По­яс­ни­тель­ная за­пис­ка к про­ек­ту про­фес­сио­наль­но­го стан­дар­та

**«Специалист по безопасности компьютерных систем и сетей»**

**Ог­лав­ле­ние**

[ПОЯСНИТЕЛЬНАЯ ЗАПИСКА К ПРОЕКТУ ПРОФЕССИОНАЛЬНОГО СТАНДАРТА 1](#_Toc433721218)

[**«СПЕЦИАЛИСТ ПО БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ И СЕТЕЙ»** 1](#_Toc433721219)

[РАЗДЕЛ 1 "ОБЩАЯ ХАРАКТЕРИСТИКА ВИДА ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ, ТРУДОВЫХ ФУНКЦИЙ" 1](#_Toc433721220)

[1.1. ИНФОРМАЦИЯ О ПЕРСПЕКТИВАХ РАЗВИТИЯ ВИДА ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ. 1](#_Toc433721221)

[1.2. ОПИСАНИЕ ОБОБЩЕННЫХ ТРУДОВЫХ ФУНКЦИЙ, ВХОДЯЩИХ В ВИД ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ. 3](#_Toc433721222)

[1.3. ОПИСАНИЕ СОСТАВА ТРУДОВЫХ ФУНКЦИЙ И ОБОСНОВАНИЕ ИХ ОТНЕСЕНИЯ К КОНКРЕТНЫМ УРОВНЯМ (ПОДУРОВНЯМ) КВАЛИФИКАЦИИ. 4](#_Toc433721223)

[РАЗДЕЛ 2 «ОСНОВНЫЕ ЭТАПЫ РАЗРАБОТКИ ПРОЕКТА ПРОФЕССИОНАЛЬНОГО СТАНДАРТА» 7](#_Toc433721224)

[2.1. ИНФОРМАЦИЯ ОБ ОРГАНИЗАЦИЯХ, НА БАЗЕ КОТОРЫХ ПРОВОДИЛИСЬ ИССЛЕДОВАНИЯ, И ОБОСНОВАНИЕ ВЫБОРА ЭТИХ ОРГАНИЗАЦИЙ 7](#_Toc433721225)

[2.2. ЭТАПЫ РАЗРАБОТКИ ПРОЕКТА ПРОФЕССИОНАЛЬНОГО СТАНДАРТА. 7](#_Toc433721226)

[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). 10](#_Toc433721227)

[РАЗДЕЛ 3 «ОБСУЖДЕНИЕ ПРОЕКТА ПРОФЕССИОНАЛЬНОГО СТАНДАРТА» 18](#_Toc433721228)

[3.1. ИНФОРМАЦИЯ О ПОРЯДКЕ ОБСУЖДЕНИЯ 18](#_Toc433721229)

# "Общая характеристика вида профессиональной деятельности, трудовых функций"

## 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 EC3, 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.

## 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.

## 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.

# «Основные этапы разработки проекта профессионального стандарта»

## 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.

## 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.

## 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 С/07.7, ТФ С/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 С/03.7, ТФ С/04.7, знания и умения ТФ С/02.7, С/03.7, С/04.7 |
| ГОСТ ИСО/МЭК 13335-1-2006 | ТФ С/03.7, ТФ С/04.7, знания и умения ТФ С/02.7, С/03.7, С/04.7 |
| 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 C/03.7, ТФ C/04.7, ТД, знания и умения ТФ C/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 C/03.7, ТФ C/04.7, ТД, знания и умения ТФ C/04.7 |
| «Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры», утверждены заместителем директора ФСТЭК России 18 мая 2007г | знания и умения ТФ C/01.7, ТФ C/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 C/01.7, ТФ C/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 C/01.7, ТФ C/02.7, ТФ C/03.7 |

# «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.

## 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.