ПРОТОКОЛ № 5 - 2021

заседания Совета по профессиональным квалификациям в области ИТ

от 25 июня 2021 г. **Совещание в формате онлайн**

ПРИСУТСТВОВАЛИ:

Сопредседатели СПК-ИТ:
Комлев Н.В., АПКИТ
Нуралиев Б.Г., Фирма «1С»

Члены СПК-ИТ и их официальные представители:
Аншина М.Л., СОДИТ
Белов Е.Б., УМО ИБ
Лашин Р.Л., АРПП «Отечественный софт»
Лебедев С.А., Фирма «1С»
Мальцева С.В., Высшая школа экономики
Мельникова О.И., Университет «Дубна»
Мельников Ю.В., ПАО «Ростелеком»
Нежурина М.И., ИИБС НИТУ «МИСиС»
Осадчий А.В., ГБПОУ «Московский центр развития профессионального образования»
Пролетарский Андрей Викторович, ФУМО в сфере высшего образования по УГСН 09.00.00
Филиппович А.Ю., Московский политехнический университет

Приглашённые участники:

Члены Комиссии по информационной безопасности (КИБ) СПК-ИТ:
Лось В.П., заместитель председателя КИБ, АЗИ
Зарубин А.В., АО «ИнфоВотч»
Шапошников В.А., АЗИ
Чернышев В.И., Минобороны России
Хайров И.Е., АНО ДПО АИС
Харитонов С.В., АО «ИнфоВотч»

Представитель ВНИИ Труда Минтруда России:
Зайцева О.М., Центр развития профессиональных квалификаций ВНИИ Труда Минтруда России

Ассоциация предприятий компьютерных и информационных технологий
Тел. +7 495 739-8928; e-mail: info@apkit.ru; www.apkit.ru; 101000 Москва, а/я 626

Представители Центрального Банка Российской Федерации (Банка России):
Уваров В.А., директор Департамента информационной безопасности Банка России
Сычёв А.М., первый заместитель директора Департамента информационной безопасности Банка России
Выборнов А.О., заместитель директора Департамента информационной безопасности Банка России, начальник Управления методологии и стандартизации информационной безопасности и киберустойчивости Департамента информационной безопасности Банка России
Раудина О.Н., Заведующий сектором киберграмотности и образовательных инициатив Управления методологии и стандартизации информационной безопасности и киберустойчивости Департамента информационной безопасности Банка России
Зубарева О.С., заместитель начальника Управления методологии и стандартизации информационной безопасности и киберустойчивости Департамента информационной безопасности Банка России

Ответственный секретарь СПК-ИТ:
Кузора И.В., Фирма «1С»

Менеджер проектов СПК-ИТ по оценке квалификаций:
Позднеева О.Б.

Форма проведения совещания: видео-конференц-связь Zoom.
Кворум достигнут.
Вел заседание: сопредседатель СПК-ИТ Комлев Н.В.

Ассоциация предприятий компьютерных и информационных технологий
Тел. +7 495 739-8928; e-mail: info@apkit.ru; www.apkit.ru; 101000 Москва, а/я 626

1. **Текущее состояние национальной системы независимой оценки квалификаций.**

Докладчик: Н.В. Комлев

Решение:

1.1. Принять к сведению доклад Н.В. Комлева.

2. **О согласовании заключения СПК-ИТ на основе заключения Комиссии по информационной безопасности (КИБ) СПК-ИТ по итогам экспертизы профессионального стандарта «Специалист по информационной безопасности в кредитно-финансовой сфере».**

Докладчики: Е.Б. Белов, Н.В. Комлев

Решение:

2.1. Принять к сведению доклады Н.В. Комлева, Е.Б. Белова и представителей Центрального Банка Российской Федерации (Банка России): А.М. Сычева, А.О. Выборнова, О.С. Зубаревой, О.Н. Раудиной.

2.2. Проект профессионального стандарта «Специалист по управлению информационной безопасностью в организациях кредитно-финансовой сферы» (ПС) направить на доработку для повторного рассмотрения, и после устранения замечаний рекомендовать к утверждению. Совет зафиксировал следующие принципиальные положения, необходимые для доработки:

2.2.1. Скорректировать название ПС в целях более адекватного соответствия названия ПС его содержанию (функциональной карты вида профессиональной деятельности). Например (один из вариантов), назвать его «Специалист по управлению информационной безопасностью в организациях кредитно-финансовой сферы».

2.2.2. Исправить ПС с учетом представленных в отзыве КИБ (Приложение 1) методических замечаний. Так, например, в проекте ПС применяется терминология и понятийный аппарат в соответствии с нормативными документами Банка России, отсутствуют ссылки на нормативные акты ФСТЭК России. В последующем ПС будет применяться в учебном процессе в образовательных организациях, что повлечет разное толкование однородных процессов и событий.

2.2.3. Добавить в ПС ОТФ по организационным вопросам обеспечения безопасности критической информационной инфраструктуры в банковской сфере. В соответствии с Федеральным законом от 26.07.2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» банковская сфера и иные сферы финансового рынка подпадают под

Ассоциация предприятий компьютерных и информационных технологий
Тел. +7 495 739-8928; e-mail: info@apkit.ru; www.apkit.ru; 101000 Москва, а/я 626

действие этого закона, реализация которого определена приказами ФСТЭК России.

2.2.4. Отнести ПС к ведению СПК-ИТ. В случае же отнесения ПС к иным СПК в других областях экономической деятельности (например, СПК финансового рынка), из названия ПС необходимо изъять термин «информационная безопасность».

2.3. Проинформировать Минцифры России и Минтруд России о позиции СПК-ИТ в отношении ПС «Специалист по информационной безопасности в кредитно-финансовой сфере».

2.4. Обратиться в Минцифры России с предложением согласовать эксперта (экспертов) от Минцифры России, компетентного, в том числе, в области инфобезопасности для обсуждения данного вопроса.

3. <u>Об актуализации профессиональных стандартов в области ИТ в 2021 году с учётом цифровых технологий.</u>

Докладчики: И.В. Кузора, С.А. Лебедев, А.Ю. Филиппович

<u>Решение:</u>

3.1. Принять к сведению доклады И.В. Кузоры, С.А. Лебедева, А.Ю. Филипповича об организации работ по актуализации ПС «Программист», «Руководитель разработки программного обеспечения», «Специалист по информационным ресурсам», «Технический писатель».

3.2. Одобрить предложенную последовательность актуализации профессиональных стандартов.

3.3. В состав рабочей группы (РГ) по актуализации ПС «Технический писатель» ввести сопредседателя СПК-ИТ Н.В. Комлева и одобрить первичные составы рабочих групп (Приложение 2). Членам СПК-ИТ направить предложения по дополнению составов РГ (до 02.07.2021).

4. <u>О перспективах развития процедур независимой оценки квалификаций в области ИТ по квалификациям, требующим среднего профессионального образования.</u>

Докладчик: И.В. Кузора, О.Б. Позднеева

<u>Решение:</u>

4.1. Принять к сведению доклад И.В. Кузоры.

4.2. В связи с появлением перспективы превращения независимой оценки квалификации (НОК) в обязательную процедуру для выпускников СПО, отметить необходимость приоритетной разработки квалификаций и оценочных средств (ОС) для нижних (3, 4, 5) квалификационных

Ассоциация предприятий компьютерных и информационных технологий
Тел. +7 495 739-8928; e-mail: info@apkit.ru; www.apkit.ru; 101000 Москва, а/я 626

уровней профессиональных стандартов (не менее 50% от общего количества таких квалификаций).

4.3. Рабочей группе СПК-ИТ по независимой оценке квалификаций на основании представленной на заседании информации о состоянии разработки примеров и комплектов оценочных средств определить наиболее востребованные квалификации, по которым разработку ОС следует вести в приоритетном порядке.

4.4. Предложить разработчикам оценочных средств провести доработку одобренных СПК-ИТ ранее примеров оценочных средств (ПОС) до полноценных комплектов оценочных средств. При доработке ПОС учитывать то, что некоторые ПС были актуализированы уже после разработки ПОС, или находятся в состоянии актуализации в настоящий момент.

5. О новых перечнях в системе высшего образования в области ИБ и ИКТ.

Докладчики: Е.Б. Белов, А.В. Пролетарский

Решение:

5.1. Принять к сведению доклады Е.Б. Белова, А.В. Пролетарского. Поручить Е.Б. Белову, А.В. Пролетарскому и Ю.В. Мельникову подготовить проект совместного обращения СПК-ИТ и СПК в области телекоммуникаций, почтовой связи и радиотехники в Минобрнауки России по вопросу об УГС в области связи (ответственный: Ю.В. Мельников).

Ассоциация предприятий компьютерных и информационных технологий
Тел. +7 495 739-8928; e-mail: info@apkit.ru; www.apkit.ru; 101000 Москва, а/я 626

Приложение 1
к протоколу № 5- 2021
от 25.06.2021г.

Заключение

комиссии по информационной безопасности Совета по профессиональным квалификациям в области информационных технологий (далее - СПК-ИТ) на проект профессионального стандарта «Специалист по информационной безопасности в кредитно-финансовой сфере», представленного Банком России

Проект профессионального стандарта «Специалист по информационной безопасности в кредитно-финансовой сфере», пояснительная записка и справка к нему рассмотрены в комиссии по информационной безопасности СПК-ИТ (далее - КИБ СПК-ИТ).

Проект профессионального стандарта разработан в соответствии с нормативными правовыми и методическими документами Минтруда России.
Замечания и предложения по проекту профессионального стандарта (ПС).

1. Название профессионального стандарта, вид профессиональной деятельности, ее цель и перечень обобщенных трудовых функций (ОТФ) не в полной мере соотнесены между собой. Если исходить из наименования представленных ОТФ, то целями вида профессиональной деятельности являются:

- управление рисками информационной безопасности (ОТФ E);
- аналитическая деятельность в области информационной безопасности (ОТФ D);
- административно-управленческая деятельность в области информационной безопасности (ОТФ C и B);
- управление инцидентами информационной безопасности (ОТФ A).

В пояснительной записке представлены основные задачи профессиональной деятельности, где ключевыми словами являются:
управление инцидентами информационной безопасности,
контроль обеспечения информационной безопасности,
методологическое обеспечение процессов информационной безопасности,
аналитическое сопровождение деятельности,
организация процессов обеспечения информационной безопасности.

Данные цели вида профессиональной деятельности хорошо соотносятся с группой занятий 1330 «Руководители служб и подразделений в сфере информационно-коммуникационных технологий», указанной в стандарте.

Ассоциация предприятий компьютерных и информационных технологий
Тел. +7 495 739-8928; e-mail: info@apkit.ru; www.apkit.ru; 101000 Москва, а/я 626

К обеспечению информационной безопасности и построению комплексной системы обеспечения информационной безопасности относится не только управление рисками информационной безопасности и защита информации, но также комплекс организационных (создание политик безопасности, анализ требований регуляторов), технических (администрирование и наладка программного и аппаратного обеспечения информационных и автоматизированных систем кредитно-финансовой сферы) и правовых аспектов. Стандарт направлен, в основном, на управление рисками информационной безопасности, что является лишь составляющей комплексного процесса и подхода к управлению информационной безопасностью.

Концепция профессиональных стандартов в сфере информационной безопасности (утвержденных в 2016 году) с наименованием «специалист по защите информации…» предполагает включение всех ключевых этапов, связанных с жизненным циклом объекта трудовой деятельности (профессиональной сферы) по защите информации. Такой жизненный цикл как правило включает в себя совокупность следующих этапов: Разработка программных, программно-аппаратных или технических средств защиты информации; Разработка систем защиты информации автоматизированных систем; Администрирование средств защиты информации; Диагностика систем защиты информации; Обеспечение работоспособности систем защиты информации; Эксплуатация и техническое обслуживание средств защиты информации; Разработка проектных решений по защите информации; Разработка эксплуатационной документации на системы защиты информации; Обеспечение функционирования средств связи сетей связи специального назначения; Контроль защищенности от НСД; Разработка технологических процессов производства программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты; Проведение аттестации объектов информатизации; Проектирование объектов информатизации; Производство, сервисное обслуживание и ремонт средств защиты информации; Проведение контроля защищенности информации.

В проект ПС разработчики обоснованно не включили ОТФ и трудовые функции (ТФ), конкретно связанные с вышеперечисленными этапами. Объяснения разработчиков в ходе обсуждения проекта стандарта на поступившие аналогичные замечания показали, что эти объяснения сводятся только к отсылке наименования «Вида профессиональной деятельности» и его интерпретации. Более того, для должностей «Главный специалист по информационной безопасности, Ведущий специалист по информационной безопасности» 7 уровня с двумя ОТФ предусмотрены требования к образованию на уровне бакалавриата «Юриспруденция» и иных

Ассоциация предприятий компьютерных и информационных технологий
Тел. +7 495 739-8928; e-mail: info@apkit.ru; www.apkit.ru; 101000 Москва, а/я 626

юридических направлений и специальностей. В качестве требований к образованию к работникам по реализации данного ПС представлены смежные направления подготовки по отношении к укрупненной группе специальностей «Информационная безопасность». Все отчетливо подчеркивает «управленческую» направленность и сущность стандарта.

В пояснительной записке (р.2.2. Сведения о нормативно-правовых документах, регулирующих вид профессиональной деятельности, для которого разработан проект профессионального стандарта) отсутствуют нормативные правовые акты, методические и руководящие документы ФСБ России, ФСТЭК России, Госты и документы национальной системы стандартизации Российской Федерации в области защиты информации. В пояснительной записке указано, что проект профессионального стандарта разработан с учетом международных стандартов в сфере управления рисками информационной безопасности, обеспечения защиты информации и операционной надежности (киберустойчивости), а также лучших международных практик в указанных сферах.

Нет упоминания в тексте ПС и федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации и федерального органа исполнительной власти, уполномоченного в области криптографичекой защиты информации.

Отсутствие ОТФ и ТФ (соответственно трудовых действий, знаний и умений), связанных с жизненным циклом профессиональной деятельности специалиста по защите информации подтверждает и обуславливает иной вид профессиональной деятельности.

Исходя из вышеизложенного, предлагаем скорректировать наименование вида профессиональной деятельности и изложить его в редакции, например, «управление информационной безопасностью в организациях кредитно-финансовой сферы».

Замечанием принципиального характера, с учетом изложенного, является изменение наименования профессионального стандарта «Специалист по информационной безопасности в кредитно-финансовой сфере» на «Специалист по управлению информационной безопасностью в организациях кредитно-финансовой сферы».

В ином случае, с позиции выполнения «Специалистом по информационной безопасности» задач комплексной системы информационной безопасности в организациях кредитно-финансовой сферы, необходимо существенно дорабатывать указанный ПС (расширять ОТФ и

Ассоциация предприятий компьютерных и информационных технологий
Тел. +7 495 739-8928; e-mail: info@apkit.ru; www.apkit.ru; 101000 Москва, а/я 626

ТФ) в плане включения организационных, технических, криптографических, правовых мер защиты информации.

Следует отметить, что управление информационной безопасностью в организациях кредитно-финансовой сферы представляет собой сложный и многофункциональный процесс, которому, до последнего времени, не уделялось должного внимания. Это многократно отмечалось экспертами на конференциях по вопросам безопасности кредитно-финансовой сферы и разработчиками данного профессионального стандарта.

Более того, при разработке в 2015-2016 г. «линейки» ПС в перечень рассматриваемых проектов стандартов входил ПС «Специалист по управлению информационной безопасностью», а в области информационных технологий СПК-ИТ организовал разработку ПС «Менеджер по информационным технологиям», что подтверждает актуальность вопросов управления в области информационной безопасности и информационных технологий.

2. В соответствии с Федеральным законом от 26.07.2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» банковская сфера и иные сферы финансового рынка подпадают под действие этого закона. Однако в проекте ПС об этом законе почему-то ничего не говорится, даже отсутствует ссылка на данный законодательный акт.

Безопасность значимых объектов обеспечивается субъектами критической информационной инфраструктуры (КИИ) в рамках функционирования систем безопасности значимых объектов, создаваемых субъектами критической информационной инфраструктуры в соответствии со статьей 10 Федерального закона № 187-ФЗ. Приказом ФСТЭК России от 25 декабря 2017 № 239 утверждены «Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

С учетом согласованной позиции на заседании межведомственной рабочей группы Минтруда России в 2015 году по определению принципов формирования и перечня «линейки» профессиональных стандартов в области информационной безопасности, для отдельных сфер профессиональной деятельности профессиональные стандарты не планировались.

Поэтому для банковской сферы, кроме рассматриваемого стандарта организационно-управленческого профиля, больше отдельных ПС не планируется. Кроме того, в ряде ОТФ, ТФ заложены действия, связанные с

Ассоциация предприятий компьютерных и информационных технологий
Тел. +7 495 739-8928; e-mail: info@apkit.ru; www.apkit.ru; 101000 Москва, а/я 626

безопасностью объектов КИИ и вопросами компьютерных атак – ОТФ 3.1., ТФ 3.1.2., 3.1.3.

Более того, в пояснительной записке утверждается, что банковская система относится к субъектам критической информационной инфраструктуры России.

В тексте ПС понятие «обеспечение» используется 176 раз. И если при определении наименования вида профессиональной деятельности, основной цели вида профессиональной деятельности и, в какой-то мере, при формулировке ОТФ это оправданно, то при формулировке ТФ, а тем более при определении содержания трудовых действий, это понятие должно быть конкретизировано через конкретные меры и средства защиты информации в информационной инфраструктуре кредитно-финансовых организаций. Отсюда вытекают вопросы, которые должны быть отражены в тексте ПС при его доработке: принадлежность используемых в кредитно-финансовой организации информационных систем к значимым объектам КИИ в соответствии с Федеральным законом от 26.07.2017 № 187-ФЗ. В зависимости от решения этого вопроса возникает необходимость выполнения ряда мероприятий (трудовых действий), прописанных в этом законе и нормативных правовых актах ФСТЭК России (в частности, вопросы категорирования, модели угроз и др.).

В связи с этим представляется целесообразным включение в указанный профессиональный стандарт соответствующей обобщенной трудовой функции по организационным вопросам обеспечения безопасности КИИ в банковской сфере.

Замечания и предложения по тексту профессионального стандарта.

3. **3.1. Обобщенная трудовая функция.** Управление инцидентами информационной безопасности в организациях КФС. Уровень 6.

Требования к образованию и обучению	Высшее образование или Высшее образование (непрофильное) и дополнительное профессиональное образование в области информационной безопасности

Ассоциация предприятий компьютерных и информационных технологий
Тел. +7 495 739-8928; e-mail: info@apkit.ru; www.apkit.ru; 101000 Москва, а/я 626

Если указано высшее образование профильное и непрофильное, то для профильного образования предлагается указать «в области информационной безопасности». Для непрофильного образования необходимо конкретизировать вид дополнительного профессионального образования, а именно - программы профессиональной переподготовки в конкретной области (программы повышения квалификации считаем недостаточным условием), предлагаем провести редакцию.

4. Предлагаем исключить для 6 уровня непрофильное образование в гуманитарных сферах - Юриспруденция, Правовое обеспечение национальной безопасности.

Для специалистов с указанным образованием, даже с прохождением курсов дополнительного профессионального образования, весьма проблематично выполнять трудовые действия: Автоматизация процедур выявления наличия индикаторов компрометации в организации КФС; Выполнение действий по восстановлению функционирования бизнес- и технологических процессов и объектов информатизации после инцидентов информационной безопасности в соответствии с едиными правилами и процедурами после реализации таких инцидентов в организации КФС, а также умения - Осуществлять работу с техническими средствами защиты информации и системами, реализующими функции управления инцидентами защиты информации в организации КФС; Настраивать средства (агентов, интерфейсов) сбора технических данных для выявления событий информационной безопасности в организации КФС.

5. Для уровня квалификации 6 – определено высшее образование как на уровне бакалавриата, так и на уровне специалитета и магистратуры, который относится к 7 уровню квалификации.

Предлагаем для профильного образования установить уровень образования – бакалавриат.

Предлагаем провести консультации с Минтрудом России по соотношению уровня образования квалификационной рамке, утвержденной Минтрудом России.

6. 3.1.2. Трудовая функция. Реагирование на инциденты информационной безопасности в организациях КФС. **3.1.3. Трудовая функция.** Восстановление функционирования бизнес- и технологических

Ассоциация предприятий компьютерных и информационных технологий
Тел. +7 495 739-8928; e-mail: info@apkit.ru; www.apkit.ru; 101000 Москва, а/я 626

процессов и объектов информатизации после реализации инцидентов информационной безопасности в организациях КФС.

Необходимые знания - **«Базовый состав** и функциональные возможности технических средств сбора технических данных для выявления событий информационной безопасности в КФС»

В каких документах раскрыт термин «базовый состав». Предлагаем провести редакцию или данные слова удалить, состав средств у всех может быть разный, специалист должен знать все средства, которые есть в организации.

Трудовые действия – «Сбор и фиксация **технических данных (свидетельств)** в рамках восстановления функционирования бизнес- и технологических процессов и объектов информатизации после реализации инцидентов». «Анализировать **технические данные**, свидетельствующие о возникновении событий информационной безопасности в организации КФС».

По тексту термин «технические данные» упоминается часто в разной интерпретации. Термин не гостирован. Предлагаем в тексте уточнить его содержание.

7. **3.2. Обобщенная трудовая функция.** Контроль обеспечения информационной безопасности и операционной надежности (киберустойчивости) в организациях КФС. Уровень 6.

Аналогичные замечания к уровню образования см. в п. 3 по отношению к ОТФ 3.1.

8. **3.2.2. Трудовая функция.** Контроль процессов защиты информации и обеспечения операционной надежности (киберустойчивости) в организациях КФС

Необходимые знания - «**Базовый состав** организационных и технических мер защиты информации и обеспечения операционной надежности (киберустойчивости) в организации КФС».

В каких документах раскрыт термин «базовый состав». Предлагаем провести редакцию или данные слова удалить, по тексту стандарта эти слова повторяются в разной интерпретации.

9. **3.2.3. Трудовая функция.** Реализация программ обучения и повышения осведомленности организаций КФС по вопросам защиты

Ассоциация предприятий компьютерных и информационных технологий
Тел. +7 495 739-8928; e-mail: info@apkit.ru; www.apkit.ru; 101000 Москва, а/я 626

информации и обеспечения операционной надежности (киберустойчивости) в организациях КФС. Уровень 6.

Из 6 трудовых действий данной ТФ, 5 действий носят организационный – методический и педагогический профиль. В приведенных необходимых умениях присутствует только одно умение обобщающего характера. В приведенных знаниях вообще отсутствуют позиции, связанные с реализацией указанных трудовых действий.

Предлагаем провести необходимую декомпозицию трудовых действий, данной трудовой функции.

10. **3.3. Обобщенная трудовая функция** Методологическое обеспечение процессов информационной безопасности в организациях КФС. 7 уровень.

Требования к образованию и обучению	Высшее образование или Высшее образование (непрофильное) и дополнительное профессиональное образование в области информационной безопасности
Требования к опыту практической работы	Не менее двух лет в области информационной безопасности в организации КФС

Если указано высшее образование профильное и непрофильное, то для профильного образования предлагается указать «в области информационной безопасности». Для непрофильного образования необходимо конкретизировать вид дополнительного профессионального образования, а именно - программы профессиональной переподготовки в конкретной области (программы повышения квалификации считаем недостаточным условием), предлагаем провести редакцию.

Ассоциация предприятий компьютерных и информационных технологий
Тел. +7 495 739-8928; e-mail: info@apkit.ru; www.apkit.ru; 101000 Москва, а/я 626

Предлагаем исключить для 7 уровня непрофильное образование в гуманитарных сферах - Юриспруденция, Правовое обеспечение национальной безопасности.

Для специалистов с указанным образованием, даже с прохождением курсов дополнительного профессионального образования, весьма проблематично выполнять трудовые действия: Подготовка предложений по базовому составу организационных и технических мер по защите информации и обеспечению операционной надежности (киберустойчивости) организации КФС; Методологическое сопровождение реализации программ контроля и аудита защиты информации и обеспечения операционной надежности (киберустойчивости) в организации КФС; Анализ результатов (валидация) применения методологии обеспечения защиты информации и операционной надежности (киберустойчивости) в организации КФС; Анализ результатов (валидация) применения методологии управления риском информационной безопасности в организации КФС; Методологическое сопровождение оценки эффективности функционирования системы управления риском информационной безопасности в организации КФС; Разработка, согласование внутренних документов, определяющих порядок восстановления функционирования бизнес- и технологических процессов и объектов информатизации после инцидентов информационной безопасности в организации КФС.

11. Для уровня квалификации 7 (должности - Главный специалист по информационной безопасности, Ведущий специалист по информационной безопасности) – определено высшее образование на уровне бакалавриата – 6 наименований направлений подготовки, в т.ч. одно гуманитарное и 5 непрофильных. Анализ трудовых действий, умений показывает, что их квалификационный уровень сложности превосходит профессиональный уровень бакалавров, особенно непрофильных. Считаем, что это недостаточно, предлагаем уточнить. По тексту рекомендуется учесть аналогичные замечания других ОТФ.

12. **3.3.2. Трудовая функция.** Разработка методологии обеспечения защиты информации и операционной надежности (киберустойчивости) в организациях КФС. 7 уровень.

Трудовые действия и знания - «Подготовка предложений по **базовому составу** организационных и технических мер по защите информации и обеспечению операционной надежности (киберустойчивости) организации КФС. **Базовый состав** организационных и технических мер по защите информации …»

Ассоциация предприятий компьютерных и информационных технологий
Тел. +7 495 739-8928; e-mail: info@apkit.ru; www.apkit.ru; 101000 Москва, а/я 626

В каких документах раскрыт термин «базовый состав». Предлагаем провести редакцию или данные слова удалить.

13. **3.4. Обобщенная трудовая функция** - Аналитическое сопровождение деятельности по управлению рисками информационной безопасности в организациях КФС. 7 уровень.

Требования к образованию и обучению	Высшее образование или Высшее образование (непрофильное) и дополнительное профессиональное образование в области информационной безопасности

Если указано высшее образование профильное и непрофильное, то профильное образование предлагается указать «в области информационной безопасности».

Для непрофильного образования необходимо конкретизировать вид дополнительное профессиональное образование, а именно - программы профессиональной переподготовки в конкретной области.

Предлагаем исключить для 7 уровня непрофильное образование в гуманитарных сферах - Юриспруденция, Правовое обеспечение национальной безопасности.

Для специалистов с указанным образованием весьма проблематично выполнять трудовые действия: Формирование модели внутреннего и внешнего нарушителя безопасности информации в организации КФС, Оценка возможности эксплуатации уязвимостей в отношении критичной архитектуры, Организация и выполнение оценки вероятности возникновения инцидентов информационной безопасности, Определение технологических мер защиты информации, обрабатываемой в рамках технологических операций при выполнении бизнес- и технологических процессов, Определение организационных и технических мер защиты информации и обеспечение операционной надежности (киберустойчивости) в организации КФС, Установление требований к ключевым индикаторам риска информационной безопасности в организации КФС

Ассоциация предприятий компьютерных и информационных технологий
Тел. +7 495 739-8928; e-mail: info@apkit.ru; www.apkit.ru; 101000 Москва, а/я 626

14. Для уровня квалификации 7 (должности - Главный специалист по информационной безопасности, Ведущий специалист по информационной безопасности) – определено высшее образование на уровне бакалавриата – 6 наименований направлений подготовки, в т.ч. одно гуманитарное и 5 непрофильных. Считаем, что это недостаточно, предлагаем уточнить.

Для 7 уровня (в соответствии с квалификационной рамкой Минтруда России 7 уровень предполагает образование – специалитет или магистратура) нет возможности сразу после окончания образовательной организации по специальности или программе магистратуры выполнять данные две ОТФ и устраиваться на работу. Для этого необходимо пройти курсы ДПО. Нарушение правил Минтруда России (должна быть одна ОТФ, к которой готов выпускник соответствующего уровня образования без дополнительной подготовки и опыта работы).

15. **3.4.2. Трудовая функция.** Моделирование угроз безопасности информации в организациях КФС.

Трудовые действия - «Проведение анализа риска **базы событий** информационной безопасности в организации КФС».

Предлагаем слова «базы событий» удалить.

16. **3.4.2. Трудовая функция.** Для выполнения трудового действия – «Организация и проведение интервьюирования работников организации кредитно-финансовой сферы в целях идентификации риска информационной безопасности» отсутствуют умения и знания.

Предлагаем данное ТД исключить или провести декомпозицию и дополнить соответствующие умения и знания.

17. **3.4.2. Трудовая функция.** Необходимые умения – «Анализировать и применять действующую нормативно-правовую и методологическую базу, а также требования законодательства Российской Федерации и нормативных актов Банка России, международных и национальных стандартов в сфере управления риском информационной безопасности, обеспечения защиты информации и операционной надежности (киберустойчивости)».

Предлагаем слово «базу» исключить, рассмотреть следующую редакцию и применить ее по тексту стандарта.

Ассоциация предприятий компьютерных и информационных технологий
Тел. +7 495 739-8928; e-mail: info@apkit.ru; www.apkit.ru; 101000 Москва, а/я 626

«Применять законодательные акты Российской Федерации, нормативно-правовые акты, нормативно-методические и руководящие документы уполномоченных государственных органов и Банка России, документы национальной системы стандартизации Российской Федерации и государственные стандарты в области защиты информации, управления риском информационной безопасности и операционной надежности (киберустойчивости)».

18. **3.4.2. Трудовая функция.** Необходимые умения – «Разрабатывать проекты внутренних документов организации кредитно-финансовой сферы»;

Предлагаем изложить в другой редакции и применить ее по тексту стандарта: «Разрабатывать локальные акты, организационно-распорядительные документы и методические материалы по управлению рисками информационной безопасности, обеспечению защиты информации и операционной надежности (киберустойчивости) в организациях кредитно-финансовой сферы».

19. **3.4.2. Трудовая функция.** Необходимые знания – «Основы проведения анализа баз данных».

Предлагаем исключить данные требования т.к. в трудовых действиях и умениях этих позиций нет, что за анализ и каких баз данных.

20. **3.4.3. Трудовая функция** - Сбор и регистрация информации о выявленном риске информационной безопасности в организациях КФС.

Позиции трудовых действий и умений:

«Ведение базы данных и регистрация событий риска информационной безопасности КФС»

«Разрабатывать проекты внутренних документов организации КФС по ведению базы событий риска информационной безопасности организации КФС»

«Обеспечивать ведение базы данных событий риска информационной безопасности КФС»

Предлагаем провести редактирование понятий (базы данных или базы событий).

21. **3.4.4. Трудовая функция -** Разработка мероприятий, направленных на уменьшение негативного влияния риска информационной безопасности в организациях КФС. Уровень 7.

Ассоциация предприятий компьютерных и информационных технологий
Тел. +7 495 739-8928; e-mail: info@apkit.ru; www.apkit.ru; 101000 Москва, а/я 626

Умения - «Разрабатывать предложения по организации **необходимого и достаточного ресурсного (кадрового и финансового)** обеспечения процессов системы управления риском информационной безопасности в организации КФС».

Предлагаем провести редактирование.

22. **3.5. Обобщенная трудовая функция.** Организация процессов обеспечения информационной безопасности в организациях кредитно-финансовой сферы. Уровень 8.

Возможные наименования должностей, профессий	Руководитель структурного подразделения Руководитель департамента Руководитель управления

Для 8 уровня должность «Руководитель структурного подразделения», является недостаточной, это уровень стратегического управления, см. квалификационную рамку Минтруда России. Предлагаем удалить.

23. **3.5. Обобщенная трудовая функция.**

Требования к образованию и обучению	Высшее образование – магистратура или специалитет или Высшее образование (непрофильное) – магистратура или специалитет и дополнительное профессиональное образование в области информационной безопасности

Если указано высшее образование профильное и непрофильное, то профильное образование предлагается указать «в области информационной безопасности».

Для непрофильного образования необходимо конкретизировать вид дополнительное профессиональное образование, а именно - программы профессиональной переподготовки в конкретной области.

Ассоциация предприятий компьютерных и информационных технологий
Тел. +7 495 739-8928; e-mail: info@apkit.ru; www.apkit.ru; 101000 Москва, а/я 626

В разделе «Другие характеристики» для профильного предлагается указать повышение квалификации в области организации процессов обеспечения информационной безопасности в организациях кредитно-финансовой сферы. Так как это высокий уровень управления и одного опыта недостаточно.

24. **3.5.2. Трудовая функция.** Организация обеспечения защиты информации и операционной надежности (киберустойчивости) в организациях КФС. 8 уровень.

Уточнить объект трудового действия.

Трудовое действие.

«Организация и осуществление деятельности по сценарному анализу и тестированию готовности (**всей сферы или подразделений?**) кредитно-финансовой сферы противостоять реализации информационных угроз».

«Организация работ по выполнению процессов защиты информации в КФС».

Необходимо уточнить - всей сферы или подразделений (организаций) КФС.

Необходимые умения - «Анализировать и обосновывать общую стратегию организации КФС по вопросам защиты информации и операционной надежности (киберустойчивости) в соответствии с законодательством Российской Федерации, на основе современных методов и лучших практик».

В стандартах эксперты Минтруда России предлагали не использовать слова – «Лучшие», «современные», «существующие» и т.д. Предлагаем по всему тексту провести редакцию и такие слова убрать.

25. По всему тексту применяется термин «критичная архитектура» (устранению уязвимостей в критичной архитектуре; работы по идентификации критичной архитектуры; Подходы к идентификации критичной архитектуры; Оценка возможности эксплуатации уязвимостей в отношении критичной архитектуры. В тоже время имеются позиции - Принципы построения архитектуры информационной безопасности).

В каком документе ФСТЭК России, Госте указан данный термин, может целесообразней связать его с объектами КИИ. Предлагаем дать нормативное пояснение данного термина или провести редакцию по тексту стандарта.

26. В описаниях трудовых действий трудовой функции **3.4.4.**

Ассоциация предприятий компьютерных и информационных технологий
Тел. +7 495 739-8928; e-mail: info@apkit.ru; www.apkit.ru; 101000 Москва, а/я 626

«Разработка мероприятий, направленных на уменьшение негативного влияния риска информационной безопасности в организациях КФС» используется термин «технологические меры защиты информации». Такой термин в национальных стандартах в области защиты информации не определен. Можно предположить, что имелась ввиду некоторая совокупность криптографических, программных, технических и программно-технических мер защиты. Если трактовать трудовое действие «Определение технологических мер защиты информации, обрабатываемой в рамках технологических операций при выполнении бизнес- и технологических процессов» и другое трудовое действие «Реализация и совершенствование процессов применения технологических мер защиты информации, обрабатываемой в рамках технологических операций при выполнении бизнес- и технологических процессов» с этих позиций, то такая формулировка трудового действия становится слишком размытой, по сути, подменяющей собой целый ряд других профессиональных стандартов.

27. На взгляд ряда экспертов, уровень квалификации 8 избыточен. Достаточно ограничиться уровнем 7.

28. В пояснительной записке указано «ПС разработан в соответствии приказом Министерства труда и социальной защиты Российской Федерации от 12 апреля 2013 г. № 148н и с учетом Отраслевой рамки квалификаций для каждой ОТФ установлены уровни квалификаций». Вопрос- какой отрасли использовали разработчики квалификационную рамку?

Проект смотрится как внутриведомственный (узкокорпоративный, прикладной) документ для решения формальных кадровых задач. За основу брали должностные инструкции корпорации (Банк России). Но в системе банков и так все должны выполнять соответствующие инструкции, установленные Банком России в качестве регулятора.

Например, в проекте ПС указаны термины «инциденты информационной безопасности», но имеются гостированные термины «компьютерные инциденты», «инциденты защиты информации». Объяснение Банка России (приложение 3 пояснительной записки - Термины и определения приведены в соответствии с нормативными правовыми актами Российской Федерации, нормативными актами Банка России, а на практике, только в соответствии с актами Банка России (без учета ФСТЭК России). Если по такому принципу идти, то надо разработать десятки ПС в области ИБ.

В проекте ПС также указаны термины разной интерпретации:

Ассоциация предприятий компьютерных и информационных технологий
Тел. +7 495 739-8928; e-mail: info@apkit.ru; www.apkit.ru; 101000 Москва, а/я 626

- защита информации, обеспечение защиты информации, техническая защита информации, обеспечение безопасности информации, информационная безопасность;

- угрозы безопасности информации, угрозы информационной безопасности, информационные угрозы;

- нормативные правовые акты, нормативно-правовая база, нормативные акты, нормативная документация.

В Российской Федерации используются понятия законодательных актов, нормативных правовых актов основных регуляторов (ФСБ России, ФСТЭК России), национальных стандартов. Разработчики используют термины и понятия Банка России. Считаем, что необходимо провести редакцию или дать пояснения.

При разработке проекта ПС использован актуальный макет профессионального стандарта, наименование ПС и ВПД соответствуют друг другу, в формулировках ОТФ, ТФ, ТД отражена специфика ВПД.

Проект профессионального стандарта отражает современные требования к специалистам, участвующим в управлении рисками информационной безопасности, обеспечении защиты информации и операционной надежности (киберустойчивости) в организациях кредитно-финансовой сферы.

С учетом общественного обсуждения проекта стандарта экспертами банковского сообщества и позиции Банка России представляется обоснованным, что для кредитно-финансовой сферы нужен соответствующий профессиональный стандарт.

Комиссия КИБ СПК-ИТ предлагает с учетом устранения высказанных замечаний рекомендовать профессиональный стандарт к утверждению в Минтруде России.

Ассоциация предприятий компьютерных и информационных технологий
Тел. +7 495 739-8928; e-mail: info@apkit.ru; www.apkit.ru; 101000 Москва, а/я 626

1. Состав рабочей группы по актуализации ПС «Программист» и «Руководитель разраб

ФИО	Организация, долж
Лебедев Сергей Аркадьевич, руководитель рабочей группы	к.э.н., руководитель департамента программно руководитель направления компании «1С», чле
Авдошин Сергей Михайлович	профессор департамента программной инжене исполнительного комитета SEMAT Russian Ch
Тельнов Юрий Филиппович	д.э.н., профессор, заведующий кафедрой прикл информационной безопасности РЭУ им. Г.В. П
Старичков Никита Юрьевич	заместитель директора компании «1С» по рабо
Овчинников Павел Евгеньевич	старший преподаватель кафедры информацион секретарь подкомитета 3/4 технического комит
Осадчий Александр Владимирович	начальник отдела мониторинга и прогнозиро кадров ГБПОУ «Московский центр развития и Международный эксперт Worldskills Russia решения для бизнеса"
Лебедев Виктор Аркадьевич, секретарь РГ	к.э.н., зав. учебно-проектной лаборатории меж компетенций РЭУ им. Г.В. Плеханова

2. Состав рабочей группы по актуализации ПС «Технический писатель»

ФИО	Организация, должность
Острогорский Михаил Юрьевич, руководитель группы	ООО "Философт", Генеральный директор
Факторович Семён Борисович	Docimentat.io, Технический директор
Поташников Николай Михайлович	ООО "КУРС-ИТ", Руководитель проектов,
Родионова Татьяна Юрьевна	Positive Technologies, Директор по продуктовым сервисам
Каюшина Светлана Владимировна	Сбертех, Руководитель направления
Комлев Николай Васильевич	Сопредседатель СПК-ИТ, исполнительный директор АПКИТ
Лебедева Анастасия Владимировна	ООО "Русские инновационные, информационные технологии"
Лебедев Александр Александрович	ООО "Философт", Директор по проектам
Второва Анна	ООО "Акуматика" (ex-Abbyy), Head of Education Operations

3. Состав рабочей группы по актуализации ПС «Специалист по информационным ресурсам»

ФИО	Организация, должность
Филиппович Андрей Юрьевич	декан ИТ-факультета Московского Политеха, Руководитель направления по методологии и работе с органами государственной власти Департамента исследований, разработок и развития образовательных организаций АНО «Агентство развития профессионального мастерства (Ворлдскиллс Россия)»
Шукалова Екатерина Вячеславовна	директор Центра интернет-маркетинга Екатерины Шукаловой, преподаватель Московского Политеха, ВШБ, МГУ, эксперт чемпионатов WorldSkills по специальности "Интернет-маркетинг"

Ассоциация предприятий компьютерных и информационных технологий
Тел. +7 495 739-8928; e-mail: info@apkit.ru; www.apkit.ru; 101000 Москва, а/я 626

Даньшина Марина Владимировна	старший преподаватель ИТ-факультета Московского Политеха, руководитель образовательной программы "Веб-технологии"
Ефимова Валентина Михайловна	заместитель руководителя отдела по выпуску релизов в компании «Новая Афина», специалист в организации ЦП ВОГ по комплексной инновационной научно-технической программе «Слух».
Кривоносова Наталья Викторовна	преподаватель ФГБОУ ВО Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, Сертифицированный эксперт ВСР по компетенции Программные решения для бизнеса
Иванова Наталья Юрьевна	руководитель Компании IPR media, разработчик электронно-образовательных ресурсов ЭБС IPR books, Profобразование, платформы «Русский как иностранный». 89378028752, adm@iprmedia.ru
Попов Алексей Эдуардович	начальник отдела дополнительного образования и повышения квалификации, Институт сферы обслуживания и предпринимательства (филиал) ФГБУ ВО «Донской государственный технический университет» в г. Шахты Ростовской области
Владимирова Светлана Николаевна	Индивидуальный предприниматель. Основатель и научный руководитель Центра аналитики Глубинного поведенческого кода. Кандидат экономических наук (специализация "Поведенческая экономика, экономика эмоций"), магистр менеджмента, сертифицированный бизнес-тренер, автор научно-прикладных разработок и ИТ программ в области поведенческих наук

Ассоциация предприятий компьютерных и информационных технологий
Тел. +7 495 739-8928; e-mail: info@apkit.ru; www.apkit.ru; 101000 Москва, а/я 626