Пояснительная записка к проекту профессионального стандарта
«Специалист по защите информации в автоматизированных системах»

Оглавление

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 автоматизированных системах**» 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 угрозам 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 — обеспечение безопасности информации в автоматизированных системах.

В настоящее время проблема обеспечения защиты информации в автоматизированных системах, особенно предназначенных для обработки конфиденциальной и персональной

информации, приобрела особую актуальность. По мнению Совета Безопасности Российской Федерации информационная сфера Российской Федерации является одним из основных приоритетов обеспечения национальной безопасности Российской Федерации.

В современных условиях к автоматизированным систем с точки зрения задач обеспечения защиты информации предъявляется широкий спектр требований, определяющий перспективы развития вида профессиональной деятельности – «обеспечение безопасности информации в автоматизированных системах». Среди основных особенностей профессиональной деятельности в области защиты информации в автоматизированных системах можно выделить следующие.

1. Высокая степень интеграция современных автоматизированных систем ведет к необходимости поиска комплексных решений в области разработки методов обеспечения безопасности информационной, учитывающих особенности работы операционных систем, сетевого многоуровневого взаимодействия и прикладных программ, ориентированных на решение различных информационных задач.

2. Необходимость использование в автоматизированных системах сложных информационных технологий передачи, обработки и хранения информации в сочетании с их широкой доступностью. Простота доступа и широкая аудитория являются принципиальным требованием для некоторых категорий автоматизированных систем, прежде всего в банковской сфере, электронной коммерции и в сфере оказания электронных государственных услуг.

3. Развитие сетевых технологий и телекоммуникаций с различной архитектурой и коммуникационными протоколами, большим набором сетевых служб и сервисов, широкое использование сервис-ориентированной архитектуры. Эта особенность, с одной стороны, расширяет возможности организации скрытого взаимодействия и обеспечения анонимности, а, с другой стороны, повышает требования к безопасности работы в недоверенном и зачастую агрессивном окружении. Появление новых видов сетевого взаимодействия, включая интенсивное развитие аппаратных средств и протоколов беспроводной и мобильной связи, приводит к необходимости расширения и совершенствования методов защиты информации в автоматизированных системах, учитывающих особенности новых технологий организации доступа и обработки информации.

4. Широкое использование для построения автоматизированных систем зарубежных компьютерных и коммуникационных технологий дает потенциальную возможность спецслужбам зарубежных стран во взаимодействии с глобальными интернет-компаниями, а также с производителями компьютерного и коммуникационного оборудования и программного обеспечения выстраивать широкий спектр атак с целью получения конфиденциальной информации, обрабатываемой автоматизированными системами.

5. Необходимость обеспечения бесперебойной работы автоматизированных систем требует реализации методов и технологий быстрого восстановления обрабатываемой информации после возникновения внештаных ситуаций.

6. Появление сложных организационных, технологических, криптографических и правовых проблем в связи с широким внедрением в государственных структурах и субъектах экономической деятельности систем электронного документооборота. Проблема создания юридически значимого электронного документооборота особенно усложнена отсутствием отечественных разработок в области текстовых процессоров и других современных средств обработки, сопровождения и архивирования документов, занимающих сколько-нибудь заметное место на рынке. Для защиты электронного документооборота в РФ был принят Федеральный закон «Об электронной цифровой подписи» и разработан проект закона об электронном документе. Происходило активное внедрение нового государственного стандарта электронной цифровой подписи на основе эллиптических кривых и разработка возможных вариантов реализации удостоверяющего центра. Вместе с тем, пока остается много нерешенных технических проблем с обеспечением безопасности удостоверяющих центров.

7. В качестве угроз безопасности информации автоматизированных систем выступают и преступления в сфере компьютерной информации. Так, по данным МВД России, за период с 2010 по

сентябрь 2014 года зарегистрировано 12816 преступлений по ст. 273 УК РФ (Неправомерный доступ к компьютерной информации) и 3828 преступлений по ст. 273 УК РФ (Создание, использование и распространение вредоносных компьютерных программ). Эффективное блокирование этих угроз возможно только на основе сочетания слаженных действий высококвалифицированного персонала автоматизированных систем и средств защиты информации.

8. Повышение технологического уровня и совершенствование тактики информационно-технических воздействий на автоматизированные системы предъявляет новые требования к архитектуре и степени интеграции систем защиты информации в автоматизированных системах.

9. Расширение номенклатуры сертифицированных средств защиты информации, применяемых в автоматизированных системах, требует от специалистов регулярной актуализации умений и знаний для эффективного выполнения трудовых функций.

10. Использование сертифицированных криптографических средств в системах защиты информации в автоматизированных системах как для идентификации пользователей систем, так и для обеспечения целостности и конфиденциальности обрабатываемой информации, все чаще становится обязательным требованием при проектировании современных автоматизированных систем не только для государственных, но и для коммерческих организаций.

Специалисты в области защиты информации в автоматизированных системах должны владеть широким спектром языков программирования, в том числе для серверных и многопоточных приложений, средствами разработки, отладки, инструментами виртуализации, иметь навыки работы в современных операционных системах на уровне системного программиста и системного администратора, знать и применять на практике передовые приемы разработки и эксплуатации систем защиты информации автоматизированных систем, разработки моделей, методов и методик проектирования и формирования требований к системам защиты информации в автоматизированных системах.

Таким образом, результаты анализа актуальных тенденций в сфере защиты информации в автоматизированных системах в условиях увеличения сложности их реализации, объемов и значимости решаемых задач и сложившаяся система профессиональных отношений в рассматриваемой области обуславливают необходимость стандартизации трудовых функций специалистов в области защиты информации в автоматизированных системах.

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

В проекте предлагаемого профессионального стандарта приведены следующие обобщенные трудовые функции, входящие в вид профессиональной деятельности:

– обслуживание систем защиты информации в автоматизированных системах (ОТФ1 – 5 уровень квалификации);

– обеспечение защиты информации в автоматизированных системах в процессе их эксплуатации (ОТФ2 – 6 уровень квалификации);

– внедрение систем защиты информации автоматизированных систем (ОТФ3 – 6 уровень квалификации);

– разработка систем защиты информации автоматизированных систем (ОТФ4 – 7 уровень квалификации);

– формирование требований к защите информации в автоматизированных системах (ОТФ5 – 8 уровень квалификации).

ОТФ1 «Обслуживание систем защиты информации в автоматизированных системах» 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.

ОТФ2 «Обеспечение защиты информации в автоматизированных системах в процессе их 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.

ОТФ3 «Внедрение систем защиты информации автоматизированных систем» 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.

ОТФ4 «Разработка систем защиты информации автоматизированных систем» 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.

ОТФ5 «Формирование требований к защите информации в автоматизированных системах» 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 включают следующие трудовые функции:

	Ур. квалификации	Наименование трудовых функций
ОТФ1	5	Обеспечение защиты информации при выводе из эксплуатации автоматизированных систем
		Ведение технической документации, связанной с эксплуатацией систем защиты информации автоматизированных систем
		Проведение регламентных работ по эксплуатации систем защиты информации автоматизированных систем
ОТФ2	6	Диагностика систем защиты информации автоматизированных систем
		Администрирование систем защиты информации автоматизированных систем
		Управление защитой информации в автоматизированных системах
		Восстановление работоспособности систем защиты информации при возникновении нештатных ситуаций
		Мониторинг защищенности информации в автоматизированных системах
		Аудит защищенности информации в автоматизированных системах
ОТФ3	6	Установка и настройка средств защиты информации в автоматизированных системах
		Разработка организационно-распорядительных документов по защите информации в автоматизированных системах
		Анализ уязвимостей внедряемой системы защиты информации
		Внедрение организационных мер по защите информации в автоматизированных системах
ОТФ4	7	Тестирование систем защиты информации автоматизированных систем

		Разработка проектных решений по защите информации в автоматизированных системах
		Разработка эксплуатационной документации на системы защиты информации автоматизированных систем
		Разработка программных и программно-аппаратных средств для систем защиты информации автоматизированных систем
ОТФ5	8	Обоснование необходимости защиты информации в автоматизированной системе
		Определение угроз безопасности информации, обрабатываемой автоматизированной системой
		Разработка архитектуры системы защиты информации автоматизированной системы
		Моделирование защищенных автоматизированных систем с целью анализа их уязвимостей и эффективности средств и способов защиты информации

Для выполнения трудовых функций, отнесенных к ОТФ1, требуется среднее профессиональное образование или высшее образование по УГС (направлению подготовки) «Информационная безопасность». Для выполнения трудовых функций, отнесенных к ОТФ2 – ОТФ5 требуется соответствующее высшее образование.

ТФ «Обеспечение защиты информации при выводе из эксплуатации автоматизированных систем» 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 «Ведение технической документации, связанной с эксплуатацией систем защиты информации автоматизированных систем» 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 «Проведение регламентных работ по эксплуатации систем защиты информации автоматизированных систем» 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 «Диагностика систем защиты информации автоматизированных систем» 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 «Администрирование систем защиты информации автоматизированных систем» 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 защитой информации в автоматизированных системах» 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 «Восстановление работоспособности систем защиты информации при возникновении нештатных ситуаций» 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 «Мониторинг защищенности информации в автоматизированных системах» 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 «Аудит защищенности информации в автоматизированных системах» 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 «Установка и настройка средств защиты информации в автоматизированных системах» 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 «Разработка организационно-распорядительных документов по защите информации в автоматизированных системах» 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 «Анализ уязвимостей внедряемой системы защиты информации» 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 «Внедрение организационных мер по защите информации в автоматизированных системах» 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 «Тестирование систем защиты информации автоматизированных систем» 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 «Разработка проектных решений по защите информации в автоматизированных системах» предусматривает 7 уровень квалификации, поскольку это соответствует «Уровням квалификации в целях подготовки профессиональных стандартов» Минтруда России как по показате-

лям 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 эксплуатационной документации на системы защиты информации автоматизированных систем» 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 «Разработка программных и программно-аппаратных средств для систем защиты информации автоматизированных систем» 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 «Обоснование необходимости защиты информации в автоматизированной системе» 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 «Определение угроз безопасности информации, обрабатываемой автоматизированной системой» 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 архитектуры системы защиты информации автоматизированной системы» 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 «Моделирование защищенных автоматизированных систем с целью анализа их уязвимостей и эффективности средств и способов защиты информации» 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 научных исследований, разработки и эксплуатации средств защиты информации.

2. Большой опыт в организации подготовки специалистов в области информационной безопасности в целом, а также в сфере информационной безопасности автоматизированных систем.

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.

2.2. Этапы разработки проекта профессионального стандарта.

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 проекта ПС, внесение в него необходимых изменений. Оформление результатов обсуждения.

Этап 5. Экспертиза проекта профессионального стандарта.

5.1. Организация экспертизы элементов проекта ПС на всех этапах их разработки. Организация экспертизы итогового проекта профессионального стандарта.

5.2. Формирование требований к экспертам (квалификация, категории, количество) и профильным организациям, привлекаемым к экспертизе проекта ПС.

5.3. Формирование состава независимых экспертов и проведение экспертизы проекта ПС.

5.4. Формирование состава профильных организаций и экспертиза проекта профессионального стандарта – не менее 20 организаций.

5.5. Обобщение и анализ замечаний и предложений по проекту профессионального стандарта, поступивших от экспертов и организаций, внесение в них необходимых изменений. Оформление результатов экспертизы.

Этап 6. Согласование проекта профессионального стандарта.

6.1. Организация и проведение согласования проекта профессионального стандарта с федеральными органами исполнительной власти, осуществляющими функции по выработке государственной политики и нормативно-правовому регулированию в соответствующей сфере информационной безопасности и иными заинтересованными федеральными органами исполнительной власти (при наличии в проекте профессионального стандарта трудовых функций, особо регулируемых законодательством).

Этап 7. Утверждение проекта профессионального стандарта.

7.1. Организация работы по доработке проекта ПС по результатам общественного обсуждения проектов профессиональных стандартов и их рассмотрения федеральными органами исполнительной власти, осуществляющими функции по выработке государственной политики и нормативно-правовому регулированию в соответствующей сфере информационной безопасности, организованного Минтрудом России (при наличии замечаний).

7.2. Устранение замечаний, поступивших в ходе рассмотрения **проекта профессионального стандарта** на заседании Национального совета при Президенте Российской Федерации по профессиональным квалификациям (при наличии).

Для реализации обозначенной технологической «дорожной карты» разработки ПС была определена система методических приемов, с помощью которых можно выполнить эту задачу. Предлагается выделить четыре группы методических приемов (таблица 1).

Таблица 1

Группы методов по разработке профессиональных стандартов

Системный анализ практической деятельности	**Нормативное проектирование деятельности**	**Прогнозирование деятельности специалиста по ЗИ**	**Экспертный метод**
наблюдение; хронометраж; анализ перечня должностей и функциональных обязанностей сотрудника; анкетирование; беседа; анализ отзывов на выпускников.	анализ нормативных документов (законов, приказов, инструкций и т.д.); анализ литературы, НИР; анализ функциональных классификаторов, функциональных систем; моделирование.	анализ документов, содержащих концепции и прогнозы в области теории и практики обеспечения ИБ; опрос; анализ вероятных изменений в профессиональной деятельности специалиста по ЗИ.	экспертная оценка результатов; экспертная проверка результатов.

Первая группа предназначена для системного анализа практической деятельности выпускника. Она включает в себя: наблюдение; хронометраж профессиональных функций, выполняемых специалистами по защите информации, с оценкой их значимости; "фотографирование" и "самофотографирование" рабочего дня специалистов; анкетирование выпускников и руководителей подразделений по обеспечению ИБ; анализ данных интервью, бесед с руководителями предприятий и организаций; анализ результатов расследования правонарушений в сфере ИБ; анализ отзывов на выпускников.

Вторая группа обеспечивает нормативное проектирование деятельности специалиста по защите информации. Это достигается на основе: анализа нормативных правовых документов (законов, указов, доктрин, концепций, международных и отраслевых стандартов в области информационной безопасности, служебных инструкций, положений, приказов); изучения литературы в области обеспечения ИБ и научно-исследовательских работ; проработки федеральных классификаторов, квалификационных справочников по специальностям и функциональных схем по родственным специальностям; моделирования профессиональной деятельности.

С помощью **третьей группы** методов достигается прогнозирование деятельности специалиста. При этом осуществляется: анализ прогнозных документов (федеральных, ведомственных, региональных, корпоративных), содержащих концепции и прогнозы в области ИБ, научно-технического прогресса; опрос; прогнозирование вероятных изменений в видах профессиональной деятельности специалиста по защите информации и его профессионального роста, анализ опыта подготовки зарубежных специалистов в области информационной безопасности.

Четвертая группа базируется на методе экспертных оценок, который позволяет как выявлять, так и оценивать необходимые результаты и положения в интересах разработки ПС. Более того, этот метод органично может входить во вторую и в третью группу.

2.3. 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. Указ Президента Российской Федерации от 12 мая 2009 г. № 537 «О Стратегии национальной безопасности Российской Федерации до 2020 года».
2. Указ Президента Российской Федерации от 15 января 2013 г. № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации».
3. Указ Президента Российской Федерации от 6 марта 1997г. № 188 «Об утверждении перечня сведений конфиденциального характера» (в ред. Указа Президента Российской Федерации от 23 сентября 2005г. № 1111).
4. Указ Президента Российской Федерации от 30 мая 2005г. № 609 «Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела».
5. Указ Президента Российской Федерации от 3 апреля 1995г. № 334 «О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации (в ред. Указа Президента Российской Федерации от 25 июля 2000г. №1358)».
6. Указ Президента Российской Федерации от 17 марта 2008г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».
7. Указ Президента Российской Федерации от 16 августа 2004г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю» (Выписка).
8. Указ Президента Российской Федерации от 16 апреля 2014 г. №249 «О Национальном совете при Президенте Российской Федерации по профессиональным квалификациям».
9. Федеральный Закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
10. Федеральный Закон от 11 июля 2011г. № 200-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального Закона «Об информации, информационных технологиях и о защите информации».
11. Федеральный Закон от 19 декабря 2005г. № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных».
12. Федеральный Закон от 27 июля 2006г. № 152-ФЗ «О персональных данных».
13. Федеральный Закон от 29 июля 2004г. № 98-ФЗ «О коммерческой тайне».

14. Федеральный закон от 2 декабря 1990г. № 395-1 «О банках и банковской деятельности».

15. Федеральный закон от 4 мая 2011г. № 99-ФЗ «О лицензировании отдельных видов деятельности».

16. Федеральный закон от 6 апреля 2011г. № 63-ФЗ «Об электронной подписи».

17. Федеральный Закон от 10 января 2002 г. № 1-ФЗ «Об электронной цифровой подписи».

18. Федеральный закон от 27 декабря 2002г. № 184-ФЗ «О техническом регулировании».

19. Закон Российской Федерации от 21 июля 1993г. № 5485-1 «О государственной тайне».

20. Федеральный закон от 28 декабря 2010г. № 390-ФЗ «О безопасности».

21. Федеральный закон от 3 апреля 1995г. № 40-ФЗ «О Федеральной службе безопасности».

22. Федеральный закон от 7 июля 2003г. № 126-ФЗ «О связи».

23. Федеральный закон от 27 июля 2004г. № 79-ФЗ «О государственной гражданской службе Российской Федерации».

24. Федеральный закон от 27 мая 1996 г. №57-ФЗ «О государственной охране» (с изменениями и дополнениями).

25. Федеральный закон от 31 мая 2001 г. №73-ФЗ «О государственной судебно-экспертной деятельности в Российской Федерации» (с изменениями и дополнениями).

26. Постановление Правительства Российской Федерации от 16 марта 2009г. № 228 «О федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций».

27. Постановление Правительства Российской Федерации от 15 сентября 2008г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

28. Постановление Правительства Российской Федерации от 1 ноября 2012г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

29. Постановление Правительства Российской Федерации от 16 апреля 2012г. № 313 «Об утверждении Положения о лицензирования деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)».

30. Постановление Правительства Российской Федерации от 31 августа 2006г. № 532 «О лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации».

31. Постановление Правительства Российской Федерации от 3 февраля 2012г. № 79 «О лицензировании деятельности по технической защите конфиденциальной информации».

32. Постановление Совета Министров – Правительства Российской Федерации от 15 сентября 1993г. № 912-51 «Об утверждении Положения о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам» (Извлечения).

33. Постановление Правительства Российской Федерации от 18 мая 2009г. № 424 «Об особенностях подключения федеральных государственных информационных систем к информационно-телекоммуникационным сетям».

34. Постановление Правительства Российской Федерации от 15 мая 2010г. № 330 «Об особенностях оценки соответствия продукции (работ, услуг),используемой в целях защиты сведений, относимых к охраняемой в соответствии с законодательством Российской Федерации информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, а также процессов ее проектирования (включая изыскании), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации, утилизации и захоронения, об особенностях аккредитации органов по сертификации и испытательных лабораторий (центров), выполняющих работы по подтверждению соответствия указанной продукции (работ, услуг)».

35. Постановление Правительства Российской Федерации от 26 июня 1995г. № 608 «О сертификации средств защиты информации».

36. Постановление Правительства Российской Федерации от 21.04.2010 № 266 «Об особенностях оценки соответствия продукции (работ, услуг), используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа, и продукции (работ, услуг), сведения о которой составляют государственную тайну, предназначенной для эксплуатации в загранучреждениях Российской Федерации, а также процессов ее проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации, утилизации и захоронения, об особенностях аккредитации органов по сертификации и испытательных лабораторий (центров), выполняющих работы по подтверждению соответствия указанной продукции (работ, услуг), и о внесении изменения в Положение о сертификации средств защиты информации».

37. Постановление Правительства Российской Федерации от 3 ноября 1994г. № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти».

38. Постановление Правительства Российской Федерации от 21 марта 2012г. №211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным Законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

39. «Об утверждении Методических рекомендаций по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации», утверждены Приказом ФСБ Российской Федерации 21 февраля 2008г. № 149/54-144.

40. «Об утверждении типовых требований по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных», утверждены Приказом ФСБ Российской Федерации 21 февраля 2008 г. № 149/6/6-622.

41. Приказ ФСБ Российской Федерации от 9 февраля 2005г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)».

42. Распоряжение Правительства Российской Федерации от 29 ноября 2012 года №2204-р «Об утверждении плана разработки профессиональных стандартов на 2012 – 2015 годы».

43. Приказ Министерства труда и социальной защиты Российской Федерации от 30 ноября 2012 года № 565 «Об утверждении плана-графика подготовки профессиональных стандартов в 2013 – 2014 годах».

44. Закон «О внесении изменений в Трудовой кодекс Российской Федерации (в части законодательного определения понятия профессионального стандарта, порядка его разработки и утверждения)».

45. Постановление Правительства Российской Федерации от 22 января 2013 г. № 23 «О Правилах разработки, утверждения и применения профессиональных стандартов».

46. Распоряжение Правительства Российской Федерации от 31 марта 2014 г. № 487-р (Комплексный план мероприятий по разработке профессиональных стандартов, их независимой профессионально-общественной экспертизе и применению на 2014 - 2016 годы).

47. Общероссийский классификатор специальностей по образованию ОК 009-2003 (ОКСО) (принят и введен в действие постановлением Госстандарта РФ от 30 сентября 2003 г. №276-ст) (с изменениями и дополнениями).

48. Приказ Министерства образования и науки РФ от 12 января 2005 г. №4 «Об утверждении перечня направлений подготовки (специальностей) высшего профессионального образования» (с изменениями и дополнениями).

49. Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ от 9 сентября 2000 г. №Пр-1895).

50. Постановление Правительства РФ от 17 ноября 2007 г. №781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».

51. Приказ Федеральной службы по тарифам от 31 июля 2010 г. №340-к «Об утверждении Перечня должностей государственной гражданской службы ФСТ России, исполнение должностных обязанностей по которым связано с использованием сведений, составляющих государственную тайну, при назначении на которые конкурс в соответствии с частью 3 статьи 22 Федерального закона от 27 июля 2004 г. №79-ФЗ «О государственной гражданской службе Российской Федерации» может не проводиться».

52. Распоряжение Правления ПФР от 11 октября 2007 г. №190р «О внедрении защищенного электронного документооборота в целях реализации законодательства Российской Федерации об обязательном пенсионном страховании» (с изменениями и дополнениями).

53. Трудовой кодекс Российской Федерации от 30 декабря 2001 г. №197-ФЗ (ТК РФ) (с изменениями и дополнениями).

54. Приказ Министерства связи и массовых коммуникаций РФ от 25 августа 2009 г. №1 04 «Об утверждении Требований по обеспечению целостности, устойчивости функционирования и безопасности информационных систем общего пользования».

55. Приказ Министерства здравоохранения и социального развития РФ от 22 апреля 2009 г. №205 «Об утверждении Единого квалификационного справочника должностей руководителей, специалистов и служащих, раздел «Квалификационные характеристики должностей руководителей и специалистов по обеспечению безопасности информации в ключевых системах информационной инфраструктуры, противодействию техническим разведкам и технической защите информации».

56. Приказ ФСТЭК Российской Федерации, ФСБ Российской Федерации, Министерства информационных технологий и связи Российской Федерации от 13 февраля 2008г. № 55/86/20 «Об утверждении порядка проведения классификации информационных систем персональных данных», зарегистрирован в Министерстве юстиции Российской Федерации 3 апреля 2008г. № 11462.

57. «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утверждена Заместителем директора ФСТЭК России 14 февраля 2008г.

58. «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка)», утверждена Заместителем директора ФСТЭК России 15 февраля 2008г.

59. «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных», утверждено Приказом ФСТЭК Российской Федерации от 5 февраля 2010г. № 58, зарегистрировано в Министерстве юстиции Российской Федерации 19 февраля 2010г. № 16456.

60. «Методические рекомендации по технической защите информации, составляющей коммерческую тайну», утверждены Заместителем директора ФСТЭК России 25 декабря 2006г.

61. «Пособие по организации технической защиты информации, составляющей коммерческую тайну», утверждены Заместителем директора ФСТЭК России 25 декабря 2006г.

62. «Положение о сертификации средств защиты информации по требованиям безопасности информации», утверждено приказом председателя Государственной технической комиссии при Президенте Российской Федерации от 27 октября 1995г. № 199.

63. «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)», утверждены приказом председателя Государственной технической комиссии при Президенте Российской Федерации от 30 августа 2002г. № 282.

64. «Положение по аттестации объектов информатизации по требованиям безопасности информации», утверждено председателем Государственной технической комиссии при Президенте Российской Федерации 25 ноября 1994 г.

65. «Методические рекомендации управлениям ФСТЭК России по федеральным округам об организации работ по аттестации объектов информатизации по требованиям безопасности информации», утверждены заместителем директора ФСТЭК России 25 апреля 2006г.

66. «Сборник временных методик оценки защищённости конфиденциальной информации, обрабатываемой техническими средствами и системами», утверждены приказом председателя Государственной технической комиссии при Президенте Российской Федерации, 2001г.

67. «Сборник руководящих документов по защите информации от НСД», утверждены приказом председателя Государственной технической комиссии при Президенте Российской Федерации, 1998г.

68. «Методические документы по обеспечению безопасности информации в ключевых системах информационной инфраструктуры», утверждены Заместителем директора ФСТЭК России 18 мая 2007г. и 19 ноября 2007г.

69. «Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Часть 1, Часть 2, Часть3», утвержден приказом председателя Гостехкомиссии России от 19 июня 2002г. №187.

70. «Руководящий документ. Безопасность информационных технологий. Положение по разработке профилей защиты и заданий по безопасности», Гостехкомиссия России, 2003г.

71. «Руководящий документ. Безопасность информационных технологий. Руководство по регистрации профилей защиты», Гостехкомиссия России, 2003г.

72. «Руководящий документ. Безопасность информационных технологий. Руководство по формированию семейств профилей защиты», Гостехкомиссия России, 2003г.

73. «Руководство по разработке профилей защиты и заданий по безопасности», Гостехкомиссия России, 2003г.

74. «Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности», введен в действие Приказом Гостехкомиссии России от 19 июня 2002г. № 187.

75. «Сборник временных методик оценки защищённости конфиденциальной информации от утечки по техническим каналам», утвержден первым заместителем председателя Гостехкомиссии России 8 ноября 2001г.

76. «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», ФСТЭК России, 2008г., пометка «для служебного пользования» снята Решением ФСТЭК России от 16 ноября 2009г.

77. «Общие требования по обеспечению безопасности информации в ключевых системах информационной инфраструктуры», утверждены заместителем директора ФСТЭК России 18 мая 2007г.

78. «Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры», утверждены заместителем директора ФСТЭК России 18 мая 2007г.

79. «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка)», (при рассмотрении угроз утечки информации по каналам побочных электромагнитных излучений и наводок (ПЭМИН) необходимо применять полную версию данного документа), ФСТЭК России, 2008г.

80. «Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры», утверждены заместителем директора ФСТЭК России 18 мая 2007г.

81. «Рекомендации по обеспечению безопасности информации в ключевых системах информационной инфраструктуры», утверждены заместителем директора ФСТЭК России 19 ноября 2007г.

82. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

83. ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. Госстандарт России

84. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. Госстандарт России

85. ГОСТ Р 51188-98. Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство. Госстандарт России

86. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Госстандарт России

87. ГОСТ Р 51583-2014. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения

88. ГОСТ Р 51624-2000. Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования

89. ГОСТ Р 52069-2003. Защита информации. Система стандартов. Основные положения

90. ГОСТ Р 53131-2008 (ИСО/МЭК ТО 24762-2008). Защита информации. Рекомендации по услугам восстановления после чрезвычайных ситуаций функций и механизмов безопасности информационных и телекоммуникационных технологий. Общие положения

91. ГОСТ Р ИСО 7498-1-99. Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель. Госстандарт России

92. ГОСТ Р ИСО 7498-2-99. Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. Госстандарт России

93. 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

94. ГОСТ Р ИСО/МЭК ТО 13335-3-2007. Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий

95. ГОСТ Р ИСО/МЭК ТО 13335-4-2007. Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер

96. ГОСТ Р ИСО/МЭК ТО 13335-5-2007. Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети.

97. ГОСТ Р ИСО/МЭК 15408-1-2008. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Госстандарт России

98. ГОСТ Р ИСО/МЭК 15408-2-2008. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности. Госстандарт России

99. ГОСТ Р ИСО/МЭК 15408-3-2008. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности. Госстандарт России

100. ГОСТ Р ИСО/МЭК ТО 15443-1-2011. Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к безопасности ИТ. Часть 1. Обзор и основы

101. ГОСТ Р ИСО/МЭК ТО 15443-2-2011. Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к безопасности ИТ. Часть 2. Методы доверия

102. ГОСТ Р ИСО/МЭК ТО 15443-3-2011. Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к безопасности ИТ. Часть 3. Анализ методов доверия.

103. ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Методы и средства обеспечения безопасности. Практические правила управления информационной безопасностью

104. ГОСТ Р ИСО/МЭК 18028-1-2008. Информационная технология. Методы и средства обеспечения безопасности. Сетевая безопасность информационных технологий. Менеджмент сетевой безопасности

105. ГОСТ Р ИСО/МЭК ТО 19791-2008. Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем

106. ГОСТ Р ИСО/МЭК 27001-2006. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования

107. ГОСТ Р ИСО/МЭК 27004-2011. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения

108. ГОСТ Р ИСО/МЭК 27005-2009. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности

109. ГОСТ Р ИСО/МЭК 27033-1-2011. Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции

Таблица 2

Базовые нормативные документы, использованные при разработке стандарта

Нормативный документ	Элемент ПС
Федеральный Закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»	ОТФ D, ОТФ B, ТД, знания и умения в C/03.6, D/04.7
Постановление Правительства Российской Федерации от 16 апреля 2012г. № 313	ТД, знания и умения в E/01.8, E/03.8, D/04.7
Постановление Правительства Российской Федерации от 3 февраля 2012г. № 79	ТД, знания и умения в E/01.8, E/02.8, B/06.6, D/04.7
Постановление Правительства РФ от 3 марта 2012 г. № 171	ТД, знания и умения в E/01.8, E/02.8 и E/03.8, D/04.7
Приказ ФСТЭК №17 раздел 14	ОТФ E, ТФ E/01.8, E/02.8, E/03.8, ТД в ТФ E/01.8
Приказ ФСТЭК №17 раздел 14.1	ТД, знания и умения в E/01.8
Приказ ФСТЭК №17 раздел 14.2	ТД, знания и умения в E/01.8
Приказ ФСТЭК №17 раздел 15	ОТФ D
Приказ ФСТЭК №17 раздел 15.1	ТД, знания и умения в D/02.7, D/04.7
Приказ ФСТЭК №17 раздел 15.2	ТФ D/03.7, ТД, знания и умения в C/02.6
Приказ ФСТЭК №17 раздел 15.3	ТФ D/01.7, ТД, знания и умения в D/02.7, D/03.7
Приказ ФСТЭК №17 раздел 16	ОТФ C
Приказ ФСТЭК №17 раздел 16.1	ТФ C/01.6
Приказ ФСТЭК №17 раздел 16.2	ТФ C/02.6
Приказ ФСТЭК №17 раздел 16.3	ТФ C/04.6
Приказ ФСТЭК №17 раздел 16.4	ТД, знания и умения в ТФ C/01.6, C/03.6, C/04.6
Приказ ФСТЭК №17 раздел 16.5	ТД, знания и умения в ТФ C/03.6, C/04.6, B/01.6
Приказ ФСТЭК №17 раздел 16.6	ТД, знания и умения в ТФ C/03.6
Приказ ФСТЭК №17 раздел 16.7	ТД, знания и умения в ТФ C/01.6
Приказ ФСТЭК №17 раздел 18	ОТФ B
Приказ ФСТЭК №17 раздел 18.1	ТФ B/01.6, ТФ B/02.6
Приказ ФСТЭК №17 раздел 18.2	ТФ B/03.6, ТФ B/04.6
Приказ ФСТЭК №17 раздел 18.3	ТФ B/06.6, ТД, знания и умения в ТФ B/03.6, B/04.6, B/05.6

Приказ ФСТЭК №17 раздел 18.4	ТФ B/05.6, ТФ A/02.5
Приказ ФСТЭК №17 раздел 19	ОТФ A
Приказ ФСТЭК №17 раздел 19.1	ТД, знания и умения в ТФ A/03.5
Приказ ФСТЭК №17 раздел 19.2	ТФ A/01.5, ТД, знания и умения в ТФ A/01.5
ГОСТ Р 51583-2014 раздел 6.1	ОТФ E
ГОСТ Р 51583-2014 раздел 6.3	ТФ E/01.8
ГОСТ Р 51583-2014 раздел 6.3.1	ТФ E/02.8, ТД, знания и умения в E/01.8
ГОСТ Р 51583-2014 раздел 6.3.2	ТФ E/03.8 и E/04.8, ТД в E/01.8, ТД, знания и умения в E/02.8 и E/03.8
ГОСТ Р 51583-2014 раздел 6.3.3	ТД в E/01.8
ГОСТ Р 51583-2014 раздел 6.4	ТД, знания и умения в в E/02.8 и E/03.8
ГОСТ Р 51583-2014 раздел 6.5	ТД, знания и умения в в D/02.7
ГОСТ Р 51583-2014 раздел 6.6	ТД, знания и умения в E/02.8
ГОСТ Р 51583-2014 раздел 6.7	ТД, знания и умения в D/02.7 и D/04.7
ГОСТ Р 51583-2014 раздел 6.8	ТД, знания и умения в E/03.8
ГОСТ Р 51583-2014 раздел 6.9	ТД, знания и умения в E/03.8, D/03.7, A/02.5, C/02.6
ГОСТ Р 51583-2014 раздел 6.10	ТД, знания и умения в E/03.8, D/03.7, D/04.7
ГОСТ Р 51583-2014 разделы 6.11 и 6.12	ТФ C/02.6, ТФ C/04.6
ГОСТ Р 51583-2014 раздел 6.13	ТД, знания и умения в C/01.6, C/03.6 , C/04.6
ГОСТ Р 51583-2014 раздел 6.15	ТД, знания и умения в A/01.5, C/02.6
ГОСТ ИСО/МЭК 27001-2006	ТД, знания и умения в E/01.8
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	ТД, знания и умения в B/03.6, E/03.8
ГОСТ Р ИСО/МЭК ТО 13335-3-2007. Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий	ТД, знания и умения в D/02.7, D/04.7
ГОСТ ИСО/МЭК 13335-4 2007. Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер	ТД, знания и умения в E/01.8
ГОСТ Р ИСО/МЭК ТО 13335-5-2007. Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети	ТД, знания и умения в C/03.6, E/03.8
Методические рекомендации, утвержденные приказом 8 Центра ФСБ №149/54 от 21.02.2008	ТД, знания и умения в E/01.8
ГОСТ Р ИСО/МЭК ТО 19791-2008. Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем	ТД, знания и умения в E/02.8, B/01.6
ГОСТ Р 51188-98. Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство. Госстандарт России	C/03.6, ТД, знания и умения в B/05.6, C/03.6

ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Госстандарт России	ТД, знания и умения в E/04.8, D/02.7
ГОСТ Р 53131-2008 (ИСО/МЭК ТО 24762-2008). Защита информации. Рекомендации по услугам восстановления после чрезвычайных ситуаций функций и механизмов безопасности информационных и телекоммуникационных технологий. Общие положения	ТФ B/04.6
ГОСТ Р ИСО 7498-2-99. Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Госстандарт России	ТД, знания и умения в B/01.6, C/03.6, D/02.7
ГОСТ Р ИСО/МЭК 15408-1-2008. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Госстандарт России	ТД, знания и умения в E/02.8, E/04.8
ГОСТ Р ИСО/МЭК 15408-2-2008. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности. Госстандарт России	ТД, знания и умения в D/02.7, B/06.6, E/04.8
ГОСТ Р ИСО/МЭК 15408-3-2008. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности. Госстандарт России	ТД, знания и умения в D/04.7, E/04.8
ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Методы и средства обеспечения безопасности. Практические правила управления информационной безопасностью	ТД, знания и умения в B/03.6
ГОСТ Р ИСО/МЭК 27005-2009. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности	ТД, знания и умения в B/03.6, B/06.6

Элементы ПС: ОТФ (обобщенная трудовая функция), ТФ (трудовая функция), ТД (трудовое действие), знания, умения.

Раздел 3 **«Обсуждение проекта профессионального стандарта»**

К разработке проекта профессионального стандарта «Специалист по защите информации в автоматизированных системах» 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 (70человек)
образовательных организаций СПО: 1 (1 человек);
образовательных организаций ДПО: 9 (14человек);
коммерческих организаций: 5 (6 человек)
представителей ФОИВ: 6 ФОИВ (15человек);

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 (7человек);
образовательных организаций ДПО: 4 (13человек);
коммерческих организаций: 7 (10 человек);
представителей ФОИВ: 3 ФОИВ (5человек);

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 (20человек);
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» А.В. Солодянников
____ _____ 2015 г.