

**Пояснительная записка к проекту профессионального стандарта
«Специалист по защите информации
в телекоммуникационных системах и сетях»**

Оглавление

РАЗДЕЛ 1 «ОБЩАЯ ХАРАКТЕРИСТИКА ВИДА ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ, ТРУДОВЫХ ФУНКЦИЙ»	1
1.1. ИНФОРМАЦИЯ О ПЕРСПЕКТИВАХ РАЗВИТИЯ ВИДА ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ.	1
1.2. ОПИСАНИЕ ОБОБЩЕННЫХ ТРУДОВЫХ ФУНКЦИЙ, ВХОДЯЩИХ В ВИД ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ.	3
1.3. ОПИСАНИЕ СОСТАВА ТРУДОВЫХ ФУНКЦИЙ И ОБОСНОВАНИЕ ИХ ОТНЕСЕНИЯ К КОНКРЕТНЫМ УРОВНЯМ (ПОДУРОВНЯМ) КВАЛИФИКАЦИИ.	5
РАЗДЕЛ 2 «ОСНОВНЫЕ ЭТАПЫ РАЗРАБОТКИ ПРОЕКТА ПРОФЕССИОНАЛЬНОГО СТАНДАРТА»	11
2.1. ИНФОРМАЦИЯ ОБ ОРГАНИЗАЦИЯХ, НА БАЗЕ КОТОРЫХ ПРОВОДИЛИСЬ ИССЛЕДОВАНИЯ, И ОБОСНОВАНИЕ ВЫБОРА ЭТИХ ОРГАНИЗАЦИЙ	11
2.2. ОПИСАНИЕ ТРЕБОВАНИЙ К ЭКСПЕРТАМ (КВАЛИФИКАЦИЯ, КАТЕГОРИИ, КОЛИЧЕСТВО), ПРИВЛЕКАЕМЫМ К РАЗРАБОТКЕ ПРОЕКТА ПРОФЕССИОНАЛЬНОГО СТАНДАРТА, И ОПИСАНИЕ ИСПОЛЬЗОВАННЫХ МЕТОДОВ	11
2.3. ЭТАПЫ РАЗРАБОТКИ ПРОЕКТА ПРОФЕССИОНАЛЬНОГО СТАНДАРТА «СПЕЦИАЛИСТ ПО ЗАЩИТЕ ИНФОРМАЦИИ В ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ И СЕТЯХ»:	12
2.4. ОБЩИЕ СВЕДЕНИЯ О НОРМАТИВНЫХ ПРАВОВЫХ ДОКУМЕНТАХ, РЕГУЛИРУЮЩИХ ВИД ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ, ДЛЯ КОТОРОГО РАЗРАБОТАН ПРОЕКТ ПРОФЕССИОНАЛЬНОГО СТАНДАРТА (СПИСОК НОРМАТИВНЫХ ПРАВОВЫХ ДОКУМЕНТОВ С УКАЗАНИЕМ ИХ РЕКВИЗИТОВ, КОНКРЕТНЫХ СТАТЕЙ И ПУНКТОВ)	14
РАЗДЕЛ 3 «ОБСУЖДЕНИЕ ПРОЕКТА ПРОФЕССИОНАЛЬНОГО СТАНДАРТА»	16
3.1. ИНФОРМАЦИЯ О ПОРЯДКЕ ОБСУЖДЕНИЯ	17

**Раздел 1 «Общая характеристика вида профессиональной деятельности,
трудовых функций»**

1.1. Информация о перспективах развития вида профессиональной деятельности.

Профессиональный стандарт «Специалист по защите информации в телекоммуникационных системах и сетях» разработан ООО «АСИС», МОО «АЗИ», Академией ФСБ России, Учебно-методическим объединением по образованию в области информационной безопасности (УМО ИБ) в целях реализации Указов Президента Российской Федерации от 7 мая 2012 г. № 596 «О долгосрочной государственной экономической политике», от 15 января 2013 г. № 597 «О мероприятиях по реализации государственной социальной политики», от 15 января 2013 г. № 31с, решения Совета Безопасности Российской Федерации от 1 октября 2014 года (п.7 протокола заседания) «О противодействии уг-

розам национальной безопасности Российской Федерации в информационной сфере», постановления Правительства Российской Федерации от 31 марта 2014 г. № 487-р и протокольного решения Минтруда России от 8 февраля 2015 г. № 14-3/10/П-576 по итогам совещания по вопросу «О разработке профессиональных стандартов специалистов по группе занятий (профессий) «Специалисты в области информационной безопасности».

Вид профессиональной деятельности - Разработка, внедрение, эксплуатация и менеджмент средств и систем обеспечения информационной безопасности телекоммуникационных систем и сетей в экономике и государственном управлении.

Непрерывный и стремительный рост объемов информации, которую необходимо передавать, приводит к бурному развитию связанной отрасли и, в первую очередь, систем телекоммуникаций. Основной тенденцией такого развития является интеграция телекоммуникационных и информационных систем и технологий, что приводит к формированию и быстрому развитию глобальной телекоммуникационной сети.

Рост объемов информации, циркулирующей в телекоммуникационных системах и сетях (ТКС) приводит к существенному возрастанию рисков несанкционированного доступа к данным, в том числе «критическим» для экономики и государственного управления, путем различного рода воздействий на технические и информационные ресурсы ТКС. Поэтому решение проблемы обеспечения защиты технических и информационных ресурсов телекоммуникационных систем и сетей в условиях существования угроз их информационной безопасности и с учетом текущего уровня развития техники и технологий ТКС продолжает оставаться актуальной задачей.

Задача обеспечения защиты информации в телекоммуникационных системах и сетях в настоящее время решается в рамках построения комплексной системы защиты информации. Без знания и квалифицированного применения современных информационных технологий, стандартов, протоколов, программных и аппаратных средств защиты информации невозможно обеспечить требуемый уровень информационной безопасности телекоммуникационных систем и сетей. Это приводит к необходимости поиска комплексных решений в области разработки методов и средств защиты информации в ТКС, обязательно учитывающих характер вероятных угроз информационной безопасности.

К основным особенностям современного этапа развития телекоммуникационных систем и сетей, влияющим на перспективы рассматриваемого вида профессиональной деятельности относятся:

1. Высокая интеграция компонентов телекоммуникационных систем и при этом распределенный характер построения и функционирования глобальных телекоммуникационных сетей, экспоненциально растущий объем информации, циркулирующей в ТКС.

2. Возрастающее разнообразие и сложность аппаратных платформ, архитектур, отраслевых стандартов, коммуникационных протоколов, сетевых служб и сервисов.

3. Появление новых видов сетевого взаимодействия, бурное развитие беспроводных и оптоволоконных технологий связи, конвергенция существующих телекоммуникационных систем и сетей в единое инфокоммуникационное пространство.

4. Большое количество национальных и международных организаций, координирующих разработки и осуществляющих стандартизацию в области современных ТКС.

5. Существенное увеличение числа угроз критической инфраструктуры, связанное с переносом традиционных информационных ресурсов в распределенные телекоммуникационные системы и сети.

6. Отсутствие правового регулирования глобальной сети Интернет и практики разрешения конфликтов в киберпространстве на международном уровне.

Без преувеличения можно констатировать, что обеспечение требуемого уровня защиты информации во всех национальных телекоммуникационных системах и сетях является важнейшим условием обеспечения государственного суверенитета, экономической безопасности, свободы личности и сохранения геополитической роли России в мире. Поэтому востребованность рассматриваемого вида профессиональной деятельности будет только возрастать.

1.2. Описание обобщенных трудовых функций, входящих в вид профессиональной деятельности.

Деятельность по обеспечению защиты технических и информационных ресурсов телекоммуникационных систем и сетей в условиях существования угроз их информационной безопасности (ИБ) включает следующие обобщенные трудовые функции (ОТФ) и соответствующие им уровни квалификации

Обобщенные трудовые функции (ОТФ)	
Наименование	Уровень квалификации
Выполнение комплекса мер по безопасному функционированию технических и информационных ресурсов ТКС	5
Обеспечение безопасности технических и информационных ресурсов ТКС в процессе эксплуатации	6
Обеспечение функционирования элементов и систем специальной связи государственного управления	6
Разработка средств защиты технических и информационных ресурсов ТКС	7
Обеспечение безопасности технических и информационных ресурсов систем специальной связи государственного управления	7
Менеджмент средств и систем защиты технических и информационных ресурсов ТКС	7
Экспертиза проектных решений в сфере защиты технических и информационных ресурсов ТКС	8

ОТФ «Выполнение комплекса мер по безопасному функционированию технических и информационных ресурсов ТКС» предусматривает 5 уровень квалификации, поскольку это соответствует «Уровням квалификации в целях подготовки профессиональных стандартов» Минтруда России как по показателям уровней квалификации (широта полномочий и ответственность; характер умений; характер знаний), так и по минимальным требованиям к уровню образования и основным путям достижения уровня квалификации.

ОТФ «Обеспечение безопасности технических и информационных ресурсов ТКС в процессе эксплуатации» предусматривает 6 уровень квалификации, поскольку это соответствует «Уровням квалификации в целях подготовки профессиональных стандартов» Минтруда России как по показателям уровней квалификации (широта полномочий и ответственность; характер умений; характер знаний), так и по минимальным требованиям к уровню образования и основным путям достижения уровня квалификации.

ОТФ «Обеспечение функционирования элементов и систем специальной связи государственного управления» предусматривает 6 уровень квалификации, поскольку это соответствует «Уровням квалификации в целях подготовки профессиональных стандартов» Минтруда России как по показателям уровней квалификации (широта полномочий и ответственность; характер умений; характер знаний), так и по минимальным требованиям к уровню образования и основным путям достижения уровня квалификации.

ОТФ «Разработка средств защиты технических и информационных ресурсов ТКС» предусматривает 7 уровень квалификации, поскольку это соответствует «Уровням квалификации в целях подготовки профессиональных стандартов» Минтруда России как по показателям уровней квалификации (широта полномочий и ответственность; характер умений; характер знаний), так и по минимальным требованиям к уровню образования и основным путям достижения уровня квалификации.

ОТФ «Обеспечение безопасности технических и информационных ресурсов систем специальной связи государственного управления» предусматривает 7 уровень квалификации, поскольку это соответствует «Уровням квалификации в целях подготовки профессиональных стандартов» Минтруда России как по показателям уровней квалификации (широта полномочий и ответственность; характер умений; характер знаний), так и по минимальным требованиям к уровню образования и основным путям достижения уровня квалификации.

ОТФ «Менеджмент средств и систем защиты технических и информационных ресурсов ТКС» предусматривает 7 уровень квалификации, поскольку это соответствует «Уровням квалификации в целях подготовки профессиональных стандартов» Минтруда России как по показателям уровней квалификации (широта полномочий и ответственность; характер умений; характер знаний), так и по минимальным требованиям к уровню образования и основным путям достижения уровня квалификации.

ОТФ «Экспертиза проектных решений в сфере защиты технических и информационных ресурсов ТКС» предусматривает 8 уровень квалификации, поскольку это соответствует «Уровням квалификации в целях подготовки профессиональных стандартов» Минтруда России как по показателям уровней квалификации (широта полномочий и ответственность; характер умений; характер знаний), так и по минимальным требованиям к уровню образования и основным путям достижения уровня квалификации.

1.3. Описание состава трудовых функций и обоснование их отнесения к конкретным уровням (подуровням) квалификации.

ОТФ «Выполнение комплекса мер по безопасному функционированию технических и информационных ресурсов ТКС» включает следующие трудовые функции (ТФ) и соответствующие им уровни квалификации

Трудовые функции	Уровень квалификации
Установка программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты технических и информационных ресурсов, оборудования ТКС	5
Обеспечение бесперебойной работы программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты технических и информационных ресурсов, оборудования ТКС	5
Техническое обслуживание программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты технических и информационных ресурсов, оборудования ТКС	5

ТФ «Установка программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты технических и информационных ресурсов, оборудования ТКС» предусматривает 5 уровень квалификации, поскольку это соответствует «Уровням квалификации в целях подготовки профессиональных стандартов» Минтруда России как по показателям уровней квалификации (широта полномочий и ответственность; характер умений; характер знаний), так и по минимальным требованиям к уровню образования и основным путям достижения уровня квалификации.

ТФ «Обеспечение бесперебойной работы программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты технических и информационных ресурсов, оборудования ТКС» предусматривает 5 уровень квалификации, поскольку это соответствует «Уровням квалификации в целях подготовки профессиональных стандартов» Минтруда России как по показателям уровней квалификации (широта полномочий и ответственность; характер умений; характер знаний), так и по минимальным требованиям к уровню образования и основным путям достижения уровня квалификации.

ТФ «Техническое обслуживание программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты технических и информационных ресурсов, оборудования ТКС» предусматривает 5 уровень квалификации, поскольку это соответствует «Уровням квалификации в целях подготовки профессиональных стандартов» Минтруда России как по показателям уровней квалификации (широта полномочий и ответственность; характер умений; характер знаний), так и по минимальным требованиям к уровню образования и основным путям достижения уровня квалификации.

ОТФ «Обеспечение безопасности технических и информационных ресурсов ТКС в процессе эксплуатации» включает следующие трудовые функции (ТФ) и соответствующие им уровни квалификации

Трудовые функции	Уровень квалификации
Мониторинг функционирования телекоммуникационных систем и сетей, защищенности их технических и информационных ресурсов	6
Управление функционированием телекоммуникационных систем и сетей и безопасностью их технических и информационных ресурсов	6
Управление персоналом, обслуживающим программные, программно-аппаратные (в том числе криптографические) и технические средства и системы защиты технических и информационных ресурсов, оборудования телекоммуникационных систем и сетей	6

ТФ «Мониторинг функционирования телекоммуникационных систем и сетей, защищенности их технических и информационных ресурсов» предусматривает 6 уровень квалификации, поскольку это соответствует «Уровням квалификации в целях подготовки профессиональных стандартов» Минтруда России как по показателям уровней квалификации (широта полномочий и ответственность; характер умений; характер знаний), так и по минимальным требованиям к уровню образования и основным путям достижения уровня квалификации.

ТФ «Управление функционированием телекоммуникационных систем и сетей и безопасностью их технических и информационных ресурсов» предусматривает 6 уровень квалификации, поскольку это соответствует «Уровням квалификации в целях подготовки профессиональных стандартов» Минтруда России как по показателям уровней квалификации (широта полномочий и ответственность; характер умений; характер знаний), так и по минимальным требованиям к уровню образования и основным путям достижения уровня квалификации.

ТФ «Управление персоналом, обслуживающим программные, программно-аппаратные (в том числе криптографические) и технические средства и системы защиты технических и информационных ресурсов, оборудования телекоммуникационных систем и сетей» предусматривает 6 уровень квалификации, поскольку это соответствует «Уровням квалификации в целях подготовки профессиональных стандартов» Минтруда России как по показателям уровней квалификации (широта полномочий и ответственность; характер умений; характер знаний), так и по минимальным требованиям к уровню образования и основным путям достижения уровня квалификации.

ОТФ «Обеспечение функционирования элементов и систем специальной связи государственного управления» включает следующие трудовые функции (ТФ) и соответствующие им уровни квалификации

Трудовые функции	Уровень квалификации
Установка специальных технических средств и систем специальной связи государственного управления, включая СКЗИ	6
Обеспечение бесперебойной работы специальных технических средств и систем специальной связи государственного управления, включая СКЗИ	6
Ведение специального делопроизводства и технических документов в процессе эксплуатации средств и систем специальной связи государственного управления, включая СКЗИ	6

ТФ «Установка специальных технических средств и систем специальной связи государственного управления, включая СКЗИ» предусматривает 6 уровень квалификации, поскольку это соответствует «Уровням квалификации в целях подготовки профессиональных стандартов» Минтруда России как по показателям уровней квалификации (широта полномочий и ответственность; характер умений; характер знаний), так и по минимальным требованиям к уровню образования и основным путям достижения уровня квалификации.

ТФ «Обеспечение бесперебойной работы специальных технических средств и систем специальной связи государственного управления, включая СКЗИ» предусматривает 6 уровень квалификации, поскольку это соответствует «Уровням квалификации в целях подготовки профессиональных стандартов» Минтруда России как по показателям уровней квалификации (широта полномочий и ответственность; характер умений; характер знаний), так и по минимальным требованиям к уровню образования и основным путям достижения уровня квалификации.

ТФ «Ведение специального делопроизводства и технических документов в процессе эксплуатации средств и систем специальной связи государственного управления, включая СКЗИ» предусматривает 6 уровень квалификации, поскольку это соответствует «Уровням квалификации в целях подготовки профессиональных стандартов» Минтруда России как по показателям уровней квалификации (широта полномочий и ответственность; характер умений; характер знаний), так и по минимальным требованиям к уровню образования и основным путям достижения уровня квалификации.

ОТФ «Разработка средств защиты технических и информационных ресурсов ТКС» включает следующие трудовые функции (ТФ) и соответствующие им уровни квалификации.

Трудовые функции	Уровень квалификации
Анализ угроз информационной безопасности ТКС	7
Реализация средств и систем защиты технических и информационных ресурсов ТКС	7

Проведение НИР и ОКР в сфере разработки средств и систем защиты технических и информационных ресурсов ТКС	7
---	---

ТФ «Анализ угроз информационной безопасности ТКС» предусматривает 7 уровень квалификации, поскольку это соответствует «Уровням квалификации в целях подготовки профессиональных стандартов» Минтруда России как по показателям уровней квалификации (широта полномочий и ответственность; характер умений; характер знаний), так и по минимальным требованиям к уровню образования и основным путям достижения уровня квалификации.

ТФ «Реализация средств и систем защиты технических и информационных ресурсов ТКС» предусматривает 7 уровень квалификации, поскольку это соответствует «Уровням квалификации в целях подготовки профессиональных стандартов» Минтруда России как по показателям уровней квалификации (широта полномочий и ответственность; характер умений; характер знаний), так и по минимальным требованиям к уровню образования и основным путям достижения уровня квалификации.

ТФ «Проведение НИР и ОКР в сфере разработки средств и систем защиты технических и информационных ресурсов ТКС» предусматривает 7 уровень квалификации, поскольку это соответствует «Уровням квалификации в целях подготовки профессиональных стандартов» Минтруда России как по показателям уровней квалификации (широта полномочий и ответственность; характер умений; характер знаний), так и по минимальным требованиям к уровню образования и основным путям достижения уровня квалификации.

ОТФ «Обеспечение безопасности технических и информационных ресурсов систем специальной связи государственного управления» включает следующие трудовые функции (ТФ) и соответствующие им уровни квалификации.

Трудовые функции	Уровень квалификации
Организация функционирования элементов и систем специальной связи государственного управления	7
Проведение НИР и ОКР в сфере разработки средств и элементов систем специальной связи государственного управления, включая СКЗИ	7
Контроль безопасности и функциональности систем специальной связи государственного управления	7

ТФ «Организация функционирования элементов и систем специальной связи государственного управления» предусматривает 7 уровень квалификации, поскольку это соответствует «Уровням квалификации в целях подготовки профессиональных стандартов» Минтруда России как по показателям уровней квалификации (широта полномочий и ответственность; характер умений; характер знаний), так и по минимальным требованиям к уровню образования и основным путям достижения уровня квалификации.

ТФ «Проведение НИР и ОКР в сфере разработки средств и элементов систем специальной связи государственного управления, включая СКЗИ» предусматривает 7 уровень квалификации, поскольку это соответствует «Уровням квалификации в целях подготовки профессиональных стандартов» Минтруда России как по показателям уровней квалификации (широта полномочий и ответственность; характер умений; характер знаний), так и по минимальным требованиям к уровню образования и основным путям достижения уровня квалификации.

ТФ «Контроль безопасности и функциональности систем специальной связи государственного управления» предусматривает 7 уровень квалификации, поскольку это соответствует «Уровням квалификации в целях подготовки профессиональных стандартов» Минтруда России как по показателям уровней квалификации (широта полномочий и ответственность; характер умений; характер знаний), так и по минимальным требованиям к уровню образования и основным путям достижения уровня квалификации.

ОТФ «Менеджмент средств и систем защиты технических и информационных ресурсов ТКС» включает следующие трудовые функции (ТФ) и соответствующие им уровни квалификации.

Трудовые функции	Уровень квалификации
Управление рисками систем защиты технических и информационных ресурсов ТКС	7
Управление отношениями с поставщиками и потребителями программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты технических и информационных ресурсов ТКС	7
Управление отношениями с регуляторами в сфере защиты информации	7

ТФ «Управление рисками систем защиты технических и информационных ресурсов ТКС» предусматривает 7 уровень квалификации, поскольку это соответствует «Уровням квалификации в целях подготовки профессиональных стандартов» Минтруда России как по показателям уровней квалификации (широта полномочий и ответственность; характер умений; характер знаний), так и по минимальным требованиям к уровню образования и основным путям достижения уровня квалификации.

ТФ «Управление отношениями с поставщиками и потребителями программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты технических и информационных ресурсов ТКС» предусматривает 7 уровень квалификации, поскольку это соответствует «Уровням квалификации в целях подготовки профессиональных стандартов» Минтруда России как по показателям уровней квалификации (широта полномочий и ответственность; характер умений; характер знаний), так и по минимальным требованиям к уровню образования и основным путям достижения уровня квалификации.

ТФ «Управление отношениями с регуляторами в сфере защиты

информации» предусматривает 7 уровень квалификации, поскольку это соответствует «Уровням квалификации в целях подготовки профессиональных стандартов» Минтруда России как по показателям уровней квалификации (широта полномочий и ответственность; характер умений; характер знаний), так и по минимальным требованиям к уровню образования и основным путям достижения уровня квалификации.

ОТФ «Экспертиза проектных решений в сфере защиты технических и информационных ресурсов ТКС» включает следующие трудовые функции (ТФ) и соответствующие им уровни квалификации.

Трудовые функции	Уровень квалификации
Исследование эффективности способов, средств и систем защиты технических и информационных ресурсов ТКС	8
Разработка технологических процессов производства программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты технических и информационных ресурсов ТКС	8
Проведение НИР в области разработки методов и средств обеспечения безопасности функционирования систем специальной связи государственного управления	8

ТФ «Исследование эффективности способов, средств и систем защиты технических и информационных ресурсов ТКС» предусматривает 8 уровень квалификации, поскольку это соответствует «Уровням квалификации в целях подготовки профессиональных стандартов» Минтруда России как по показателям уровней квалификации (широта полномочий и ответственность; характер умений; характер знаний), так и по минимальным требованиям к уровню образования и основным путям достижения уровня квалификации.

ТФ «Разработка технологических процессов производства программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты технических и информационных ресурсов ТКС» предусматривает 8 уровень квалификации, поскольку это соответствует «Уровням квалификации в целях подготовки профессиональных стандартов» Минтруда России как по показателям уровней квалификации (широта полномочий и ответственность; характер умений; характер знаний), так и по минимальным требованиям к уровню образования и основным путям достижения уровня квалификации.

ТФ «Разработка средств и элементов систем специальной связи государственного управления, включая СКЗИ» предусматривает 7 уровень квалификации, поскольку это соответствует «Уровням квалификации в целях подготовки профессиональных стандартов» Минтруда России как по показателям уровней квалификации (широта полномочий и ответственность; характер умений; характер знаний), так и по минимальным требованиям к уровню образования и основным путям достижения уровня квалификации.

ТФ «Проведение НИР в области разработки методов и средств обеспечения

безопасности функционирования систем специальной связи государственного управления» предусматривает 8 уровень квалификации, поскольку это соответствует «Уровням квалификации в целях подготовки профессиональных стандартов» Минтруда России как по показателям уровней квалификации (широта полномочий и ответственность; характер умений; характер знаний), так и по минимальным требованиям к уровню образования и основным путям достижения уровня квалификации.

Раздел 2 «Основные этапы разработки проекта профессионального стандарта»

2.1. Информация об организациях, на базе которых проводились исследования, и обоснование выбора этих организаций

Организации, на базе которых проводились исследования:

1. ООО «АСИС»;
2. МОО «Ассоциация защиты информации»;
3. Учебно-методическое объединение по образованию в области информационной безопасности (УМО ИБ);
4. Институт криптографии, связи и информатики Академии ФСБ России.

Выбор этих организаций основывался на следующих требованиях:

1. Практический опыт в сфере защиты информации в телекоммуникационных системах и сетях.

2. Большой опыт в организации подготовки специалистов в области информационной безопасности в целом, а также в сфере разработки, внедрения и эксплуатации средств и систем обеспечения информационной безопасности телекоммуникационных систем и сетей в экономике и государственном управлении, в частности.

3. Содействие организациям, предприятиям и органам государственной власти Российской Федерации в реализации государственной политики в области обеспечения защиты информации.

4. Наличие у организаций разработчиков лицензии на проведение работ с использованием сведений, составляющих государственную тайну.

Перечень организаций, сведения об уполномоченных лицах, участвовавших в разработке проекта профессионального стандарта, приводятся в приложении № 1 к пояснительной записке.

2.2. Описание требований к экспертам (квалификация, категории, количество), привлекаемым к разработке проекта профессионального стандарта, и описание использованных методов

К разработке проекта профессионального стандарта «Специалист по информационной безопасности» были привлечены эксперты трех категорий:

- 1) Представители организаций-заказчиков/потребителей услуг в области информационной безопасности;
- 2) Представители образовательных организаций, реализующих специальности (направления подготовки) в области информационной безопасности;
- 3) Представители организаций-работодателей отрасли информационной безопасности, осуществляющих не менее 5 лет деятельность в области информационной безопасности, предприятий различных форм собственности.

В экспертную группу разработки проекта профессионального стандарта вошли руководители и специалисты-эксперты в данном виде профессиональной деятельности, специалисты в области управления, обучения и развития персонала, другие специалисты. Требования к квалификации экспертов-разработчиков проекта профессионального стандарта:

- 1) Должность - не ниже руководителя подразделения или ведущего специалиста;
- 2) Стаж - не менее 5 лет работы в области информационной безопасности в организации, которая является работодателем в отрасли, либо является представителем системы профессионального образования, оказывающей образовательные услуги в области информационной безопасности.

2.3. Этапы разработки проекта профессионального стандарта «Специалист по защите информации в телекоммуникационных системах и сетях»:

Этап 1. Анализ нормативных правовых актов, руководящих, методических и организационно-распорядительных документов федеральных органов исполнительной власти, научной и методической литературы в области обеспечения информационной безопасности (далее – ИБ) и разработки профессиональных стандартов.

1.1. Анализ российских и международных профессиональных стандартов (проектов стандартов) по схожим видам профессиональной деятельности, проектов профессиональных стандартов (далее – ПС) в области информационной безопасности (не менее 30 стандартов);

1.2. Анализ состояния и перспектив развития соответствующего вида экономической деятельности, группы занятий, к которым относится профессиональный стандарт. Предметом анализа являются: прогнозные документы (федеральных, ведомственных, региональных, корпоративных органов и организаций), содержащие концепции и прогнозы в области информационных технологий и информационной безопасности; состояние и развитие научно-технического прогресса в области информационных технологий и информационной безопасности; материалы по прогнозированию вероятных изменений в видах профессиональной деятельности специалиста по защите информации и его профессионального роста, анализ опыта подготовки отечественных и зарубежных специалистов в области информационной безопасности (не менее 50 документов).

1.3. Анализ тарифно-квалификационных характеристик, содержащихся в Едином тарифно-квалификационном справочнике работ и профессий рабочих, и квалификационных характеристик, содержащихся в Едином квалификационном справочнике должностей руководителей, специалистов и служащих соотнесенные с отраслью «Информационная безопасность» и со смежными отраслями (не менее 30 должностей).

1.4. Анализ нормативных правовых актов, иных организационно-распорядительных документов, которыми определены требования к квалификации по профессиям, должностям, специальностям, соответствующим данному виду профессиональной деятельности: Законов, Указов и распоряжений Президента Российской Федерации, постановлений Правительства Российской Федерации – не менее 40; нормативных правовых и руководящих документов ФСБ России, ФСТЭК России – не менее 20 документов; ГОСТов в области информационной безопасности – не менее 20.

Этап 2. Системный анализ практической деятельности специалистов в области информационной безопасности.

2.1. Сбор и анализ перечня должностей и должностных обязанностей специалистов в области обеспечения ИБ подразделений по защите информации в органах государственной власти и управления, в организациях различных форм собственности, находящихся в субъектах Российской Федерации.

2.2. Анализ профессиональной деятельности специалистов в области обеспечения информационной безопасности на местах (наблюдение; хронометраж профессиональных функций, выполняемых специалистами, оценка их значимости; анкетирование специалистов и руководителей подразделений по обеспечению информационной безопасности; анализ данных интервью, бесед со специалистами по защите информации разных квалификационных уровней).

2.3. Составление обобщенного (типового) классификатора трудовых функций и трудовых действий, сгруппированных по функциональным областям и уровням квалификаций.

Этап 3. Разработка профессионального стандарта.

3.1. Обоснование и определение наименования вида профессиональной деятельности и основной цели вида профессиональной деятельности. Обоснование и определение группы занятий, в которой указывается наименование одной или нескольких базовых групп занятий и одного или нескольких видов, подгрупп или групп экономической деятельности в соответствии с ОКВЭД, к которым относится данный вид профессиональной деятельности конкретного профессионального стандарта.

3.2. Обоснование и разработка функциональной карты вида профессиональной деятельности: разработка обобщенных трудовых функций, соотнесенных с уровнем квалификации; разработка и определение перечня трудовых функций соответствующего вида профессиональной деятельности, входящих в состав обобщенных трудовых функций; определение уровня квалификации для каждой трудовой функции; разработка и описание перечня основных трудовых действий, обеспечивающих выполнение трудовой функции; разработка и описание умений и знаний, обеспечивающих выполнение всех трудовых действий. Анкетирование работодателей по определению важности элементов функциональной карты.

3.3. Определение возможных наименований должностей работников, выполняющих каждую обобщенную трудовую функцию. Обоснование и определение требований к опыту практической работы (характер и продолжительность такого опыта).

3.4. Обоснование и определение требований к уровню профессионального образования, направленности основных и (или) дополнительных программ профессионального образования.

3.5. Определение особых условий допуска к работе - наличие специального права в соответствии с федеральными законами и иными нормативными правовыми актами Российской Федерации, необходимого для выполнения работы, а также ссылки на документы, содержащие эти требования.

3.6. Определение дополнительных характеристик обобщенных трудовых функций. Разработка и описание факторов производственной среды и трудового процесса с учетом специфики отрасли «Информационная безопасность».

3.7. Обоснование и уточнение формулировок наименований проекта профессионального стандарта в соответствии со спецификой деятельности и сложившимся разделением труда между специалистами по информационной безопасности. Согласование

формулировок с основными регуляторами в области информационной безопасности.

3.8. Проведение мониторинга технологий и содержания профессиональной деятельности в целях внесения изменений в проект ПС.

Этап 4. Профессионально-общественное обсуждение проекта профессионального стандарта.

4.1. Организация обсуждения проекта профессионального стандарта (элементов проекта профессионального стандарта) с заинтересованными организациями (работодателями и их объединениями, профессиональными сообществами, саморегулируемыми организациями, профессиональными союзами и их объединениями, федеральными и региональными органами исполнительной власти, государственными компаниями и государственными корпорациями, образованными в соответствии с федеральными законами, и другими организациями).

4.2. Проведение конференций, круглых столов, семинаров и других публичных мероприятий.

4.3. Информирование представителей заинтересованных организаций о состоянии разработки и согласования проекта ПС.

4.4. Проведение сбора, обобщения и анализа замечаний и предложений по проекту ПС, внесение в него необходимых изменений. Оформление результатов обсуждения.

2.4. Общие сведения о нормативных правовых документах, регулирующих вид профессиональной деятельности, для которого разработан проект профессионального стандарта (список нормативных правовых документов с указанием их реквизитов, конкретных статей и пунктов)

1. ГОСТ 19.201-78 Техническое задание. Требования к содержанию и оформлению.
2. ГОСТ 19.301-79 Программа и методика испытаний. Требования к содержанию и оформлению.
3. ГОСТ 24375-80. Радиосвязь. Термины и определения.
4. ГОСТ 17422-82. Системы передачи данных. Скорости передачи данных.
5. ГОСТ 28147-89 Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.
6. ГОСТ 29099-91 Сети вычислительные локальные. Термины и определения.
7. ГОСТ 13661-92 Совместимость технических средств электромагнитная. Пассивные помехоподавляющие фильтры и элементы. Методы измерения вносимого затухания
8. ГОСТ Р ИСО 9542-93 Информационная технология. Передача данных и обмен информацией между системами.
9. ГОСТ Р 50842-95 Совместимость радиоэлектронных средств электромагнитная. Устройства радиопередающие народнохозяйственного применения. Требования к побочным радиоизлучениям. Методы измерения и контроля.
10. ГОСТ 15.101-98. Система разработки и постановки продукции на производство. Порядок выполнения научно-исследовательских работ.
11. ГОСТ Р ИСО 7498-1-99 ИТ. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель.
12. ГОСТ Р ИСО 7498-2-99 ИТ. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации.

13. ГОСТ Р ИСО 7498-4-99 ИТ. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 4. Основы административного управления.
14. ГОСТ Р ИСО/МЭК 7498-1-99. Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель.
15. ГОСТ Р ИСО/МЭК 7498-4-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 4. Основы административного управления
16. ГОСТ Р 51664-2000. Системы и аппаратура автоматического управления каналами радиосвязи.
17. ГОСТ Р 52069.0-2003 Защита информации. Система стандартов. Основные положения.
18. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации. Номенклатура показателей качества.
19. ГОСТ Р 50.1.056-2005. Техническая защита информации. Основные термины и определения.
20. ГОСТ Р 52448-2005 Защита информации. Обеспечение безопасности сетей электросвязи. Общие положения.
21. ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью.
22. ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий.
23. ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента ИБ.
24. ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети.
25. ГОСТ Р ИСО/МЭК ТО 13335-3-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий.
26. ГОСТ Р ИСО/МЭК ТО 13335-4-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер.
27. ГОСТ Р 53109-2008 Система обеспечения информационной безопасности сети связи общего пользования.
28. ГОСТ Р ИСО/МЭК 15408-1-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационная технологий. Часть 1.
29. ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационная технологий. Часть 2.
30. ГОСТ Р ИСО/МЭК 15408-3-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационная технологий. Часть 3.
31. ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи
32. ГОСТ Р 34.11-2012. Информационная технология. Криптографическая защита информации. Функция хэширования.

Базовые нормативные документы, использованные при разработке стандарта

Нормативный документ	Элемент ПС
ГОСТ Р 51583-2014 п. 5, 6, 7	ТФ F/01.7, ТФ F/02.7, ТФ F/03.7, ТФG/02.8
ГОСТ Р 51583-2014, п. 6.1	ТФ A/01.5, ТФ A/02.5, ТФ A/03.5
ГОСТ Р 51583-2014 п. 6.3	ТФ E/03.7, ТФ E/01.7, ТФG/03.8
ГОСТ Р 51583-2014 п.6.3.1	ТФ D/01.7
ГОСТ Р 51583-2014, п. 6.3.2	ТФА/02.5, ТФ A/03.5
Приказ ФСБ России от 09.02.2005 № 66	ОТФ B, C, D, E, F, G
Приказ ФСБ России от 21.02.08 г. № 149	ТФ E/02.7
Приказ ФСТЭК № 17 п. 14	ОТФ C
Приказ ФСТЭК №17 п. 14.2	ТФ D/01.7
ГОСТ Р 50922-2006 п.2.6.8	ТФD/01.7
ГОСТ Р 50922-2006 п.2.4.3	ТФ D/02.7, ТФ D/03.7, ТФG/01.8
ГОСТ Р ИСО/МЭК 13335-1 – 2006 п. 3.3	ТФ D/01.7
ГОСТ Р ИСО 7498-2-99 ч. 2	ТФ C/01.6
ГОСТ 15.101-98 п.5	ТФ D/02.7, ТФ D/03.7, ТФG/01.8
ГОСТ 34.601 п. 1 – 3	ТФ E/02.7
ГОСТ ИСО/МЭК 27001-2006 п. 6	ТФ E/03.7
ГОСТ Р ИСО/МЭК 27001-2006 п. 4,5,7	ТФG/02.8
ГОСТ Р ИСО 9001-2008 п. 4, 7	ТФ F/01.7, ТФ F/03.7
ГОСТ Р ИСО 9001-2008 п. 4, 5	ТФ F/02.7

Раздел 3 «Обсуждение проекта профессионального стандарта»

К разработке проекта профессионального стандарта «**Специалист по защите информации в телекоммуникационных системах и сетях**» были привлечены эксперты трех категорий:

- 1) Представители организаций-заказчиков (потребителей) услуг в области информационной безопасности;
- 2) Представители образовательных организаций, реализующих специальности (направления подготовки) в области информационной безопасности;
- 3) Представители организаций-работодателей отрасли информационной безопасности, осуществляющих не менее 5 лет деятельность в области информационной безопасности, предприятий различных форм собственности.

В экспертную группу разработки проекта профессионального стандарта вошли руководители и специалисты-эксперты в данном виде профессиональной деятельности, специалисты в области управления, обучения и развития персонала, другие специалисты.

Требования к квалификации экспертов-разработчиков проекта профессионального стандарта:

Должность - не ниже руководителя подразделения или ведущего специалиста;

1) Стаж - не менее 5 лет работы в области информационной безопасности в организации, которая является работодателем в отрасли, либо является представителем системы профессионального образования, оказывающей образовательные услуги в области информационной безопасности.

2) Наличие у экспертов допуска к сведениям, составляющим государственную тайну.

3.1. Информация о порядке обсуждения

Мероприятия, на которых проводилось обсуждение проектов профессиональных стандартов

1. 17-й Национальный форум информационной безопасности «Информационная безопасность России в цифровую эпоху: новые вызовы, угрозы, решения» (Инфофорум-2015).

5-6 февраля 2015 года, г. Москва.

Количество участников: 839

Количество организаций: 472

из них:

образовательных организаций ВО: 103 (161 человек)

образовательных организаций СПО: 8 (11 человек);

образовательных организаций ДПО: 6 (7 человек);

коммерческих организаций: 116 (260 человек)

представителей ФОИВ: 44 ФОИВ (138 человек);

представителей рег. органов исполнительной и законодательной власти: 73 (91 человек)

Остальные участники представляли: зарубежные страны, научные и общественные организации, СМИ, другие организации.

2. Пленум регионального отделения УМО ИБ по Центральному федеральному округу.

27 марта 2015 года, г. Москва.

Количество участников: 106

Количество организаций: 58

из них:

образовательных организаций ВО: 37 (70 человек)

образовательных организаций СПО: 1 (1 человек);

образовательных организаций ДПО: 9 (14 человек);

коммерческих организаций: 5 (6 человек)

представителей ФОИВ: 6 ФОИВ (15 человек);

3. Совместное заседание Совета учебно-методического центра по защите информации Приволжского федерального округа (далее – Совет УМЦ) и регионального отделения Учебно-методического объединения высших учебных заведений Российской Федерации по образованию в области информационной безопасности в Приволжском федеральном округе; методический сбор с

преподавательским составом образовательных организаций, осуществляющих в пределах округа подготовку специалистов по защите информации.

01 апреля 2015 года, г. Нижний Новгород

Количество участников: 30

Количество организаций: 25

4. IV Форум АЗИ «Актуальные вопросы информационной безопасности».

14 апреля 2015 года, г. Москва.

Количество участников: 292

Количество организаций: 197

из них:

образовательных организаций ВО: 18 (24 участника)

образовательных организаций СПО: 1 (1 участник);

образовательных организаций ДПО: 43 (57 участников);

коммерческих организаций: 132 (204 участника)

представителей ФОИВ: 3 ФОИВ (6 участников);

5. Партнерская конференция ИнфоТеКС 2015.

19-22 мая 2015 г., г. Москва

Количество участников: 113

Количество организаций: 76

из них:

образовательных организаций ВО: 57 (78 человек)

образовательных организаций СПО: 5 (7 человек);

образовательных организаций ДПО: 4 (13 человек);

коммерческих организаций: 7 (10 человек);

представителей ФОИВ: 3 ФОИВ (5 человек);

6. XIX Пленум УМО ИБ, XIV международная научно-практическая конференция «Информационная безопасность», заседания ЮгРоУМО ИБ и курсы повышения квалификации по программе «Нормативно-правовое и научно-методическое обеспечение учебного процесса в контексте практического опыта реализации ФГОС нового поколения и образовательных программ в области информационной безопасности».

3-7 июня 2015 года, г. Таганрог.

Количество участников: 128

Количество организаций: 81

из них:

образовательных организаций ВО: 55 (80 человек)

образовательных организаций СПО: 2 (3 человека);

образовательных организаций ДПО: 13 (20 человек);

коммерческих организаций: 7 (10 человек)

представителей ФОИВ: 4 ФОИВ (6 человек).

7.Вебинар «Проблемы реализации требований профессиональных стандартов в области информационной безопасности в образовательных программах высшего образования».

18 июня 2015 г., г. Москва.

Всего участников: 40

Всего организаций: 36

8. 24-ая научно-техническая конференция «Методы и технические средства обеспечения безопасности информации».

29 июня – 02 июля 2015 г., г. Санкт-Петербург.

Всего участников: 150

Всего организаций: 60

Из них:

Представителей образовательных учреждений высшего образования: 20 (из 16 организаций)

Представителей образовательных учреждений дополнительного профессионального образования: 5 (из 5 организаций)

Представителей коммерческих организаций: 113 (из 33 организаций)

Представителей федеральных органов исполнительной власти: 12 (из 6 организаций).

9. XI Евразийский форум информационной безопасности «ИНФОФОРУМ - КРЫМ», 6-10 июля 2015 г., г. Севастополь.

Всего участников: 318

Всего организаций: 83

10. XIV Всероссийская конференция «Информационная безопасность. Региональные аспекты. ИнфоБЕРЕГ», 8-11 сентября 2015 г., г. Сочи.

Всего участников: 130

Всего организаций: 62

11. Конференция «Состояние и перспектив развития ИКТ-инфраструктуры при обеспечении доверия и безопасности», 7-8 октября 2015 г., г. Москва, Ассоциация документальной электросвязи.

Всего участников: 128

Всего организаций: 63

Генеральный директор ЗАО
«Ассоциация специалистов информационных систем»
Солодянников

А.В.

_____ 2015 г.