС
	Основные подходы к реагированию на риски информационной безопасности в организациях КФС
	Принципы построения и совершенствования систем защиты информации и обеспечения операционной надежности (киберустойчивости) в организациях КФС
	Подходы к реализации технологических мер защиты информации, обрабатываемой в рамках технологических операций при выполнении бизнес-процессов и технологических процессов в организациях КФС
	Подходы к выявлению инцидентов, реагированию на инциденты информационной безопасности и восстановлению функционирования

	бизнес-процессов и технологических процессов организаций КФС и объектов информатизации
	Специфика платежных процессов в организациях КФС
	Принципы построения архитектуры информационной безопасности
	Базовый состав организационных и технических мер защиты информации и обеспечения операционной надежности (киберустойчивости) в организациях КФС
	Классификация инцидентов защиты информации организаций КФС
	Принципы и порядок подтверждения реализации функций безопасности и отсутствия уязвимостей в используемых объектах информатизации прикладного уровня
	Принципы целеполагания, виды и методы организационного планирования
Особые условия допуска к работе	-
Другие характеристики	-

3.3.3. Трудовая функция

Наименование	Определение угроз информационной безопасности в организациях КФС	Код	C/01.7	Уровень квалификации	7

Происхождение обобщенной трудовой функции	Оригинал X	Заимствовано из оригинала	Код оригинала	Регистрационный номер профессионального стандарта
				1593

Трудовые действия	Подготовка предложений по организации и выполнению действий по определению и анализу угроз информационной безопасности, характерных для организаций КФС
	Определение возможных сценариев реализации угроз информационной безопасности в организациях КФС
	Организация процесса выявления возможных уязвимостей критичной архитектуры в организациях КФС
	Формирование модели внутреннего и внешнего нарушителя безопасности информации в организациях КФС
	Разработка модели угроз информационной безопасности в организациях КФС
	Оценка возможности эксплуатации уязвимостей в отношении критичной архитектуры в организациях КФС
Необходимые умения	Анализировать и применять методологическую базу, требования законодательства Российской Федерации, нормативных актов Банка России, международных и национальных стандартов в области защиты информации, обеспечения информационной безопасности, управления рисками информационной безопасности в организациях КФС
	Разрабатывать модели угроз информационной безопасности в организациях КФС
	Разрабатывать проекты внутренних документов (локальные акты,

	организационно-распорядительные документы и методические материалы) организации КФС по вопросам моделирования угроз информационной безопасности
	Оценивать возможности эксплуатации уязвимостей в отношении критичной архитектуры в организациях КФС
	Оценивать потенциал нарушителя безопасности информации в организациях КФС
	Осуществлять сбор и анализ информации об актуальных угрозах информационной безопасности и уязвимостях в организациях КФС
Необходимые знания	Законодательство Российской Федерации, нормативные правовые акты, национальные, межгосударственные и международные стандарты в области защиты информации, обеспечения информационной безопасности, управления рисками информационной безопасности в организациях КФС, а также в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации
	Руководящие и методические документы уполномоченных федеральных органов исполнительной власти, нормативные акты Банка России в области защиты информации, обеспечения информационной безопасности, управления рисками информационной безопасности в организациях КФС, а также в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации
	Модели безопасности компьютерных систем в организациях КФС
	Модели нарушителя, методика построения модели нарушителя и методы классификации нарушителей
	Принципы обеспечения информационной безопасности, управления рисками информационной безопасности в организациях КФС
	Специфика платежных процессов в организациях КФС
	Принципы построения архитектуры информационной безопасности в организациях КФС
	Основные источники рисков информационной безопасности в рамках бизнес-процессов и технологических процессов организаций КФС
	Основные угрозы информационной безопасности и уязвимости в организациях КФС
	Основы функционирования автоматизированных систем и приложений
Особые условия допуска к работе	-
Другие характеристики	-

3.3.4. Трудовая функция

Наименование	Выявление, идентификация и оценка рисков информационной безопасности в организациях КФС	Код	C/02.7	Уровень квалификации	7

Происхождение обобщенной трудовой функции	Оригинал	X	Заимствовано из оригинала		1593
				Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Идентификация рисков информационной безопасности в организациях КФС
	Проведение оценки рисков информационной безопасности по каждому виду деятельности организаций КФС
	Организация и выполнение оценки вероятности возникновения инцидентов информационной безопасности в организациях КФС
	Проведение оценки степени тяжести последствий инцидентов информационной безопасности в организациях КФС
	Проведение анализа базы данных о событиях рисков информационной безопасности в организациях КФС
	Организация и проведение самооценки (в частности, путем анкетирования персонала) рисков информационной безопасности в организациях КФС
	Организация и проведение интервьюирования работников организаций КФС в целях идентификации рисков информационной безопасности
Необходимые умения	Анализировать и применять методологическую базу, требования законодательства Российской Федерации, нормативных актов Банка России, международных и национальных стандартов в области управления рисками информационной безопасности, обеспечения защиты информации и операционной надежности (киберустойчивости) в организациях КФС
	Применять методологию проведения оценки рисков информационной безопасности по каждому виду деятельности организаций КФС
	Разрабатывать проекты внутренних документов (локальные акты, организационно-распорядительные документы и методические материалы) организации КФС по выявлению, идентификации и оценке рисков информационной безопасности в организациях КФС
	Разрабатывать предложения по совершенствованию внутренних документов организаций КФС, определяющих методологию оценки рисков информационной безопасности в организациях КФС
	Разрабатывать предложения по совершенствованию внутренних документов организаций КФС, определяющих методологию проведения самооценки (в частности, путем анкетирования персонала) рисков информационной безопасности в организациях КФС, и проведения интервьюирования работников организаций КФС в целях идентификации рисков информационной безопасности
Необходимые знания	Законодательство Российской Федерации, нормативные правовые акты, национальные, межгосударственные и международные стандарты в области защиты информации, обеспечения информационной безопасности, управления рисками информационной безопасности в организациях КФС
	Руководящие и методические документы уполномоченных федеральных органов исполнительной власти, нормативные акты Банка России в области защиты информации, обеспечения информационной безопасности, управления рисками информационной безопасности в организациях КФС
	Основы проведения анализа баз данных в организациях КФС
	Специфика платежных процессов в организациях КФС
	Принципы построения архитектуры информационной безопасности в организациях КФС

	Принципы управления рисками информационной безопасности, обеспечения информационной безопасности в организациях КФС
	Основные источники рисков информационной безопасности в рамках бизнес-процессов и технологических процессов организаций КФС
	Подходы к оценке и лучшие практики оценки рисков информационной безопасности в организациях КФС
	Подходы к проведению и лучшие практики проведения самооценки (в частности, путем анкетирования персонала) рисков информационной безопасности в организациях КФС, и проведения интервьюирования работников организаций КФС в целях идентификации рисков информационной безопасности
	Классификация событий рисков информационной безопасности организаций КФС
Особые условия допуска к работе	-
Другие характеристики	-

3.3.5. Трудовая функция

Наименование	Мониторинг рисков информационной безопасности и контроль показателей уровня рисков информационной безопасности в организациях КФС	Код	C/05.7	Уровень квалификации	7

Происхождение обобщенной трудовой функции	Оригинал	X	Заимствовано из оригинала		1593
				Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Определение набора ключевых индикаторов рисков информационной безопасности в организациях КФС и требований к ним
	Документирование ключевых индикаторов рисков информационной безопасности в организациях КФС
	Организация и осуществление деятельности по расчету значений ключевых индикаторов рисков информационной безопасности и контрольных показателей уровня рисков информационной безопасности в организациях КФС
	Проведение оценки потенциала превышения сигнальных и контрольных значений показателей уровня рисков информационной безопасности в организациях КФС
	Определение порядка реагирования на превышение пороговых значений ключевых индикаторов рисков информационной безопасности в организациях КФС
	Организация и контроль выполнения мероприятий по переоценке рисков информационной безопасности в организациях КФС
	Формирование внутренней отчетности о фактических значениях показателей уровня рисков информационной безопасности в организациях КФС

Необходимые умения	Анализировать и применять методологическую базу, требования законодательства Российской Федерации, нормативных актов Банка России, международных и национальных стандартов в области управления рисками информационной безопасности, обеспечения защиты информации и операционной надежности (киберустойчивости) в организациях КФС
	Разрабатывать проекты внутренних документов (локальные акты, организационно-распорядительные документы и методические материалы) организации КФС, определяющих набор ключевых индикаторов рисков и требования к ним
	Применять методологию оценки потенциала превышения сигнальных и контрольных значений показателей уровня рисков информационной безопасности в организациях КФС
	Производить измерения ключевых индикаторов рисков информационной безопасности в организациях КФС
	Обосновывать пороговые значения ключевых индикаторов рисков информационной безопасности в организациях КФС
	Организовывать сбор информации для расчета ключевых индикаторов рисков и контрольных показателей уровня рисков информационной безопасности в организациях КФС
Необходимые знания	Законодательство Российской Федерации, нормативные правовые акты, национальные, межгосударственные и международные стандарты в области защиты информации, обеспечения информационной безопасности, управления рисками информационной безопасности в организациях КФС
	Руководящие и методические документы уполномоченных федеральных органов исполнительной власти, нормативные акты Банка России в области защиты информации, обеспечения информационной безопасности, управления рисками информационной безопасности в организациях КФС
	Принципы управления рисками информационной безопасности, обеспечения информационной безопасности в организациях КФС
	Способы расчета ключевых индикаторов рисков информационной безопасности в организациях КФС, в том числе с использованием средств информатизации
	Принципы построения архитектуры информационной безопасности
	Специфика платежных процессов в организациях КФС
	Подходы к определению состава контрольных показателей уровня рисков информационной безопасности в организациях КФС
	Подходы к организации составления отчетности в рамках управления рисками информационной безопасности
Особые условия допуска к работе	-
Другие характеристики	-

3.3.6. Трудовая функция

Наименование	Обеспечение информационной безопасности значимых объектов критической информационной	Код	C/06.7	Уровень квалификации	7

инфраструктуры в организациях КФС		

Происхождение обобщенной трудовой функции	Оригинал	X	Заимствовано из оригинала		1593
				Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Разработка, согласование и применение внутренних документов организации КФС, определяющих методологию обеспечения защиты информации значимых объектов критической информационной инфраструктуры в организациях КФС
	Организация работ по категорированию объектов критической информационной инфраструктуры Российской Федерации на этапах:
	Совершенствование методологии обеспечения защиты информации значимых объектов критической информационной инфраструктуры в организациях КФС
	Анализ результатов (валидация) применения методологии обеспечения защиты информации значимых объектов критической информационной инфраструктуры и защиты персональных данных в организациях КФС
	Разработка программ консультирования и повышения осведомленности работников организации КФС по вопросам защиты информации значимых объектов критической информационной инфраструктуры и защиты персональных данных в организациях КФС
	Методологическое сопровождение реализации программ контроля и аудита защиты информации значимых объектов критической информационной инфраструктуры в организациях КФС
	Определение форматов представления отчетности в рамках обеспечения защиты информации значимых объектов критической информационной инфраструктуры в организациях КФС
Необходимые умения	Анализировать нормативные правовые акты, национальные и международные документы, регламентирующие разработку методологии обеспечения защиты информации в организациях КФС
	Анализировать и применять методологическую базу, требования законодательства Российской Федерации и федеральных органов исполнительной власти Российской Федерации, уполномоченных в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, защиты персональных данных
	Анализировать и применять методологическую базу, требования законодательства Российской Федерации, нормативных актов Банка России, международных и национальных стандартов в области управления рисками информационной безопасности и обеспечения защиты информации
	Анализировать и обосновывать методологию обеспечения защиты информации в организациях КФС
	Разрабатывать проекты внутренних документов (локальные акты, организационно-распорядительные документы и методические материалы) организации КФС, определяющие методологию обеспечения защиты информации в организациях КФС

	Разрабатывать программы консультирования и повышения осведомленности работников организации КФС по вопросам защиты информации значимых объектов критической информационной инфраструктуры и защиты персональных данных в организациях КФС
	Подготавливать информационно-аналитические материалы по вопросам обеспечения защиты информации в организациях КФС
Необходимые знания	Законодательство Российской Федерации, нормативные правовые акты, национальные, межгосударственные и международные стандарты в области защиты информации, защиты персональных данных, управления рисками информационной безопасности, обеспечения информационной безопасности в организациях КФС, обеспечения безопасности критической информационной инфраструктуры Российской Федерации; правила категорирования объектов критической информационной инфраструктуры Российской Федерации
	Руководящие и методические документы уполномоченных федеральных органов исполнительной власти, нормативные акты Банка России в области защиты информации, защиты персональных данных, обеспечения информационной безопасности, управления рисками информационной безопасности в организациях КФС, обеспечения безопасности критической информационной инфраструктуры Российской Федерации
	Принципы разработки и совершенствования методологии обеспечения защиты информации в организациях КФС
	Принципы построения систем обеспечения защиты информации и защиты персональных данных в организациях КФС
	Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных в организациях КФС
	Методология разработки программ консультирования и повышения осведомленности работников организации КФС по вопросам защиты информации и защиты объектов критической информационной инфраструктуры в организациях КФС
	Специфика платежных процессов в организациях КФС
	Принципы организации внутренней отчетности организации КФС в рамках обеспечения защиты информации в организациях КФС
Особые условия допуска к работе	-
Другие характеристики	-

3.3.7. Трудовая функция

Наименование	Организация защиты информации, в том числе защиты персональных данных, в организациях КФС	Код	C/07.7	Уровень квалификации	7

Происхождение обобщенной трудовой функции	Оригинал	X	Заимствовано из оригинала		1593
				Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Разработка модели угроз безопасности информации, в том числе безопасности персональных данных, в организациях КФС
	Разработка организационно-распорядительных документов по защите информации, в том числе по защите персональных данных, в организациях КФС
	Организация выполнения организационных и технических мер по защите информации, в том числе по защите персональных данных, в организациях КФС
	Разработка архитектуры и конфигурации системы защиты персональных данных в организациях КФС
	Разработка систем мониторинга распространения персональных данных в организациях КФС
	Разработка методик оценки эффективности мер по обеспечению безопасности персональных данных в информационных системах в организациях КФС
	Организация контроля выполнения организационных и технических мер по защите информации, в том числе по защите персональных данных, в организациях КФС
	Проведение обучения персонала по выполнению организационных и технических мер по защите информации, в том числе по защите персональных данных в организациях КФС
Необходимые умения	Разрабатывать модели угроз безопасности информации, в том числе безопасности персональных данных, в организациях КФС
	Разрабатывать организационно-распорядительные документы по защите информации, в том числе по защите персональных данных, в организациях КФС
	Планировать и организовывать выполнение организационных и технических мер по защите информации, в том числе по защите персональных данных, в организациях КФС
	Планировать и организовывать контроль выполнения организационных технических мер по защите информации, в том числе по защите персональных данных, в организациях КФС
	Реализовывать правила разграничения доступа персонала к объектам доступа в организациях КФС
	Проводить обучение персонала по выполнению организационных и технических мер по защите информации, в том числе по защите персональных данных, в организациях КФС
	Разрабатывать архитектуру и конфигурацию системы защиты персональных данных в организациях КФС
	Разрабатывать системы мониторинга распространения персональных данных в организациях КФС
	Разрабатывать методики оценки эффективности мер по обеспечению безопасности персональных данных в информационных системах в организациях КФС
	Разрабатывать и реализовывать методы обезличивания персональных данных в информационных системах в организациях КФС
Необходимые знания	Законодательство Российской Федерации, нормативные правовые акты, национальные, межгосударственные и международные стандарты в

	области защиты информации и защиты персональных данных
	Руководящие и методические документы уполномоченных федеральных органов исполнительной власти, нормативные акты Банка России в области защиты информации и защиты персональных данных
	Современные информационные технологии (операционные системы, базы данных, вычислительные сети)
	Угрозы безопасности информации, в том числе безопасности персональных данных, в автоматизированных системах в организациях КФС
	Методы и средства защиты информации в автоматизированных системах в организациях КФС
	Порядок организации защиты и основные требования к защите информации, в том числе к защите персональных данных, в организациях КФС
	Состав и содержание организационно-распорядительных документов по защите информации, в том числе по защите персональных данных, в автоматизированных системах в организациях КФС
	Основы обеспечения безопасности объектов информатизации прикладного уровня в организациях КФС
	Порядок организации технического обслуживания систем и средств защиты информации в организациях КФС
	Основы методики обучения, повышения осведомленности и консультирования работников организации КФС по вопросам защиты информации, в том числе защиты персональных данных
	Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных в организациях КФС
	Принципы и условия обработки персональных данных в организациях КФС
	Методы и средства контроля выполнения организационных и технических мер по защите информации, в том числе по защите персональных данных, в организациях КФС
Особые условия допуска к работе	-
Другие характеристики	-

3.3.8. Трудовая функция

Наименование	Обеспечение операционной надежности (киберустойчивости) в организациях КФС	Код	С/08.7	Уровень квалификации	7

Происхождение обобщенной трудовой функции	Оригинал	X	Заимствовано из оригинала		1593
				Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Реализация организационных и технических мер защиты информации и

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

работе	
Другие характеристики	-

3.4. Обобщенная трудовая функция «Методологическое обеспечение процессов информационной безопасности в организациях КФС»

Наименование	Методологическое обеспечение процессов информационной безопасности 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, профессий	Главный специалист по информационной безопасности Ведущий специалист по информационной безопасности Руководитель структурного подразделения

Требования к образованию и обучению	Высшее профильное образование – магистратура или специалитет в области информационной безопасности или Высшее образование (непрофильное) – магистратура или специалитет и дополнительное профессиональное образование (профессиональная переподготовка) в области информационной безопасности в организациях КФС
Требования к опыту практической работы	Не менее двух лет в области информационной безопасности в организациях КФС
Особые условия допуска к работе	-
Другие характеристики	-

Дополнительные характеристики

Наименование документа	Код	Наименование базовой группы, должности (профессии) или специальности
ОКЗ	2529.	Специалисты по базам данных и сетям, не входящие в другие группы
ЕТКС или ЕКС		Главный специалист по технической защите информации
ОКПДТР	20911	Главный специалист по защите информации
ОКСО 2016	1.01.04.02	Прикладная математика и информатика
	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
	2.09.04.01	Информатика и вычислительная техника
	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
	2.11.04.02	Инфокоммуникационные технологии и системы связи
	5.38.04.01	Экономика
	5.38.04.05	Бизнес-информатика
	5.40.04.01	Юриспруденция
	2.10.05.01	Компьютерная безопасность
	2.10.05.02	Информационная безопасность телекоммуникационных систем
	2.10.05.03	Информационная безопасность автоматизированных систем
	2.10.05.04	Информационно-аналитические системы безопасности
	2.10.05.05	Безопасность информационных технологий в правоохранительной сфере
	2.10.05.06	Криптография
	2.10.05.07	Противодействие техническим разведкам
	5.38.05.01	Экономическая безопасность
	5.40.05.01	Правовое обеспечение национальной безопасности

3.4.1. Трудовая функция

Наименование	Разработка политики в области обеспечения информационной безопасности, по вопросам управления рисками информационной безопасности, обеспечения операционной надежности (киберустойчивости) и защиты информации в организациях КФС	Код	D/01.7	Уровень квалификации	7

Происхождение обобщенной трудовой функции	Оригинал	X	Заимствовано из оригинала		1593
				Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Разработка, согласование и организация утверждения политики в области обеспечения информационной безопасности, по вопросам управления рисками информационной безопасности, обеспечения операционной надежности (киберустойчивости) и защиты информации в организациях КФС
	Совершенствование политики в области обеспечения информационной безопасности, по вопросам управления рисками информационной безопасности, обеспечения операционной надежности (киберустойчивости) и защиты информации в организациях КФС
	Разработка предложений по распределению ролей и ответственности за управление рисками информационной безопасности, обеспечение защиты информации и операционной надежности (киберустойчивости) в

	вовлеченных подразделениях организаций КФС
	Разработка предложений по определению зон компетенции совета директоров (наблюдательного совета) и исполнительного органа организаций КФС
	Разработка предложений по определению состава контрольных показателей уровня рисков информационной безопасности в организациях КФС, а также его контрольных и сигнальных значений
Необходимые умения	Анализировать и обосновывать политику организаций КФС в области обеспечения информационной безопасности, по вопросам управления рисками информационной безопасности, обеспечения операционной надежности (киберустойчивости) и защиты информации
	Анализировать и применять методологическую базу, требования законодательства Российской Федерации, нормативных актов Банка России, международных и национальных стандартов в области управления рисками информационной безопасности, обеспечения защиты информации и операционной надежности (киберустойчивости) в организациях КФС
	Разрабатывать предложения по изменению и совершенствованию политики управления рисками информационной безопасности в организациях КФС
	Разрабатывать проекты внутренних документов (локальные акты, организационно-распорядительные документы и методические материалы) организации КФС, устанавливающих цели и принципы, а также определяющих методологию и правила управления рисками информационной безопасности в организациях КФС
	Разрабатывать предложения по развитию корпоративной культуры (этики), устанавливающей значимость вопросов управления рисками информационной безопасности, обеспечения защиты информации, операционной надежности (киберустойчивости) в организациях КФС
Необходимые знания	Законодательство Российской Федерации, нормативные правовые акты, национальные, межгосударственные и международные стандарты в области защиты информации, в области управления рисками информационной безопасности, обеспечения информационной безопасности и операционной надежности (киберустойчивости) в организациях КФС
	Руководящие и методические документы уполномоченных федеральных органов исполнительной власти, нормативные акты Банка России в области защиты информации, в области управления рисками информационной безопасности, обеспечения информационной безопасности и операционной надежности (киберустойчивости) в организациях КФС
	Принципы и методы распределения ролей и ответственности за управление рисками информационной безопасности, обеспечение защиты информации и операционной надежности (киберустойчивости) в организациях КФС
	Принципы целеполагания, виды и методы организационного планирования
	Принципы построения и совершенствования систем управления рисками информационной безопасности, обеспечения информационной безопасности и операционной надежности (киберустойчивости) в

	организациях КФС
	Специфика платежных процессов в организациях КФС
	Принципы разработки политики в области обеспечения информационной безопасности по вопросам управления рисками информационной безопасности, обеспечения операционной надежности (киберустойчивости) и защиты информации в организациях КФС
	Подходы к определению состава контрольных показателей уровня рисков информационной безопасности в организации КФС
Особые условия допуска к работе	-
Другие характеристики	-

3.4.2. Трудовая функция

Наименование	Разработка методологии обеспечения защиты информации и операционной надежности (киберустойчивости) в организациях КФС	Код	D/02.7	Уровень квалификации	7

Происхождение обобщенной трудовой функции	Оригинал	X	Заимствовано из оригинала		1593
				Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Разработка, согласование и применение внутренних документов организации КФС, определяющих методологию обеспечения защиты информации и операционной надежности (киберустойчивости) в организациях КФС
	Совершенствование методологии обеспечения защиты информации и операционной надежности (киберустойчивости) в организациях КФС
	Анализ результатов (валидация) применения методологии обеспечения защиты информации и операционной надежности (киберустойчивости) в организациях КФС
	Разработка программ консультирования и повышения осведомленности работников организации КФС по вопросам защиты информации и обеспечения операционной надежности (киберустойчивости) в организациях КФС
	Подготовка предложений по базовому составу организационных и технических мер по защите информации и обеспечению операционной надежности (киберустойчивости) в организациях КФС
	Методологическое сопровождение реализации программ контроля и аудита защиты информации и обеспечения операционной надежности (киберустойчивости) в организациях КФС
	Определение форматов представления отчетности в рамках обеспечения защиты информации и операционной надежности (киберустойчивости) в организациях КФС
Необходимые умения	Анализировать нормативные правовые акты, национальные и международные документы, регламентирующие разработку методологии

	обеспечения защиты информации и операционной надежности (киберустойчивости) в организациях КФС
	Анализировать и применять методологическую базу, требования законодательства Российской Федерации, нормативных актов Банка России, международных и национальных стандартов в области управления рисками информационной безопасности, обеспечения защиты информации и операционной надежности (киберустойчивости) в организациях КФС
	Анализировать и обосновывать методологию обеспечения защиты информации и операционной надежности (киберустойчивости) в организациях КФС
	Разрабатывать проекты внутренних документов (локальные акты, организационно-распорядительные документы и методические материалы) организации КФС, определяющие методологию обеспечения защиты информации и операционной надежности (киберустойчивости) в организациях КФС
	Подготавливать информационно-аналитические материалы по вопросам обеспечения защиты информации и операционной надежности (киберустойчивости) в организациях КФС
Необходимые знания	Законодательство Российской Федерации, нормативные правовые акты, национальные, межгосударственные и международные стандарты в области защиты информации, в области управления рисками информационной безопасности, обеспечения информационной безопасности и операционной надежности (киберустойчивости) в организациях КФС
	Руководящие и методические документы уполномоченных федеральных органов исполнительной власти, нормативные акты Банка России в области защиты информации, в области управления рисками информационной безопасности, обеспечения информационной безопасности и операционной надежности (киберустойчивости) в организациях КФС
	Принципы разработки и совершенствования методологии обеспечения защиты информации и операционной надежности (киберустойчивости) в организациях КФС
	Принципы построения систем обеспечения защиты информации и операционной надежности (киберустойчивости) в организациях КФС
	Базовый состав организационных и технических мер по защите информации и обеспечению операционной надежности (киберустойчивости) в организациях КФС
	Методология разработки программ консультирования и повышения осведомленности работников организации КФС по вопросам защиты информации и обеспечения операционной надежности (киберустойчивости) в организациях КФС
	Специфика платежных процессов в организациях КФС
	Принципы организации внутренней отчетности организации КФС в рамках обеспечения защиты информации и операционной надежности (киберустойчивости) в организациях КФС
Особые условия допуска к работе	-
Другие характеристики	-

3.4.3. Трудовая функция

Наименование	Разработка методологии управления рисками информационной безопасности в организациях КФС	Код	D/03.7	Уровень квалификации	7

Происхождение обобщенной трудовой функции	Оригинал	X	Заимствовано из оригинала		1593
				Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Разработка, согласование и применение внутренних документов, определяющих методологию управления рисками информационной безопасности в организациях КФС
	Совершенствование методологии управления рисками информационной безопасности в организациях КФС
	Анализ результатов (валидация) применения методологии управления рисками информационной безопасности в организациях КФС
	Разработка программ консультирования и повышения осведомленности по вопросам противодействия реализации информационных угроз работников в организациях КФС
	Разработка программ повышения осведомленности по вопросам противодействия реализации информационных угроз в отношении потребителей финансовых услуг в организациях КФС
	Определение форматов представления отчетности в рамках управления рисками информационной безопасности в организациях КФС
	Методологическое сопровождение оценки эффективности функционирования системы управления рисками информационной безопасности в организациях КФС
	Разработка методологии оценки рисков информационной безопасности в организациях КФС
	Разработка методологии определения потерь от событий информационной безопасности в организациях КФС
Необходимые умения	Анализировать и применять методологическую базу, требования законодательства Российской Федерации, нормативных актов Банка России, международных и национальных стандартов в области управления рисками информационной безопасности, обеспечения защиты информации и операционной надежности (киберустойчивости) в организациях КФС
	Анализировать и обосновывать методологию управления рисками информационной безопасности в организациях КФС
	Разрабатывать проекты внутренних документов (локальные акты, организационно-распорядительные документы и методические материалы) организации КФС, определяющие методологию управления рисками информационной безопасности в организациях КФС
	Подготавливать информационно-аналитические материалы по вопросам управления рисками информационной безопасности в организациях КФС
Необходимые знания	Законодательство Российской Федерации, нормативные правовые акты,

	национальные, межгосударственные и международные стандарты в области защиты информации, в области управления рисками информационной безопасности, обеспечения информационной безопасности и операционной надежности (киберустойчивости) в организациях КФС
	Руководящие и методические документы уполномоченных федеральных органов исполнительной власти, нормативные акты Банка России в области защиты информации, в области управления рисками информационной безопасности, обеспечения информационной безопасности и операционной надежности (киберустойчивости) в организациях КФС
	Принципы разработки и совершенствования методологии управления рисками информационной безопасности в организациях КФС
	Принципы построения систем управления рисками информационной безопасности в организациях КФС
	Специфика платежных процессов в организациях КФС
	Методология разработки программ консультирования и повышения осведомленности по вопросам противодействия реализации информационных угроз в отношении потребителей финансовых услуг в организациях КФС
	Принципы организации внутренней отчетности организации КФС в рамках управления рисками информационной безопасности в организациях КФС
Особые условия допуска к работе	-
Другие характеристики	-

3.4.4. Трудовая функция

Наименование	Разработка методологии выявления инцидентов информационной безопасности, реагирования на них и восстановления после их реализации в организациях КФС	Код	D/04.7	Уровень квалификации	7

Происхождение обобщенной трудовой функции	Оригинал	X	Заимствовано из оригинала		1593
				Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Разработка, согласование внутренних документов, определяющих порядок выявления инцидентов информационной безопасности в организациях КФС
	Разработка, согласование внутренних документов, определяющих порядок реагирования на инциденты информационной безопасности в организациях КФС, в том числе порядок информирования о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации компьютерных атак, проведенных в отношении значимых

	объектов критической информационной инфраструктуры в банковской сфере и иных сферах финансового рынка
	Разработка, согласование внутренних документов, определяющих порядок восстановления функционирования бизнес-процессов и технологических процессов и объектов информатизации после реализации инцидентов информационной безопасности в организациях КФС, в том числе порядок информирования о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры
	Разработка, согласование внутренних документов, определяющих порядок организации взаимодействия в рамках реагирования на инциденты информационной безопасности в организациях КФС, в том числе порядок информирования о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры
	Разработка, согласование внутренних документов, определяющих порядок проведения анализа причин и последствий реализации инцидентов информационной безопасности в организациях КФС, в том числе порядок информирования о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры
	Определение показателей эффективности реагирования и восстановления после реализации инцидентов информационной безопасности в организациях КФС
	Разработка, согласование внутренних документов, определяющих методологию оценки потенциала влияния (критичности) инцидента информационной безопасности в организациях КФС
Необходимые умения	Анализировать и применять методологическую базу, требования законодательства Российской Федерации, нормативных актов Банка России, международных и национальных стандартов в области управления рисками информационной безопасности, обеспечения защиты информации и операционной надежности (киберустойчивости) в организациях КФС, а также о порядке информирования о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры
	Обеспечивать методологическое сопровождение деятельности организации КФС в области выявления инцидентов, реагирования на них и восстановления после реализации инцидентов информационной безопасности в организациях КФС
	Разрабатывать проекты внутренних документов (локальные акты, организационно-распорядительные документы и методические материалы) организации КФС по выявлению инцидентов информационной безопасности, реагирования на них и восстановления после их реализации в организациях КФС, в том числе информирования о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации компьютерных атак, проведенных в отношении значимых

	объектов критической информационной инфраструктуры
	Подготавливать информационно-аналитические материалы по вопросам выявления инцидентов, реагирования на них и восстановления после реализации инцидентов информационной безопасности в организациях КФС
Необходимые знания	Законодательство Российской Федерации, нормативные правовые акты, национальные, межгосударственные и международные стандарты в области защиты информации, в области управления рисками информационной безопасности, а также о порядке информирования о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры
	Руководящие и методические документы уполномоченных федеральных органов исполнительной власти, нормативные акты Банка России в области защиты информации, в области управления рисками информационной безопасности, а также о порядке информирования о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры
	Основы организации процессов выявления инцидентов информационной безопасности, реагирования на них и восстановления после их реализации в организациях КФС, в том числе порядок информирования о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры
	Ключевые показатели эффективности деятельности организации КФС по выявлению инцидентов информационной безопасности, реагированию на них и восстановлению после их реализации в организациях КФС
	Форматы обмена информацией об инцидентах информационной безопасности в организациях КФС, в том числе порядок информирования о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры
	Принципы и методы распределения ролей и ответственности в рамках реагирования на инциденты информационной безопасности и восстановления после их реализации в организациях КФС, в том числе порядок информирования о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры
	Специфика платежных процессов в организациях КФС
	Основные подходы и лучшие практики по сбору технических данных (свидетельств) в рамках выявления инцидентов информационной безопасности, реагирования на инциденты и восстановления после их реализации в организациях КФС
Особые условия допуска к работе	-
Другие характеристики	-

3.5. Обобщенная трудовая функция «Контроль обеспечения информационной безопасности и обеспечение операционной надежности (киберустойчивости) в организациях КФС»

Наименование	Контроль обеспечения информационной безопасности и обеспечение операционной надежности (киберустойчивости) 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, профессий	Специалист по информационной безопасности Ведущий специалист по защите информации

Требования к образованию и обучению	Высшее образование – специалитет или магистратура в области информационной безопасности или Высшее образование (непрофильное) – магистратура или специалитет и дополнительное профессиональное образование (профессиональная переподготовка) в области информационной безопасности
Требования к опыту практической работы	Не менее одного года в области информационной безопасности в организациях КФС
Особые условия допуска к работе	Наличие допуска к государственной тайне (при необходимости)
Другие характеристики	-

Дополнительные характеристики

Наименование документа	Код	Наименование базовой группы, должности (профессии) или специальности
ОКЗ	2529.	Специалисты по базам данных и сетям, не входящие в другие группы
ЕТКС или ЕКС		Администратор по обеспечению безопасности информации
		Инженер по защите информации
		Инженер-программист по технической защите информации
		Специалист по обеспечению безопасности информации в ключевых системах информационной инфраструктуры
ОКПДТР	22567	Инженер по защите информации
	26579	Специалист по защите информации
ОКСО 2016	1.01.04.02	Прикладная математика и информатика
	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

	2.09.04.01	Информатика и вычислительная техника
	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
	2.10.05.01	Компьютерная безопасность
	2.10.05.02	Информационная безопасность телекоммуникационных систем
	2.10.05.03	Информационная безопасность автоматизированных систем
	2.10.05.04	Информационно-аналитические системы безопасности
	2.10.05.05	Безопасность информационных технологий в правоохранительной сфере
	2.10.05.06	Криптография
	2.10.05.07	Противодействие техническим разведкам

3.5.1. Трудовая функция

Наименование	Проведение контрольных проверок работоспособности и оценка эффективности применяемых программно-аппаратных средств защиты информации в организациях КФС	Код	E/01.7	Уровень квалификации	7

Происхождение обобщенной трудовой функции	Оригинал	X	Заимствовано из оригинала		1593
				Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Проверка работоспособности применяемых программно-аппаратных средств защиты информации с использованием штатных средств и методик в организациях КФС
	Оценка эффективности применяемых программно-аппаратных средств защиты информации с использованием штатных средств и методик в организациях КФС
	Определение уровня защищенности программно-аппаратных средств защиты информации в организациях КФС
Необходимые умения	Анализировать и применять методологическую базу, требования законодательства Российской Федерации, нормативных актов Банка России, международных и национальных стандартов в области защиты информации в организациях КФС
	Определять параметры функционирования программно-аппаратных средств защиты информации в организациях КФС
	Разрабатывать методики оценки защищенности программно-аппаратных средств защиты информации в организациях КФС
	Оценивать эффективность защиты информации в организациях КФС
	Применять разработанные методики оценки защищенности программно-

	аппаратных средств защиты информации в организациях КФС
	Анализировать программно-аппаратные средства защиты с целью определения уровня обеспечиваемой ими защищенности в организациях КФС
Необходимые знания	Законодательство Российской Федерации, нормативные правовые акты, национальные, межгосударственные и международные стандарты в области защиты информации в организациях КФС
	Руководящие и методические документы уполномоченных федеральных органов исполнительной власти, нормативные акты Банка России в области защиты информации в организациях КФС
	Принципы построения компьютерных систем и сетей в организациях КФС
	Методы и методики оценки безопасности программно-аппаратных средств защиты информации
	Принципы построения программно-аппаратных средств защиты информации в организациях КФС
	Принципы построения подсистем защиты информации в компьютерных системах в организациях КФС
	Методы и средства проверки работоспособности программно-аппаратных средств защиты информации
	Методы оценки эффективности политики безопасности, реализованной в программно-аппаратных средствах защиты информации в организациях КФС
	Методы и средства оценки эффективности программных реализаций алгоритмов защиты информации
	Способы анализа применяемых методов и средств защиты информации на предмет соответствия политике безопасности в организациях КФС
Особые условия допуска к работе	-
Другие характеристики	-

3.5.2. Трудовая функция

Наименование	Контроль процессов защиты информации и обеспечения операционной надежности (киберустойчивости) в организациях КФС	Код	E/02.7	Уровень квалификации	7

Происхождение обобщенной трудовой функции	Оригинал	X	Заимствовано из оригинала		1593
				Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Контроль реализации процессов применения технологических мер защиты инофрмации, обрабатываемой в рамках технологических операций, при выполнении бизнес-процессов и технологических процессов в организациях КФС

	Контроль реализации функций безопасности и контроля (наличия) уязвимостей объектов информатизации прикладного уровня в организациях КФС
	Контроль реализации организационных и технологических мер защиты информации и обеспечения операционной надежности (киберустойчивости) в организациях КФС
	Контроль реализации процессов обеспечения защиты информации и операционной надежности (киберустойчивости) на этапах жизненного цикла объектов информатизации прикладного уровня в организациях КФС
	Реализация программ контроля и аудита защиты информации и обеспечения операционной надежности (киберустойчивости) в организациях КФС
	Представление отчетности в рамках обеспечения защиты информации и операционной надежности (киберустойчивости) в организациях КФС
	Организация и проведение сценарного анализа и тестирования готовности организаций КФС противостоять реализации угроз информационной безопасности
Необходимые умения	Анализировать и применять методологическую базу, требования законодательства Российской Федерации, нормативных актов Банка России, международных и национальных стандартов в области управления рисками информационной безопасности, обеспечения защиты информации и операционной надежности (киберустойчивости) в организациях КФС
	Разрабатывать предложения по совершенствованию методологии обеспечения защиты информации и операционной надежности (киберустойчивости) в организациях КФС
	Применять технологические меры для обеспечения защиты информации, обрабатываемой в рамках технологических операций, при выполнении бизнес-процессов и технологических процессов в организациях КФС
	Применять организационные и технические меры по защите информации и обеспечению операционной надежности (киберустойчивости) в организациях КФС
	Анализировать техническую документацию на объекты информатизации в организациях КФС
Необходимые знания	Законодательство Российской Федерации, нормативные правовые акты, национальные, межгосударственные и международные стандарты в области защиты информации, в области реализации и контроля процессов защиты информации и обеспечения операционной надежности (киберустойчивости) в организациях КФС
	Руководящие и методические документы уполномоченных федеральных органов исполнительной власти, нормативные акты Банка России в области защиты информации, в области реализации и контроля процессов защиты информации и обеспечения операционной надежности (киберустойчивости) в организациях КФС
	Принципы построения компьютерных систем и сетей в организациях КФС
	Базовый состав организационных и технических мер защиты информации и обеспечения операционной надежности (киберустойчивости) в организациях КФС

	Подходы к сегментации вычислительных сетей
	Основы обеспечения безопасности объектов информатизации прикладного уровня
	Специфика платежных процессов в организациях КФС
Особые условия допуска к работе	-
Другие характеристики	-

3.5.3. Трудовая функция

Наименование	Реализация программ повышения осведомленности организаций КФС по вопросам защиты информации и обеспечения операционной надежности (киберустойчивости) в организациях КФС	Код	E/03.7	Уровень квалификации	7

Происхождение обобщенной трудовой функции	Оригинал X	Заимствовано из оригинала		1593
			Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Организация консультирования и инструктирования работников организаций КФС в соответствии с программами повышения осведомленности
	Организация мероприятий по повышению осведомленности членов совета директоров (наблюдательного совета) и исполнительного органа по вопросам организации и контроля управления рисками информационной безопасности, защиты информации и обеспечения операционной надежности (киберустойчивости) в организациях КФС
	Проведение контрольных мероприятий по результатам реализации программ консультирования и повышения осведомленности работников организаций КФС по вопросам противодействия реализации угроз информационной безопасности
	Организация и проведение консультирования для работников, входящих в группы повышенного риска, по вопросам выявления и противодействия реализации угроз информационной безопасности в организациях КФС
	Подготовка предложений по совершенствованию программ по повышению осведомленности в организациях КФС
	Доведение до клиентов – потребителей финансовых услуг информации, способствующей уменьшению негативного влияния рисков информационной безопасности в организациях КФС
Необходимые умения	Анализировать и применять методологическую базу, требования законодательства Российской Федерации, нормативных актов Банка России, международных и национальных стандартов в области управления рисками информационной безопасности, обеспечения защиты информации и операционной надежности (киберустойчивости) в организациях КФС

	Организовывать и проводить мероприятия по консультированию и повышению осведомленности в организациях КФС
	Определять формы, методы и средства объективной оценки процесса и результатов повышения осведомленности и консультирования
	Разрабатывать (осваивать) и внедрять современные технологии и формировать способы повышения мотивации работников в организациях КФС
	Применять технологические меры для обеспечения защиты информации, обрабатываемой в рамках технологических операций, при выполнении бизнес-процессов и технологических процессов в организациях КФС
	Применять организационные и технические меры защиты информации и обеспечению операционной надежности (киберустойчивости) в организациях КФС
Необходимые знания	Законодательство Российской Федерации, нормативные правовые акты, национальные, межгосударственные и международные стандарты в области защиты информации, в области реализации и контроля процессов защиты информации и обеспечения операционной надежности (киберустойчивости) в организациях КФС
	Руководящие и методические документы уполномоченных федеральных органов исполнительной власти, нормативные акты Банка России в области защиты информации, в области реализации и контроля процессов защиты информации и обеспечения операционной надежности (киберустойчивости) в организациях КФС
	Специфика платежных процессов в организациях КФС
	Принципы обеспечения защиты информации и операционной надежности (киберустойчивости) в организациях КФС
	Основы методики повышения осведомленности и консультирования, пути достижения результатов и способы оценки результатов повышения осведомленности и консультирования
	Процессы, методы средств побуждения работников организации к активному освоению материала
	Основы обеспечения безопасности объектов информатизации прикладного уровня
Особые условия допуска к работе	-
Другие характеристики	-

3.6. Обобщенная трудовая функция «Организация процессов обеспечения информационной безопасности в организациях КФС»

Наименование	Организация процессов обеспечения информационной безопасности в организациях КФС	Код	F	Уровень квалификации	8

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

Возможные наименования должностей, профессий	Руководитель департамента Руководитель управления

Требования к образованию и обучению	Высшее профильное образование – магистратура или специалитет в области информационной безопасности или Высшее образование (непрофильное) – магистратура или специалитет и дополнительное профессиональное образование (профессиональная переподготовка) в области информационной безопасности
Требования к опыту практической работы	Не менее пяти лет в области информационной безопасности в организациях КФС, из них не менее двух лет на руководящих должностях
Особые условия допуска к работе	Наличие допуска к государственной тайне (при необходимости)
Другие характеристики	-

Дополнительные характеристики

Наименование документа	Код	Наименование базовой группы, должности (профессии) или специальности
ОКЗ	1330.	Руководители служб и подразделений в сфере информационно-коммуникационных технологий
ЕТКС или ЕКС		Начальник отдела (лаборатории, сектора) по технической защите информации
ОКПДТР	46115	Руководитель аналитической группы подразделения по комплексной защите информации
ОКСО 2016	1.01.04.02	Прикладная математика и информатика
	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
	2.09.04.01	Информатика и вычислительная техника
	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
	2.11.04.02	Инфокоммуникационные технологии и системы связи
	5.38.04.01	Экономика
	5.38.04.05	Бизнес-информатика
	5.40.04.01	Юриспруденция
	2.10.05.01	Компьютерная безопасность
	2.10.05.02	Информационная безопасность телекоммуникационных систем
	2.10.05.03	Информационная безопасность автоматизированных систем
	2.10.05.04	Информационно-аналитические системы безопасности
	2.10.05.05	Безопасность информационных технологий в правоохранительной сфере

	2.10.05.06	Криптография
	2.10.05.07	Противодействие техническим разведкам
	5.38.05.01	Экономическая безопасность
	5.40.05.01	Правовое обеспечение национальной безопасности

3.6.1. Трудовая функция

Наименование	Организация управления рисками информационной безопасности на высшем управленческом уровне в организациях КФС	Код	F/01.8	Уровень квалификации	8

Происхождение обобщенной трудовой функции	Оригинал	X	Заимствовано из оригинала		Код оригинала	1593 Регистрационный номер профессионального стандарта

Трудовые действия	Организация и контроль выполнения работ по разработке предложений по содержанию политики в области обеспечения информационной безопасности, по вопросам управления рисками информационной безопасности, обеспечения операционной надежности (киберустойчивости) в организациях КФС
	Подготовка предложений по определению стратегических целей и задач организации КФС по вопросам управления рисками информационной безопасности, обеспечения операционной надежности (киберустойчивости) в организациях КФС
	Определение правил и требований к реализации процессов выявления, идентификации и оценки рисков информационной безопасности в организациях КФС
	Разработка предложений по мероприятиям, направленным на уменьшение негативного влияния рисков информационной безопасности на функционирование бизнес-процессов и технологических процессов в организациях КФС
	Планирование работы, установление функций, обязанностей курируемых подразделений и определение контрольных показателей для подразделений, задействованных в реализации мер по управлению рисками информационной безопасности в организациях КФС
	Организация процесса и контроль обеспечения осведомленности об актуальных информационных угрозах в организациях КФС
	Подготовка информационно-аналитических материалов по вопросам управления рисками информационной безопасности в организациях КФС
	Организация деятельности по реализации процедур управления рисками внутреннего нарушителя в отношении работников в организациях КФС
	Оценка ресурсного (кадрового и финансового) обеспечения для планирования, реализации, контроля и совершенствования процессов системы управления рисками информационной безопасности в организациях КФС
	Организация работы по формированию отчетности в рамках управления

	рисками информационной безопасности в организациях КФС
	Организация работы по выявлению, регистрации инцидентов информационной безопасности, реагированию на инциденты и восстановлению после их реализации в организациях КФС
Необходимые умения	Анализировать и применять методологическую базу, требования законодательства Российской Федерации, нормативных актов Банка России, международных и национальных стандартов в области управления рисками информационной безопасности, обеспечения защиты информации и операционной надежности (киберустойчивости) в организациях КФС
	Оценивать эффективность управления рисками информационной безопасности, в том числе эффективность выявления событий рисков информационной безопасности в организациях КФС
	Вносить предложения по изменению и совершенствованию процедуры управления рисками информационной безопасности в организациях КФС
	Разрабатывать проекты внутренних документов (локальные акты, организационно-распорядительные документы и методические материалы) организации КФС, устанавливающих цели и принципы, а также определяющих методологию и правила управления рисками информационной безопасности в организациях КФС
	Анализировать и обосновывать общую стратегию организаций КФС по вопросам управления рисками информационной безопасности в соответствии с законодательством Российской Федерации, на основе современных методов и лучших практик
	Реализовывать политику в области обеспечения информационной безопасности, по вопросам управления рисками информационной безопасности, обеспечения операционной надежности (киберустойчивости) в организациях КФС
	Устанавливать требования к процессу мониторинга рисков информационной безопасности и контролю фактических значений уровня рисков информационной безопасности в организациях КФС
Необходимые знания	Законодательство Российской Федерации, нормативные правовые акты, национальные, межгосударственные и международные стандарты в области защиты информации, в области управления рисками информационной безопасности, обеспечения информационной безопасности и операционной надежности (киберустойчивости) в организациях КФС
	Руководящие и методические документы уполномоченных федеральных органов исполнительной власти, нормативные акты Банка России в области защиты информации, в области управления рисками информационной безопасности, обеспечения информационной безопасности и операционной надежности (киберустойчивости) в организациях КФС
	Принципы управления подразделениями, задействованными в реализации мер по управлению рисками информационной безопасности в организациях КФС
	Принципы управления рисками информационной безопасности, обеспечения защиты информации в организациях КФС
	Принципы целеполагания, виды и методы организационного планирования

	Нормы профессиональной этики
	Подходы к определению ключевых показателей эффективности, в том числе показателей эффективности деятельности организаций КФС
	Принципы построения архитектуры информационной безопасности
	Специфика платежных процессов в организациях КФС
	Ключевые показатели эффективности деятельности по управлению рисками информационной безопасности, обеспечению защиты информации и операционной надежности (киберустойчивости) в организациях КФС
Особые условия допуска к работе	-
Другие характеристики	-

3.6.2. Трудовая функция

Наименование	Организация обеспечения защиты информации и операционной надежности (киберустойчивости) на высшем управленческом уровне в организациях КФС	Код	F/02.8	Уровень квалификации	8

Происхождение обобщенной трудовой функции	Оригинал	X	Заимствовано из оригинала		Код оригинала	1593 Регистрационный номер профессионального стандарта

Трудовые действия	Подготовка предложений по определению стратегических целей и задач организации КФС по вопросам обеспечения защиты информации и операционной надежности (киберустойчивости) в организациях КФС
	Подготовка информационно-аналитических материалов по вопросам защиты информации и обеспечения операционной надежности (киберустойчивости) в организациях КФС
	Организация работы по формированию отчетности о защите информации и обеспечении операционной надежности (кибербезопасности) в организации КФС
	Организация работы по выявлению, регистрации инцидентов, связанных с реализацией информационных угроз, реагированию на инциденты и восстановлению после их реализации в организациях КФС
	Организация разработки и контроль реализации организационных и технических мер по обеспечению защиты информации и операционной надежности (киберустойчивости) в организациях КФС
	Планирование работы, установление функций, обязанностей курируемых подразделений и определение контрольных показателей для подразделений, задействованных в реализации мер по обеспечению информационной безопасности и операционной надежности (киберустойчивости) в организациях КФС
	Разработка проектов внутренних документов организации КФС, устанавливающих цели и принципы, определяющих методологию и

	правила обеспечения информационной безопасности и операционной надежности (киберустойчивости) в организациях КФС
	Организация и осуществление деятельности по сценарному анализу и тестированию готовности подразделений организаций КФС противостоять реализации информационных угроз
	Организация работы по выявлению, приоритизации, классификации и устранению уязвимостей в критичной архитектуре, контролю полноты и своевременности устранения выявленных уязвимостей в организациях КФС
	Оценка ресурсного (кадрового и финансового) обеспечения для планирования, реализации, контроля и совершенствования процессов системы управления операционной надежностью (киберустойчивостью) в организациях КФС
	Организация работы по идентификации критичной архитектуры в организациях КФС
	Организация работы по выполнению процессов защиты информации в организациях КФС
Необходимые умения	Анализировать и обосновывать общую стратегию организаций КФС по вопросам защиты информации и операционной надежности (киберустойчивости) в соответствии с законодательством Российской Федерации, на основе современных методов и лучших практик
	Анализировать и применять методологическую базу, требования законодательства Российской Федерации, нормативных актов Банка России, международных и национальных стандартов в области управления рисками информационной безопасности, обеспечения защиты информации и операционной надежности (киберустойчивости) в организациях КФС
	Применять риск-ориентированный подход к выбору объектов информатизации, подвергаемых тестированию на проникновение, в организациях КФС
	Оценивать эффективность деятельности по выполнению работ, связанных с обеспечением защиты информации и операционной надежности (киберустойчивости) в организациях КФС
	Устанавливать, применять и контролировать внутренние стандарты конфигурирования объектов информатизации (стандарты конфигурирования) в организациях КФС
	Организовывать и осуществлять деятельность по тестированию готовности организаций КФС противостоять реализации информационных угроз
	Разрабатывать процессы обеспечения защиты информации и операционной надежности (киберустойчивости) и организовывать внедрение процессов обеспечения защиты информации и операционной надежности (киберустойчивости) в организациях КФС
	Разрабатывать сценарии, включающие значительные финансовые потери, в рамках проведения стресс-тестирования для определения потенциала влияния и уровня рисков для бизнес-модели организаций КФС
Необходимые знания	Законодательство Российской Федерации, нормативные правовые акты, национальные, межгосударственные и международные стандарты в области защиты информации, в области управления рисками информационной безопасности, обеспечения информационной

	безопасности и операционной надежности (киберустойчивости) в организациях КФС
	Руководящие и методические документы уполномоченных федеральных органов исполнительной власти, нормативные акты Банка России в области защиты информации, в области управления рисками информационной безопасности, обеспечения информационной безопасности и операционной надежности (киберустойчивости) в организациях КФС
	Ключевые показатели эффективности деятельности по обеспечению защиты информации и операционной надежности (киберустойчивости) в организациях КФС
	Принципы управления рисками информационной безопасности, обеспечения защиты информации и операционной надежности (киберустойчивости) в организациях КФС
	Принципы целеполагания, виды и методы организационного планирования
	Подходы к определению ключевых показателей эффективности
	Принципы построения архитектуры информационной безопасности
	Специфика платежных процессов в организациях КФС
	Подходы к идентификации и включению элементов критичной архитектуры в область применения процесса обеспечения операционной надежности в организациях КФС
	Состав и содержание, а также порядок применения организационных и технических мер обеспечения защиты информации и операционной надежности (киберустойчивости) в организациях КФС
	Нормы профессиональной этики
Особые условия допуска к работе	-
Другие характеристики	-

3.6.3. Трудовая функция

Наименование	Контроль процедур управления рисками информационной безопасности и обеспечения защиты информации и операционной надежности (киберустойчивости) на высшем управленческом уровне в организациях КФС	Код	F/03.8	Уровень квалификации	8

Происхождение обобщенной трудовой функции	Оригинал	X	Заимствовано из оригинала		1593
				Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Организация работ по установлению и реализации программ контроля и аудита обеспечения защиты информации и операционной надежности (киберустойчивости) в организациях КФС

	Обеспечение сопровождения при проведении оценки эффективности системы управления рисками информационной безопасности в организациях КФС
	Организация работы по мониторингу рисков информационной безопасности в организациях КФС
	Определение правил контроля и требований к контролю процедур управления рисками информационной безопасности, обеспечению защиты информации и операционной надежности (киберустойчивости) в организациях КФС
	Организация и координация работ по реализации стратегии управления рисками информационной безопасности и обеспечения защиты информации и операционной надежности (киберустойчивости) в организациях КФС
Необходимые умения	Вносить предложения по изменению и совершенствованию системы обеспечения защиты информации и операционной надежности (киберустойчивости) по результатам реализации программ контроля и аудита обеспечения защиты информации и операционной надежности (киберустойчивости) в организациях КФС
	Анализировать и применять методологическую базу, требования законодательства Российской Федерации, нормативных актов Банка России, международных и национальных стандартов в области управления рисками информационной безопасности, обеспечения защиты информации и операционной надежности (киберустойчивости) в организациях КФС
	Вносить предложения по изменению и совершенствованию системы управления рисками информационной безопасности по результатам оценки эффективности системы управления рисками информационной безопасности в организациях КФС
	Разрабатывать стратегии управления рисками информационной безопасности и обеспечения защиты информации и операционной надежности (киберустойчивости) в организациях КФС
	Применять требования нормативных правовых актов и методологических документов по управлению рисками информационной безопасности и обеспечению операционной надежности (киберустойчивости) в организациях КФС
	Определять подходы к организации мониторинга рисков информационной безопасности в организациях КФС
Необходимые знания	Законодательство Российской Федерации, нормативные правовые акты, национальные, межгосударственные и международные стандарты в области защиты информации, в области управления рисками информационной безопасности, обеспечения информационной безопасности и операционной надежности (киберустойчивости) в организациях КФС
	Руководящие и методические документы уполномоченных федеральных органов исполнительной власти, нормативные акты Банка России в области защиты информации, в области управления рисками информационной безопасности, обеспечения информационной безопасности и операционной надежности (киберустойчивости) в организациях КФС
	Принципы целеполагания, виды и методы организационного

	планирования
	Подходы к организации отчетности в рамках управления рисками информационной безопасности, обеспечения защиты информации и операционной надежности (киберустойчивости) в организациях КФС
	Подходы к определению ключевых показателей эффективности
	Принципы построения архитектуры информационной безопасности
	Специфика платежных процессов в организациях КФС
	Принципы управления рисками информационной безопасности, обеспечения защиты информации и операционной надежности (киберустойчивости) в организациях КФС
	Ключевые показатели эффективности деятельности по управлению рисками информационной безопасности, в области обеспечения защиты информации и операционной надежности (киберустойчивости) в организациях КФС
Особые условия допуска к работе	-
Другие характеристики	-

3.6.4. Трудовая функция

Наименование	Совершенствование системы управления рисками информационной безопасности, обеспечение защиты информации и операционной надежности (киберустойчивости) на высшем управленческом уровне в организациях КФС	Код	F/04.8	Уровень квалификации	8

Происхождение обобщенной трудовой функции				
Оригинал	X	Заимствовано из оригинала		1593
			Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Анализ необходимости совершенствования системы управления рисками информационной безопасности, обеспечения защиты информации и операционной надежности (киберустойчивости) в организациях КФС
	Планирование внедрения тактических и стратегических улучшений системы управления рисками информационной безопасности, обеспечения информационной безопасности и операционной надежности (киберустойчивости) в организациях КФС
	Организация деятельности по реализации тактических и стратегических улучшений системы управления рисками информационной безопасности, обеспечения информационной безопасности и операционной надежности (киберустойчивости) в организациях КФС
	Обеспечение участия курируемых подразделений информационной безопасности в контроле деятельности, связанной с реализацией тактических и стратегических улучшений системы управления рисками информационной безопасности, обеспечением защиты информации и

	операционной надежности (киберустойчивости) в организациях КФС
Необходимые умения	Устанавливать и поддерживать деловые контакты, связи, отношения с сотрудниками и заинтересованными сторонами по вопросам управления рисками информационной безопасности, обеспечения информационной безопасности и операционной надежности (киберустойчивости) в организациях КФС
	Анализировать и применять методологическую базу, требования законодательства Российской Федерации, нормативных актов Банка России, международных и национальных стандартов в области управления рисками информационной безопасности, обеспечения защиты информации и операционной надежности (киберустойчивости) в организациях КФС
	Анализировать и обосновывать общую стратегию организации КФС по вопросам управления рисками информационной безопасности, обеспечения информационной безопасности и операционной надежности (киберустойчивости) в организациях КФС
	Вносить предложения по изменению и совершенствованию стратегии управления рисками информационной безопасности, обеспечения информационной безопасности и операционной надежности (киберустойчивости) в организациях КФС
	Определять источники информации для проведения анализа необходимости совершенствования системы управления рисками информационной безопасности, обеспечения защиты информации и операционной надежности (киберустойчивости) в организациях КФС
Необходимые знания	Законодательство Российской Федерации, нормативные правовые акты, национальные, межгосударственные и международные стандарты в области защиты информации, в области управления рисками информационной безопасности, обеспечения информационной безопасности и операционной надежности (киберустойчивости) в организациях КФС
	Руководящие и методические документы уполномоченных федеральных органов исполнительной власти, нормативные акты Банка России в области защиты информации, в области управления рисками информационной безопасности, обеспечения информационной безопасности и операционной надежности (киберустойчивости) в организациях КФС
	Принципы целеполагания, виды и методы организационного планирования
	Ключевые показатели эффективности деятельности по управлению рисками информационной безопасности, обеспечению защиты информации и операционной надежности (киберустойчивости) в организациях КФС
	Принципы управления рисками информационной безопасности, обеспечения защиты информации и операционной надежности (киберустойчивости) в организациях КФС
	Подходы к определению ключевых показателей эффективности
	Основные подходы к проектному управлению
	Принципы построения архитектуры информационной безопасности
	Специфика платежных процессов в организациях КФС
	Нормы профессиональной этики

Особые условия допуска к работе	-
Другие характеристики	-

IV. Сведения об организациях – разработчиках профессионального стандарта

4.1. Ответственная организация-разработчик

Департамент информационной безопасности Банка России , город Москва Директор департамента Уваров Вадим Александрович

4.2. Наименования организаций-разработчиков

1	ФУМО в системе высшего образования по УГСНП 10.00.00 «Информационная безопасность», город Москва