Пояснительная записка к проекту профессионального стандарта «Специалист по безопасности компьютерных систем и сетей»

Оглавление

Раздел 1 "Общая характеристика вида профессиональной деятельности, трудовых функций"

1.1. Информация о перспективах развития вида профессиональной деятельности.

Профессиональный стандарт «**Специалист по безопасности компьютерных систем и сетей**» 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».

Стандарт относится к группе профессиональных стандартов в области информационной безопасности и охватывает такие сферы деятельности, как разработка, внедрение, эксплуатация, экспертиза и менеджмент средств и систем обеспечения информационной безопасности компьютерных систем и сетей. Основная цель вида профессиональной деятельности – обеспечение

защиты информации в компьютерных системах и сетях в условиях существования угроз их информационной безопасности.

Обеспечение информационной безопасности компьютерных систем и сетей (компьютерной безопасности) является многогранным и сложным видом профессиональной деятельности, требующим реализации скоординированных мероприятий по следующим направлениям:

1. Безопасность компьютерных систем, сетей и баз данных.
2. Безопасность распределенных компьютерных систем.
3. Безопасность высокопроизводительных вычислительных систем.
4. Программное обеспечение систем защиты информации.
5. Администрирование систем защиты информации компьютерных систем.
6. Разработка средств защиты компьютерной информации.
7. Контрольно-аналитическая экспертиза и анализ защищенности компьютерных систем.
8. Сертификация программно-аппаратных средств защиты компьютерной информации.
9. Информационно-аналитическая техническая экспертиза.
10. Консультирование по вопросам компьютерной безопасности.
11. Маркетинговая деятельность в области услуг, связанных с использованием программно-аппаратных средств защиты компьютерной информации.

Вид профессиональной деятельности — разработка, внедрение, эксплуатация, экспертиза и менеджмент средств и систем обеспечения информационной безопасности компьютерных систем и сетей.

В настоящее время проблема обеспечения защиты и эксплуатации информации в компьютерных системах и информационно-телекоммуникационных сетей имеет особую актуальность. По мнению Совета Безопасности Российской Федерации информационная сфера Российской Федерации является одним из основных приоритетов обеспечения национальной безопасности Российской Федерации.

В ряде стран сформированы специальные формирования (подразделения, институты, войсковые формирования, и др), в которых проводится разработка технологий создания и доставки информационного оружия и различных видов вредоносного программного обеспечения. Ежегодно проводятся национальные и международные (для стран НАТО) учения по отработке методов ведения информационных войн. В США создана специальная организация — киберкомандование, подчиненное помощнику Президента по национальной безопасности, объединяющее значительные силы и средства, координирующее свою работу с другими силовыми структурами, отрабатывающая различные сценарии компьютерных атак на национальном киберполигоне и проводящая специальные операции. В Евросоюзе также создана специальная организация ЕС3, занимающаяся вопросами безопасности киберпространства.

В качестве угроз в информационной сфере также выступают 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).

В целях противодействия использованию информационных и коммуникационных технологий для дискредитации суверенитета, нарушения территориальной целостности государства разработаны Стратегия национальной безопасности Российской Федерации до 2020 года и Доктрина информационной безопасности Российской Федерации, заложившие основы для обеспечения национальной безопасности в информационной сфере. В порядке реализации положений этих документов создается интегрированная сеть связи, предназначенная для обеспечения органов государственной власти в полном объеме услугами связи при решении задач в области обороны страны, безопасности государства и поддержания правопорядка.

Таким образом, результаты анализа актуальных тенденций в обеспечения информационной безопасности компьютерных систем и сетей, увеличения сложности и изощренности их реализации, активного применения средств компьютерной разведки и нападения многими развитыми странами,

а также преступными сообществами, создания в зарубежных странах кибервойск и киберкомандований с соответствующими крупными инвестициями в их оснащение, привлечения к участию в компьютерных атак значительного числа представителей хакерского сообщества, указывают на необходимость активизации подготовки специалистов по безопасности компьютерных систем и сетей.

Такие специалисты должны владеть широким спектром языков программирования, в том числе для серверных и сетевых 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 механизмы защиты и администрирования компьютерных систем и сетей , математические модели их построения, архитектуры построения, принципы разработки, тестирования современных программно-аппаратного обеспечения защиты информации.

Поэтому введение нового профессионального стандарта по данному виду профессиональной деятельности, охватывающего разработку, внедрение, эксплуатацию, экспертизу и менеджмент средств и систем обеспечения информационной безопасности компьютерных систем и сетей, представляется важной государственной задачей.

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, настройка и мониторинг защищенных компьютерных систем и сетей, применение методов и средств обеспечения их безопасности (ОТФ1 – уровень квалификации);

– администрирование программно-аппаратных средств защиты информации в компьютерных системах и сетях (ОТФ2 – 6 уровень квалификации);

– разработка и применение методов оценивания безопасности компьютерных систем, сертификация программного обеспечения, аттестация объектов информатизации (ОТФ3 – 7 уровень квалификации);

– Создание проектов и разработка специальных технических и программно-математических средств защиты информации компьютерных систем и сетей (ОТФ4 – 8 уровень квалификации).

ОТФ1 «обслуживание, настройка и мониторинг защищенных компьютерных систем и сетей, применение методов и средств обеспечения их безопасности» предусматривает 5уровень 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 «администрирование программно-аппаратных средств защиты информации в компьютерных системах и сетях» 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 «разработка и применение методов оценивания безопасности компьютерных систем, сертификация программного обеспечения, аттестация объектов информатизации» 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.

ОТФ4 «создание проектов и разработка специальных технических и программно-математических средств защиты информации компьютерных систем и сетей» 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	Обслуживание программно-аппаратных средств защиты информации компьютерных систем и сетей
		Обслуживание технических средств защиты информации в компьютерных системах и сетях
		Применение методов и средств защиты информации в компьютерных системах и сетях
ОТФ2	6	Администрирование подсистем защиты информации в компьютерных системах и сетях
		Приемка и внедрение программно-аппаратных средств защиты информации
		Сопровождение и обслуживание программно-аппаратных средств защиты информации
ОТФ3	7	Проведение контрольных проверок работоспособности и эффективности применяемых программно-аппаратных средств защиты информации
		Разработка требований по защите, составление политик безопасности компьютерных систем и сетей
		Проведение криминалистического анализа компьютерных систем
		Выполнение экспериментально-исследовательских работ при проведении сертификации программно-аппаратных средств защиты информации и анализ результатов
		Проведение экспериментально-исследовательских работ при аттестации объектов с учетом требований к обеспечению защищенности
		Проведение инструментального мониторинга защищенности компьютерных систем и сетей
		Проведение экспертизы при расследовании компьютерных преступлений, правонарушений и инцидентов
ОТФ4	8	Разработка требований к специальным техническим средствам защиты информации компьютерных систем с учетом действующих нормативных и методических документов
		Проектирование программных и аппаратных средств защиты информации компьютерных систем и сетей
		Разработка, отладка и тестирование средств защиты информации компьютерных систем
		Разработка, отладка и тестирование средств защиты информации компьютерных систем и сетей
		Сопровождение разработки средств защиты информации компьютерных систем и сетей

Для выполнения трудовых функций, отнесенных к ОТФ1, требуется среднее профессиональное образование по УГС (направлению подготовки) «Информационная безопасность». Для выполнения трудовых функций, отнесенных к ОТФ2, ОТФ3, ОТФ4 требуется соответствующее высшее образование либо дополнительное профессиональное образование.

ТФ «Обслуживание программно-аппаратных средств обеспечения информационной безопасности в компьютерных системах и сетях» 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 «Обслуживание программно-аппаратных средств защиты информации компьютерных систем и сетей» 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 «Применение методов и средств защиты информации в компьютерных системах и сетях» 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 «Администрирование подсистем защиты информации в компьютерных системах и сетях» 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 «Приемка и внедрение программно-аппаратных средств 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 «Сопровождение и обслуживание программно-аппаратных средств 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 «Проведение контрольных проверок работоспособности и эффективности применяемых программно-аппаратных средств 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.

ТФ «Разработка требований по защите, составление политик безопасности компьютерных систем и сетей» 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 криминалистического анализа компьютерных 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 «Выполнение экспериментально-исследовательских работ при проведении сертификации программно-аппаратных средств защиты информации и анализ результатов» 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 экспериментально-исследовательских работ при аттестации объектов с учетом требований к обеспечению защищенности» 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 инструментального мониторинга защищенности компьютерных систем и сетей» 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 экспертизы при расследовании компьютерных преступлений, правонарушений и инцидентов» 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 требований к специальным техническим средствам защиты информации компьютерных систем с учетом действующих нормативных и методических документов» 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 «Проектирование программных и аппаратных средств защиты информации компьютерных систем и сетей» 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, отладка и тестирование средств защиты информации компьютерных систем и сетей» 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 «Сопровождение разработки средств защиты информации компьютерных систем и сетей» 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:

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 эксплуатации защищенных компьютерных систем и сетей.

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

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. Формирование экспертной группы, в состав которой вошли руководители и специалисты-эксперты, специалисты в области управления, обучения и развития персонала, нормирования и охраны труда, другие специалисты (21 чел.);

1.2. Проведение анализа состояния и перспектив развития вида профессиональной деятельности с учетом отечественных и международных тенденций.

1.3. Проведение анализа нормативной, методической, учебной, технологической документации в области темы лота и по отдельным трудовым функциям специалистов в этой области.

1.4. Формирование репрезентативной выборки организаций (39 организаций, расположенных в разных федеральных округах Российской Федерации, относящихся к разным формам собственности с числом опрашиваемых работников более 100 человек).

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

2.1. Уяснение конкретной области профессиональной деятельности, для которой будет формироваться стандарт, охватываемых им квалификационных уровней и характеристик профессиональной деятельности.

2.2. Формирование проекта профессионального стандарта, его обсуждение, сбор замечаний и предложений, учет их при формировании окончательной редакции профессионального стандарта.

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 6 марта 1997г. № 188 «Об утверждении перечня сведений конфиденциального характера» (в ред. Указа Президента Российской Федерации от 23 сентября 2005г. № 1111).
3. 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».
4. 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».
5. Указ Президента Российской Федерации от 16 августа 2004г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю» (Выписка).
6. Указ Президента Российской Федерации от 16 апреля 2014 г. №249 «О Национальном совете при Президенте Российской Федерации по профессиональным квалификациям».
7. Федеральный Закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
8. 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».
9. Федеральный Закон от 19 декабря 2005г. № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных».
10. Федеральный Закон от 27 июля 2006г. № 152-ФЗ «О персональных данных».
11. Федеральный Закон от 29 июля 2004г. № 98-ФЗ «О коммерческой тайне».
12. Федеральный закон от 2 декабря 1990г. № 395-1 «О банках и банковской деятельности».
13. Федеральный закон от 4 мая 2011г. № 99-ФЗ «О лицензировании отдельных видов деятельности».
14. Федеральный закон от 6 апреля 2011г. № 63-ФЗ «Об электронной подписи».
15. Федеральный Закон от 10 января 2002 г. № 1-ФЗ «Об электронной цифровой подписи».
16. Федеральный закон от 27 декабря 2002г. № 184-ФЗ «О техническом регулировании».
17. Закон Российской Федерации от 21 июля 1993г. № 5485-1 «О государственной тайне».
18. Федеральный закон от 28 декабря 2010г. № 390-ФЗ «О безопасности».

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

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

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

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

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

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

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

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

27. 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)».

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

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

30. 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).

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

32. 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)».

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

34. 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».

35. 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».

36. 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».

37. «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.

38. «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. N 149/6/6-622.

39. 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)».

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

41. 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».

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

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

44. 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).

45. 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).

46. 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).

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

48. 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».

49. 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».

50. 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).

51. Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. №195-ФЗ (КоАП РФ) (с изменениями и дополнениями).

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

53. 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».

54. 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».

55. 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.

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

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

58. «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.

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

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

61. «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.

62. «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.

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

64. «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.

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

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

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

68. «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.

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

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

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

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

73. «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.

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

75. «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.

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

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

78. «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.

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

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

81. Приказ ФСТЭК России от 11 февраля 2013 г. N 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

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

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

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

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

86. ГОСТ Р 51583-2000. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения

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

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

89. 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

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

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

92. 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

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

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

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

96. 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

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

98. 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

99. 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

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

101. 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.

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

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

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

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

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

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

108. 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 «Специалист по безопасности компьютерных систем и сетей»

Нормативный документ	**Элемент ПС**
Федеральный Закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»	знания и умения ТФ A/01.05, ТФ A/02.05, ТФ B/01.05, ТФ B/02.05
Постановление Правительства Российской Федерации от 16 апреля 2012г. № 313	ТФ C/07.7, ТФ C/04.7, ОТФ D
Постановление Правительства Российской Федерации от 3 февраля 2012г. № 79 «О лицензировании деятельности по технической защите конфиденциальной информации».	ТФ C/01.7, ТФ C/02.7, ТФ D/01.8
Постановление Правительства РФ от 03.03.2012 N 171 "О лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации"	ОТФ D, ТФ D/01.8, ТФ D/02.8, ТФ D/04.8
Приказ ФСТЭК №17 раздел 19	ОТФ A, ОТФ B, знания и умения в ТФ A/01.5, ТФ A/02.5, ТФ B/01.5, ТФ B/02.5,
Приказ ФСТЭК №17 раздел 17	ОТФ C,
Приказ ФСТЭК №17 раздел 16	ОТФ A, ОТФ B, ОТФ C
Приказ ФСТЭК №17 раздел 18	ОТФ C
Приказ ФСТЭК №17 раздел 15	ОТФ D
Приказ ФСТЭК №17 раздел 14.1, 14.2	ТФ D/01.8
ГОСТ Р 51583-2014 раздел 6.1	ТФ D/01.8, знания и умения в ТФ D/01.8
ГОСТ Р 51583-2014 раздел 6.3	ТФ D/02.8, знания и умения в ТФ D/02.8
ГОСТ Р 51583-2014 раздел 6.4	ТФ D/01.8
ГОСТ ИСО/МЭК 27001-2006	ТД, знания и умения D/01.8, ТФ D/04.8
ГОСТ ИСО/МЭК 13335-4-2007	ТД, знания и умения D/01.8, ТФ D/04.8
ГОСТ ИСО/МЭК 13335-3-2007	ТФ C/03.7, ТФ C/04.7, знания и умения ТФ C/02.7, C/03.7, C/04.7
ГОСТ ИСО/МЭК 13335-1-2006	ТФ C/03.7, ТФ C/04.7, знания и умения ТФ C/02.7, C/03.7, C/04.7

Нормативный документ	Элемент ПС
ГОСТ Р ИСО/МЭК 27004-2011. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения	ТФ С/03.7, ТФ С/04.7, знания и умения ТФ С/02.7, С/03.7, С/04.7
Указ Президента Российской Федерации от 12 мая 2009 г. № 537 «О Стратегии национальной безопасности Российской Федерации до 2020 года»	ОТФ D
Постановление Правительства Российской Федерации от 15 мая 2010г. № 330	ТФ С/03.7, ТФ С/04.7, ТФ С/05.7
Постановление Правительства Российской Федерации от 18 мая 2009г. № 424 «Об особенностях подключения федеральных государственных информационных систем к информационно-телекоммуникационным сетям»	ТФ D/01.2, ТФ С/02.8, знания и умения в D/01.2 и ТФ D/02.8
Постановление Правительства Российской Федерации от 26 июня 1995г. № 608 «О сертификации средств защиты информации»	ТФ С/03.7, ТФ С/04.7, ТД, знания и умения ТФ С/04.7
«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	ТФ С/03.7, ТФ С/04.7, ТД, знания и умения ТФ С/04.7
«Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры», утверждены заместителем директора ФСТЭК России 18 мая 2007г	знания и умения ТФ С/01.7, ТФ С/02.7 ТФ D/01.8, ТФ D/02.8
«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	знания и умения ТФ С/01.7, ТФ С/02.7 ТФ D/01.8, ТФ D/02.8
ГОСТ Р ИСО/МЭК 27033-1-2011. Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции	знания и умения ТФ С/01.7, ТФ С/02.7, ТФ С/03.7

Раздел 3 «Обсуждение проекта профессионального стандарта»

К разработке проекта профессионального стандарта «Специалист по безопасности компьютерных систем и сетей» 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.