Стандартизация в информационной безопасности

Владимир Голованов
заместитель начальника аналитического отдела

Алексей Фатеев
специалист аналитического отдела

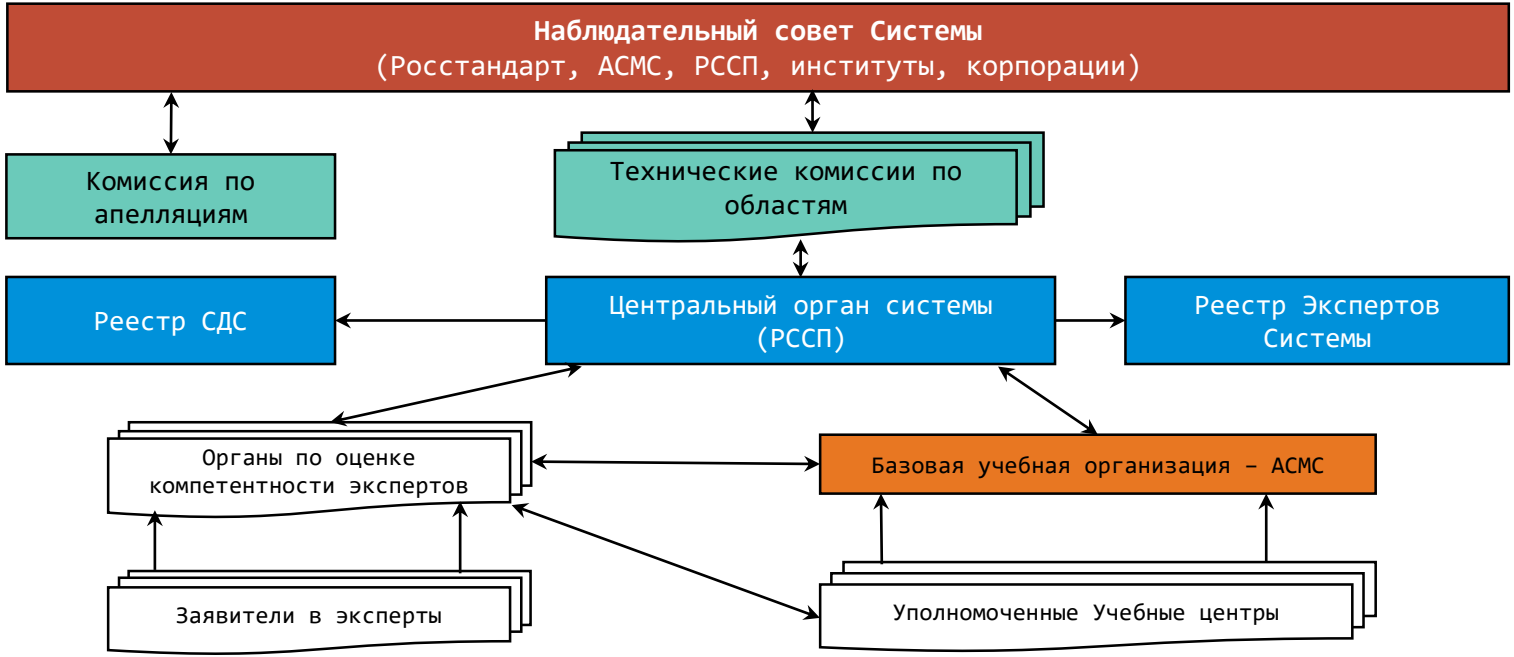
infotecs

Введение

Действующая система подготовка кадров в области стандартизации в РФ

- Среднее профессиональное образование (по ФГОС СПО) – направление 27.00.00, квалификация «техник»
- Высшее образование (по ФГОС ВО) – направление 27.00.00, бакалавриат, магистратура, аспирантура
- Дополнительное профессиональное образование (по программам ДПО и переподготовки) – Академия стандартизации, метрологии и сертификации и другие аккредитованные организации

Пример. Система сертификации персонала РОСС RU.Е177.04ЭР00



из Правил функционирования СДС экспертов стандартизации

Система сертификации персонала РОСС RU.Е177.04ЭР00. Документы

Сертификат компетентности эксперта по стандартизации


СИСТЕМА ДОБРОВОЛЬНОЙ СЕРТИФИКАЦИИ ЭКСПЕРТОВ ПО СТАНДАРТИЗАЦИИ

СЕРТИФИКАТ СООТВЕТСТВИЯ

СЭ № 0002331

Орган по сертификации экспертов удостоверяет, что

Фатеев Алексей Григорьевич

соответствует требованиям, предъявляемым к экспертам по стандартизации

Руководитель Органа по сертификации экспертов по стандартизации С.В. Бабкин

Эксперт А.А. Степанов

Зарегистрирован в Реестре экспертов по стандартизации

Протокол № 252 от 20 мая 2022 года

Действителен с 20 мая 2022 года по 19 мая 2025 года


СИСТЕМА ДОБРОВОЛЬНОЙ СЕРТИФИКАЦИИ ЭКСПЕРТОВ ПО СТАНДАРТИЗАЦИИ

СЕРТИФИКАТ СООТВЕТСТВИЯ

СЭ№0001943

Орган по сертификации экспертов удостоверяет, что

Голованов Владимир Борисович

соответствует требованиям, предъявляемым к экспертам по стандартизации

Руководитель Органа по сертификации экспертов по стандартизации С.В. Бабкин

Эксперт А.А. Степанов

Зарегистрирован в Реестре экспертов по стандартизации

Протокол № 182 от 28 января 2020 года

Действителен с 28 января 2020 года по 27 января 2023 года

эксперт по стандартизации: Специалист, который владеет знаниями и опытом для проведения работ в области стандартизации и квалификация которого подтверждена в процессе добровольной сертификации

[ГОСТ Р 1.12-2020, п.7]

Работа в области стандартизации в информационной безопасности

infotecs

Специализированные площадки в области информационной безопасности

ТК26 «Криптографическая защита информации»

ЗА ТК26 закреплены объекты стандартизации, относящиеся к методам **шифрования (криптографического преобразования)** информации, способам их реализации, а также методам обеспечения безопасности ИТ с использованием **криптографического преобразования информации** … (подробнее см. https://tc26.ru/)

ТК362 «Защита информации»

За ТК362 закреплены объекты стандартизации, относящиеся к **методам защиты информации**, способам их реализации, а также **средствам защиты информации** за исключением криптографических. (подробнее см. https://fstec.ru/tk-362/obshchaya-informatsiya)

Иные площадки в области стандартизации, на которых рассматриваются вопросы ИБ (смежные ТК): **ТК016** «Электроэнергетика», **ТК022** «ИТ», **ТК045** «Железнодорожный транспорт», **ТК164** «ИИ», **ТК167** «ПАК для КИИ и ПО для них» и другие

Работа в области стандартизации в информационной безопасности

- Достаточно ли знаний, полученных после обучения по универсальным программам ФГОС СПО, ФГОС ВО или программам ДПО по стандартизации, для работы в области стандартизации в информационной безопасности?

- Нет. Об этом далее …

Действующие нормы работ по стандартизации

Смена концепции стандартизации

Стандартизация до 27.12.2002	Стандартизация после 27.12.2002
Действовали: Закон Российской Федерации от 10 июня 1993 г. N 5151-1 «О сертификации продукции и услуг» Закон Российской Федерации от 10 июня 1993 г. N 5154-1 «О стандартизации» другие НПА	введение нового вида документов – **технические регламенты**; технические регламенты устанавливают обязательные требования, включая ссылки на стандарты; Иное применение стандартов – на добровольной основе *(статью 5 – не рассматриваем)*

ФЗ № 184-ФЗ «О техническом регулировании» принят в обеспечение обязательств по вступлению РФ в ВТО (в рамках обязательств о снятии технических барьеров в торговле, ТБТ ВТО, п.3.3)

Эволюция норм регулирования в области стандартизации. 2015г.

Федеральный закон «О стандартизации в Российской Федерации» от 29.06.2015 N 162-ФЗ принят для разделения областей технического регулирования и стандартизации:

- Установил возможность использования ссылок на стандарты не только в Технических регламентах. В этом случае статус их такой же, как и требований соответствующего НПА;
- Сохранена руководящая роль Росстандарта;
- Все нормы по стандартизации перенесены из ФЗ о техрегулировании в новый ФЗ;
- Стал основанием серьезных структурных «оптимизаций» в национальной системе стандартизации

На за период 2016-2022 гг. в НПА РФ было включено до **полутора тысяч ссылок** – https://www.rst.gov.ru/portal/gost/home/activity/standardization/standarts_it_dictionary

Виды документов по стандартизации

ФЗ №162-ФЗ устанавливает следующие виды документов по стандартизации:

- **национальный стандарт (ГОСТ Р)** – ГОСТ Р 1.2-2020;
- **предварительный национальный стандарт (ПНСТ)** – ГОСТ Р 1.16-2011;
- **правила стандартизации (ПР)** – ГОСТ Р 1.10-2004
- **рекомендации по стандартизации (Р)** – ГОСТ Р 1.10-2004;
- **техническая спецификация/отчет (ТС/ТО)** – ФЗ №162-ФЗ, ст. 21.1;
- **информационно-технический справочник (ИТС), общероссийский классификатор (ОК)** – НПА;
- **стандарт организаций (СТО)** – ГОСТ Р 1.4-2004;
- **свод правил (СП)** – ГОСТ Р 1.19-2023;
- **технические условия (ТУ)** – ГОСТ Р 1.3-2018.

Работы по стандартизации в ИБ

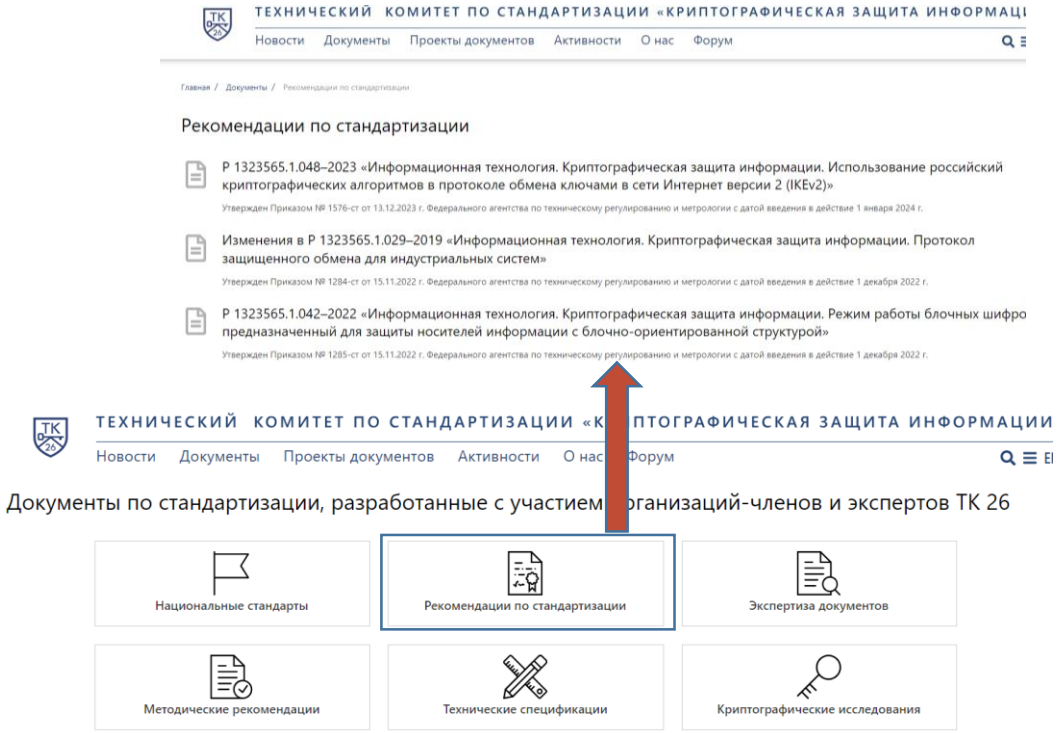
Виды разрабатываемых документов по стандартизации в области ИБ

В рамках работ профильных для области ИБ ТК26 «Криптографическая защита информации» и ТК362 «Защита информации» разрабатываются следующие виды документов по стандартизации:

- национальный стандарт (ГОСТ Р);
- предварительный национальный стандарт (ПНСТ);
- рекомендации по стандартизации (Р);
- техническая спецификация (отчет) (ТС/ТО).

В рамках работ ТК26 также разрабатывает методические рекомендации (МР) ТК26.

Документы по стандартизации, разработанные ТК26, https://tc26.ru



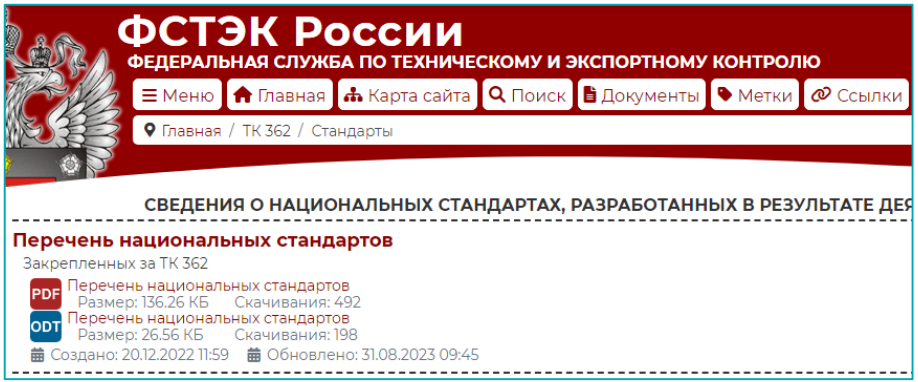
Всего разработано почти 90 документов, включая:

- **4** межгосударственных стандарта
- **6** национальных стандартов (включая один предварительный)
- более **30** рекомендаций по стандартизации
- почти **40** методических рекомендаций
- **9** технических спецификаций

(по состоянию на март 2024 года)

Документы по стандартизации, разработанные ТК362

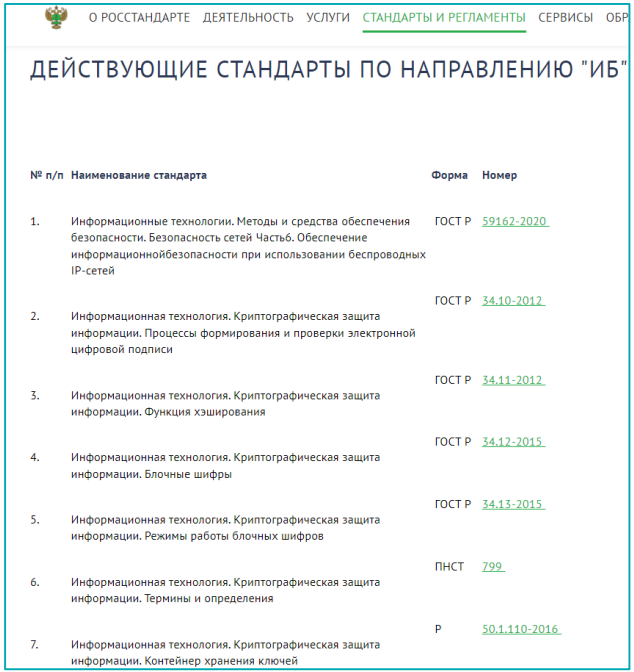
Перечень документов по стандартизации, разработанных в рамках деятельности ТК362 включает 64 документа – национальные стандарты (ГОСТ Р) и 2 рекомендации по стандартизации (Р) (по состоянию на март 2024 года, https://fstec.ru/tk-362/dokumenty



Перечень национальных стандартов, разработанных ТК 362 и принятых Ростехрегулированием (Росстандартом)

№ п/п	Наименование стандарта	№ приказа и дата введения
1.	ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования»	Постановление Госстандарта России № 49 от 09.02.1995 г.
2.	ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»	Приказ руководителя Ростехрегулирования № 373 - СТ от 27.12.2006 г. Дата введения в действие с 01.07.2007 г.
3.	ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения»	Приказ руководителя Ростехрегулирования № 374 - СТ от 27.12.2006 г. Дата введения в действие с 01.07.2007 г.
4.	ГОСТ Р 51583-2014 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения»	Приказ руководителя Росстандарта № 3-СТ от 28.01.2014 г. Дата введения в действие с 01.09.2014 г.
5.	ГОСТ Р 52069.0-2013 «Защита информации. Система стандартов. Основные положения»	Приказ руководителя Росстандарта № 3-СТ от 28.02.2013 г. Дата введения в действие с 01.09.2013 г.
6.	ГОСТ Р 52447-2005 «Защита информации. Техника защиты информации. Номенклатура показателей качества»	Приказ руководителя Ростехрегулирования № 448-СТ от 29.12.2005 г.
7.	ГОСТ Р 52448-2005 «Защита информации. Обеспечение безопасности сетей электросвязи. Общие положения»	Приказ руководителя Ростехрегулирования № 449-СТ от 29.12.2005 г.
8.	ГОСТ Р 52633.0-2006 «Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации»	Приказ руководителя Ростехрегулирования № 372 - СТ от 27.12.2006 г. Дата введения в действие с 01.04.2007 г.
9.	ГОСТ Р 52633.1-2009 «Защита информации. Техника защиты информации. Требования к формированию баз естественных биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации»	Приказ руководителя Ростехрегулирования № 839-СТ от 15.12.2009 г. Дата введения в действие 01.01.2010 г.

Документы по стандартизации в области ИБ (опубликованы)



О РОССТАНДАРТЕ ДЕЯТЕЛЬНОСТЬ УСЛУГИ СТАНДАРТЫ И РЕГЛАМЕНТЫ СЕРВИСЫ ОБР

ДЕЙСТВУЮЩИЕ СТАНДАРТЫ ПО НАПРАВЛЕНИЮ "ИБ"

№ п/п	Наименование стандарта	Форма	Номер
1.	Информационные технологии. Методы и средства обеспечения безопасности. Безопасность сетей Часть6. Обеспечение информационнойбезопасности при использовании беспроводных IP-сетей	ГОСТ Р	59162-2020
2.	Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи	ГОСТ Р	34.10-2012
3.	Информационная технология. Криптографическая защита информации. Функция хэширования	ГОСТ Р	34.11-2012
4.	Информационная технология. Криптографическая защита информации. Блочные шифры	ГОСТ Р	34.12-2015
5.	Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров	ГОСТ Р	34.13-2015
6.	Информационная технология. Криптографическая защита информации. Термины и определения	ПНСТ	799
7.	Информационная технология. Криптографическая защита информации. Контейнер хранения ключей	Р	50.1.110-2016

Росстандарт предоставил открытый доступ к 89 документам национальной системы стандартизации в сфере ИБ.

Документы по стандартизации разработаны ТК26 «Криптографическая защита информации» и ТК362 «Защита информации».

Ссылка – https://www.rst.gov.ru/portal/gost//home/standarts/InformationSecurity

Работы по стандартизации в области ИБ в «смежных» ТК

В рамках публичного обсуждения поступали проекты национальных стандартов, содержащих требования ИБ, от смежных ТК – ТК016, ТК022, ТК045, ТК057, ТК141, ТК164, ТК167, ТК194, ТК322, ТК480, в том числе:

- национальные стандарты (ГОСТ Р) – ТК016, ТК022, ТК057, ТК141, ТК164, ТК322, ТК480;
- предварительные национальные стандарты (ПНСТ) – ТК022, ТК045, ТК057, ТК164, ТК167, ТК194.

Также поступали межгосударственные стандарты, содержащие положения ИБ, от ТК436 и ТК331.

Организационная и процедурная основы разработки стандартов в области ИБ

Организационная основа. Правила деятельности ТК по стандартизации

ФЗ от 29.06.2015 N 162-ФЗ «О стандартизации в Российской Федерации»;

ГОСТ Р 1.1-2020 Стандартизация в Российской Федерации. Технические комитеты по стандартизации и проектные технические комитеты по стандартизации. Правила создания и деятельности;

ПР 1323565.1.003-2019 Методика оценки эффективности деятельности технических комитетов по стандартизации.

Процедурная основа. Процесс разработки в ТК26 и ТК362 (общий)

Предпочтительное проведение НИР силами компании-лицензиата ФСТЭК/ФСБ (или с участием такой организации) с публикацией и апробацией результатов и разработкой первой редакции документа по стандартизации;

В рамках НИР/подготовки ПЗ-обоснования: анализ действующих НПА и действующих документов по стандартизации в области ИБ (более 90 от ТК26, свыше 60 от ТК362 и др. источники), анализ их требований;

Проведение публичного обсуждения первой редакции документа по стандартизации;

Доработка в ходе которого может быть подготовлено несколько промежуточных (вторая, третья и т.д.) редакций;

По завершении доработки может быть подготовлен документ содержательно полностью отличающийся от первоначального;

Другая специфика, определяемая объектом и аспектом стандартизации.

Процедурная основа. Дополнительные требования и рекомендации. ТК26

Формирование **предложений в План работ ТК26:**


Наличие заинтересованных сторон (не менее 3-х);


Выполнение НИР с публикацией и обсуждением результатов;


Публикация статей в рецензируемых журналах (не менее 3-х);


Наличие успешных реализаций – внедрение результатов НИР;


Наличие положительного заключения экспертов ТК26;


Наличие положительных результатов экспертизы Регулятора;


Формирование Заявки на разработку документа по стандартизации, подаваемой в ТК26.

Процедурная основа. Дополнительные требования и рекомендации. ТК26

Пояснительная записка для включения в План ТК26:

- Название предполагаемого к разработке документа
- Область применения предлагаемого к стандартизации решения
- Обоснование необходимости начала разработки документа, включая:

……

2) Роль и место документа в существующей системе документов ……

3) Решаемые задачи криптографической защиты информации и сравнение с аналогами ТК 26/ISO/IETF …

……

7) Результаты сторонних криптографических исследований

8) Список экспертов (с указанием организаций) для участия в разработке ……

Процедурная основа. Практика работ по ТК362 «ЗИ»

- Проведенная НИР
  (по заказу ФСТЭК России или иного органа), на основе результатов которой разрабатывается проект стандарта;
- Либо: обоснованная потребность в гармонизации действующих МС
  (ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection, МС других организаций);
- С 2024 года:
  - Гармонизация либо с размещением перевода в Федеральном информационном фонде стандартов, либо разработка Неэквивалентного стандарта;
  - Обеспечение условий и возможности использования стандарта в качестве ссылочного в НПА Регуляторов (ориентир).

Разработка и оформление национальных стандартов

Разработка и оформление национального стандарта

Это должен знать разработчик стандарта

ГОСТ Р 1.2-2020 устанавливает правила разработки и утверждения национальных стандартов Российской Федерации, включая порядок подготовки первой и последующих редакций проекта стандарта, публичного обсуждения, подготовки сводки отзывов, утверждения и регистрации.

ГОСТ Р 1.5-2012 устанавливает правила построения, изложения, оформления и обозначения национальных стандартов. Содержит ссылки на ГОСТ 1.5-2001 в части оформления структурных элементов стандарта.

ГОСТ Р 1.16-2011 устанавливает правила разработки и утверждения ПНСТ.

ГОСТ Р 1.7-2014 устанавливает правила оформления и обозначения ГОСТ Р и ПНСТ, которые разрабатывают на основе применения международных стандартов. Содержит ссылки на ГОСТ 1.3-2014.

Требования к формированию терминологии, включаемой в стандарт, установлены ГОСТ Р ИСО 704-2010, РМГ 19-96, Р 50.1.075-2011.

Стандартизированные шаблоны форм процедурных документов

Это должен знать разработчик стандарта

ГОСТ Р 1.2-2020 устанавливает структуру и содержание документов, разрабатываемых при разработке стандартов:

- пояснительная записка к проекту национального стандарта (к первой и последующим редакциям) – разработчик стандарта;
- отзыв на проект национального стандарта – организации – члены ТК;
- сводка отзывов на проект национального стандарта – разработчик стандарта;
- мотивированное предложение об утверждении национального стандарта – секретариат ТК.

Типовые ошибки разработки проектов национальных стандартов

- Отсутствие ссылок на НПА, регулирующие применение методов, алгоритмов и протоколов ЗИ;
- Включение требований и положений, дублирующих нормы действующих НПА и документов по стандартизации, либо противоречащих им;
- Включение положений и ссылки на НПА других государств и международные документы, которые неприменимы на территории РФ (при гармонизации международных документов);
- Включение требований применения на территории РФ алгоритмов, методов и протоколов, несогласованных с Регуляторами ЗИ РФ.

Примеры некорректных требований в проектах стандартов

- «… используются предварительно опубликованные секретные криптографические ключи …»;
- «Асимметричные алгоритмы, используемые для подписи, должны быть выбраны из FIPS 186-4 или любых других признанных стандартов»;
- «Географическая юрисдикция может быть представлена в четырех типах контекста: муниципальный; штат/провинция; национальный; мульти-юрисдикционный»;
- «Нарушение безопасности в робототехническом комплексе и/или в модуле робота может привести к опасностям, связанным с безопасностью»;
- «Внедрение функций ИБ вне систем, важных для безопасности, облегчает квалификацию функций, связанных с ИБ, когда этого требуют национальные нормативные акты».

Ошибки при построения научно-технической терминологии

- Несоответствие термина его определению
- Наличие «порочного круга» – понятие определяется с помощью другого понятия, которое, в свою очередь, определяется через первое
- Определение не содержит существенных признаков понятия
- Излишне длинные и громоздкие формулировки терминов и их определений
- Несоответствие терминов и их определений нормам русского языка, наличие несогласованных выражений

Терминология в области стандартизации

Это должен знать разработчик стандарта

Установлена:

- **Федеральным законом от 27.12.2002 N 184-ФЗ «О техническом регулировании»**
- **Федеральным законом от 29.06.2015 N 162-ФЗ «О стандартизации в Российской Федерации»**
- **ГОСТ Р 1.12-2020** Стандартизация в Российской Федерации. Термины и определения
- **другими НПА и документами по стандартизации,** действующими в Российской Федерации

Элемент «Термины и определения» включают в стандарт для определения терминов, не стандартизованных в Российской Федерации на национальном уровне (ГОСТ Р 1.5-2012, п. 3.7)

Требования и рекомендации к построению терминосистем

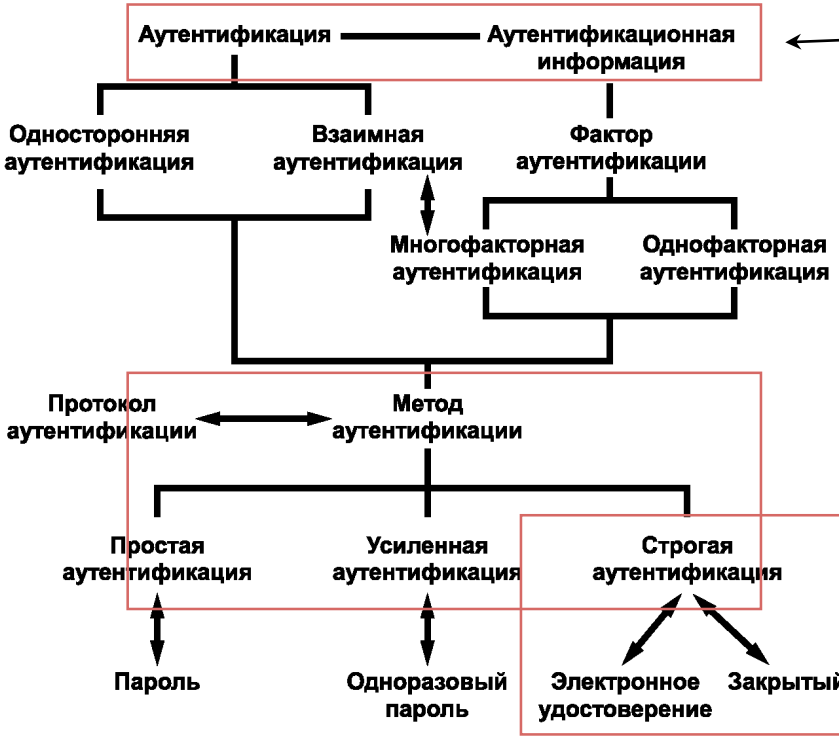
Это должен знать разработчик стандарта

Установлены:

- **ГОСТ Р ИСО 704-2010** Терминологическая работа. Принципы и методы (ISO 704:2009, IDT)
- **ГОСТ Р ИСО 10241-1-2013** Терминологические статьи в стандартах. Часть 1. Общие требования и примеры представления (ISO 10241-1:2011, IDT)
- **РМГ 19-96** Рекомендации по основным принципам и методам стандартизации терминологии
- **Р 50.1.075-2011** Рекомендации по стандартизации. Разработка стандартов на термины и определения

Очень ценный практический материал в трудах от АН СССР под ред. Д.С. Лотте и др.

Пример обоснованного построения научно-технической терминологии



родовая связь

партитивная связь

ассоциативная связь

Взаимосвязь терминов, входящих в группу, относящуюся к понятию «**аутентификация**»

ГОСТ Р 58833-2020 Защита информации. Идентификация и аутентификация. Общие положения, Приложение А

Виды проверок (экспертизы) проектов национальных стандартов

В соответствии с действующей редакцией ГОСТ Р 1.2-2020 проект национального стандарта (окончательная редакция) секретариатом ТК направляется на:

- на экспертизу в ТК в соответствии с ГОСТ Р 1.6. Экспертизу проводит рабочая группа, формируемая из членов ТК;
- метрологическую экспертизу (если согласно ПМГ 92-2009 проект национального стандарта подлежит метрологической экспертизе). Проводится одновременно с экспертизой в ТК.

Ожидается включение в ГОСТ Р 1.6 следующего вида работ: специализированная экспертиза в области ИБ.

Дополнение ГОСТ Р 1.6 (специализированная экспертиза ИБ)

ТК26 и ТК362 внесены совместные предложения по корректировке ГОСТ Р 1.6, включающие рекомендации:

- расширить оценку соответствия проектов стандартов целям и задачам, установленным в ст.3 ФЗ «О стандартизации в Российской Федерации» включив рассмотрение «*обеспечения ИБ в случае применения разрабатываемого стандарта при осуществлении процессов поиска, сбора, хранения, обработки, предоставления, распространения информации……*»;
- дополнить ГОСТ Р 1.6 проведением специализированной экспертизы в области ИБ с привлечением ТК с закрепленными объектами стандартизации в области ЗИ и (или) криптографической ЗИ (ТК26 и (или) ТК362) с возможностью проведения общей (I) и углубленной специализированной экспертизы (II) в области ИБ.

Заключение

Для разработки стандартов в ИБ востребованы соответствующие знания и квалификация.

Объемы работ по стандартизации в ИБ будут год от года увеличиваться.

Вопрос:
Востребован ли специализированный курс повышения квалификации по направлению стандартизация в ИБ?

Спасибо за внимание!

Голованов Владимир
Vladimir.Golovanov@infotecs.ru

Фатеев Алексей
Aleksey.Fateev@infotecs.ru

Подписывайтесь на наши соцсети

vk.com/infotecs_news

https://t.me/infotecs_official

rutube.ru/channel/24686363