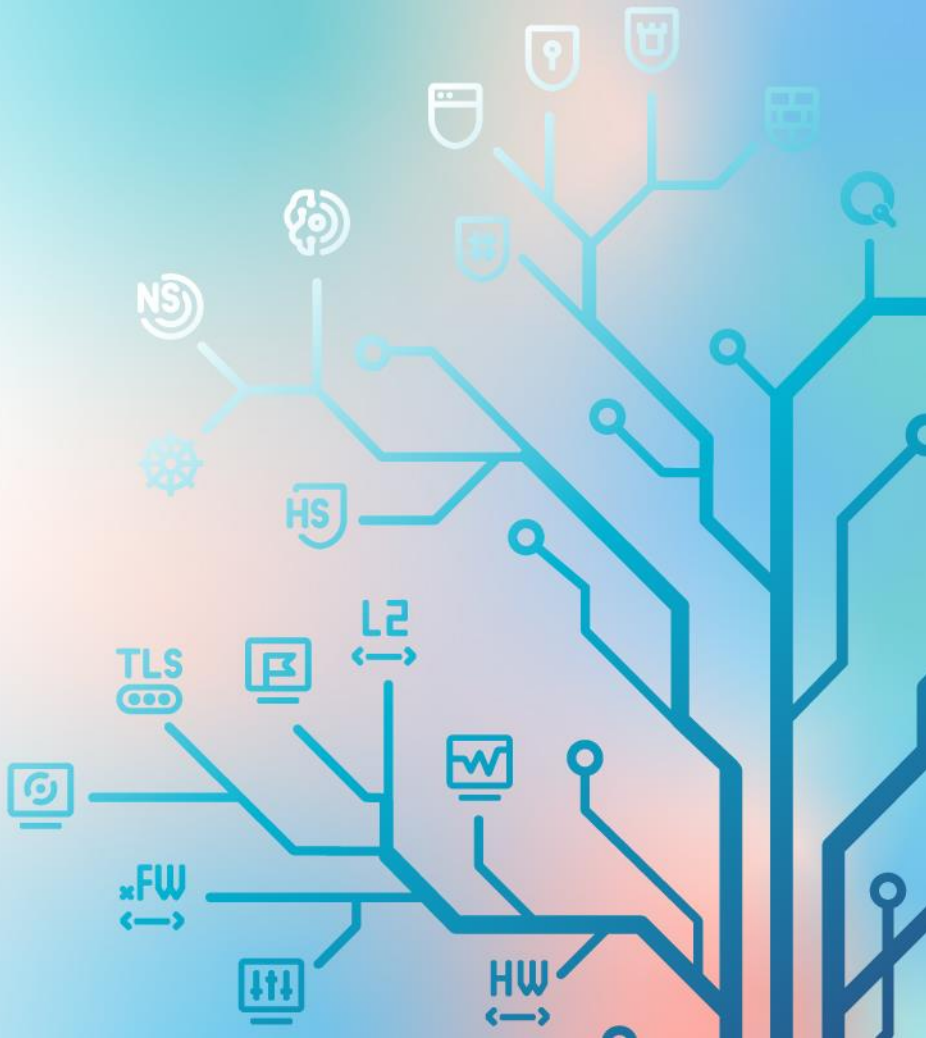
Стандартизация в информационной безопасности

Часть 2. Специфика требований и подходов по разработке и экспертизе стандартов в области ИБ

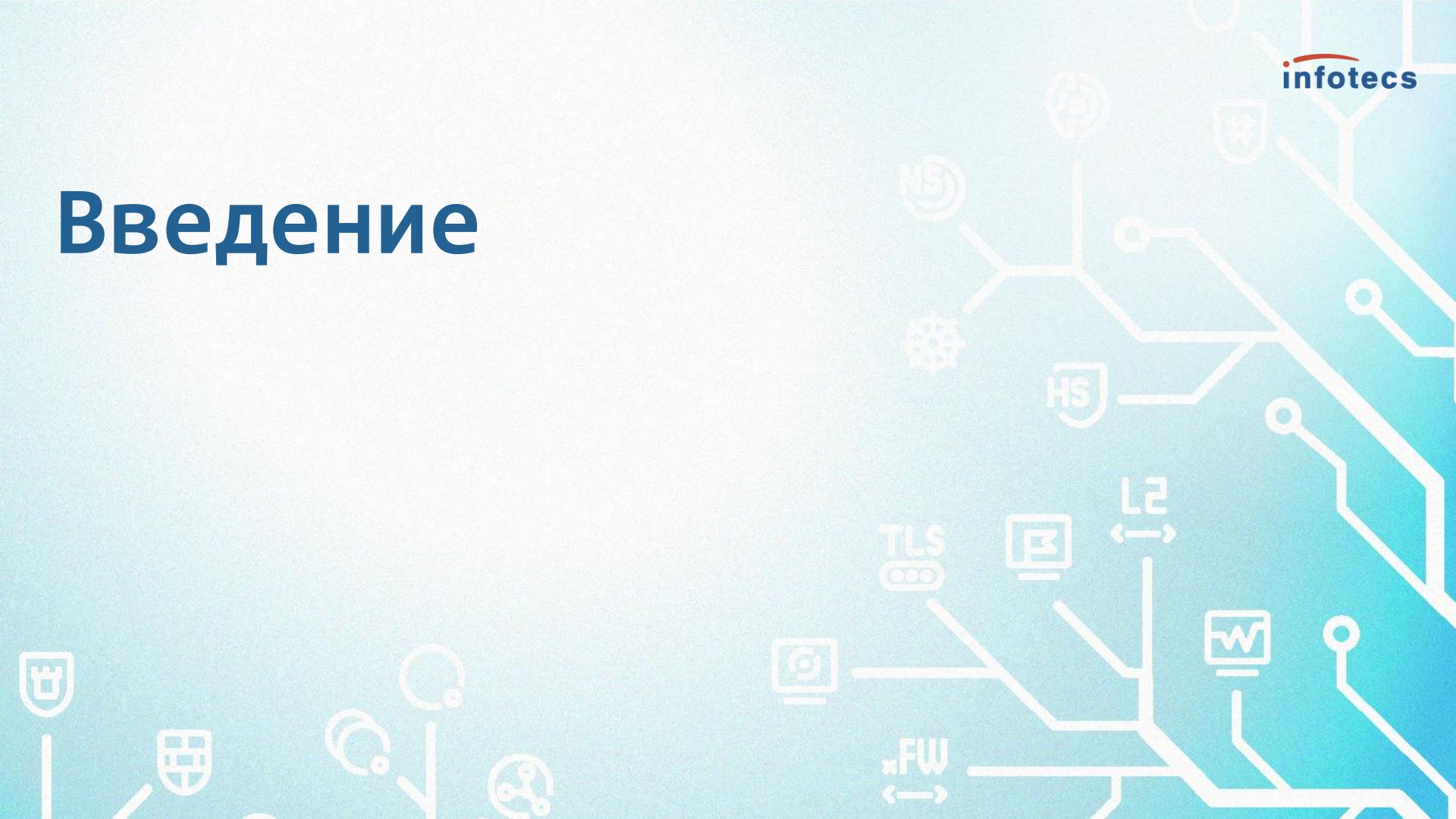
Владимир Голованов
заместитель начальника аналитического отдела

Алексей Фатеев
специалист аналитического отдела

infotecs



Введение



На чем остановимся сегодня? Детали...

- Организация работ по стандартизации в ИБ на профильных площадках
- Организационная и процедурная основы разработки стандартов в области ИБ на профильных площадках
- Почему возникли вопросы о стандартизации требований ИБ? Продолжаем тему 1-го дня
- Изменения в ГОСТ Р 1.6 по экспертизе, специализированная экспертиза требований ИБ
- Проект документа Правил по стандартизации Что это такое?
- Проведение экспертизы требований ИБ (в соответствии с Правилами …)
- Резюме

Организация работ по стандартизации в ИБ на профильных площадках

Работа в области стандартизации в информационной безопасности

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)

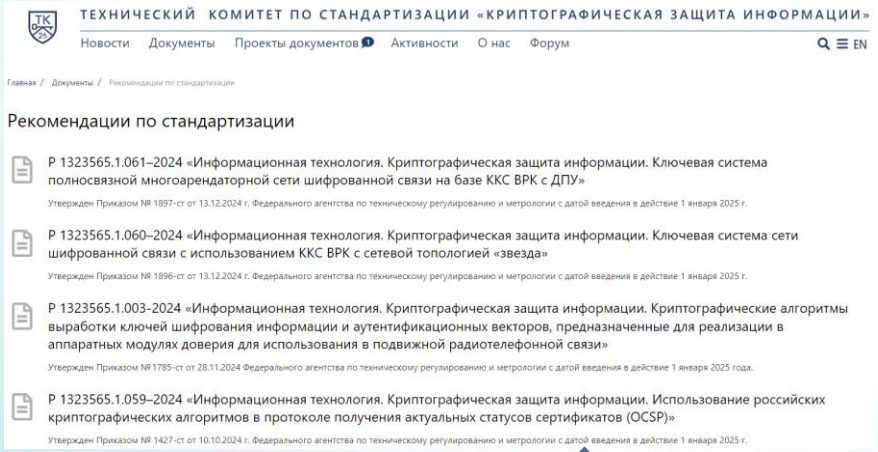
Виды разрабатываемых документов по стандартизации в области ИБ

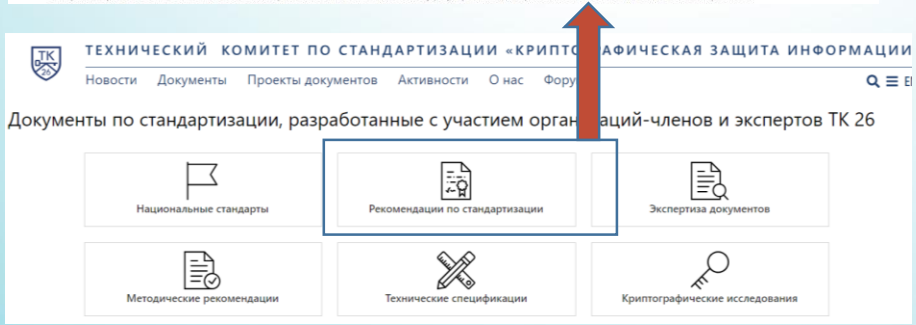
В рамках работ профильных для области ИБ ТК26 «Криптографическая защита информации» и ТК362 «Защита информации» разрабатываются следующие виды документов по стандартизации:

- 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 более 90 документов, включая:

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

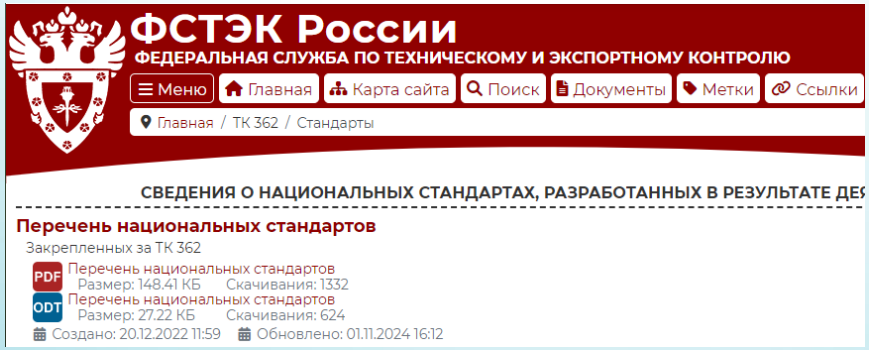
Ссылка – https://tc26.ru/standarts/

(по состоянию на март 2025 года)

Документы по стандартизации, разработанные ТК362

Перечень документов по стандартизации, разработанных в рамках деятельности ТК362 включает 67 документов – национальные стандарты (ГОСТ Р) и 2 рекомендации по стандартизации (Р) (по состоянию на март 2025 года)

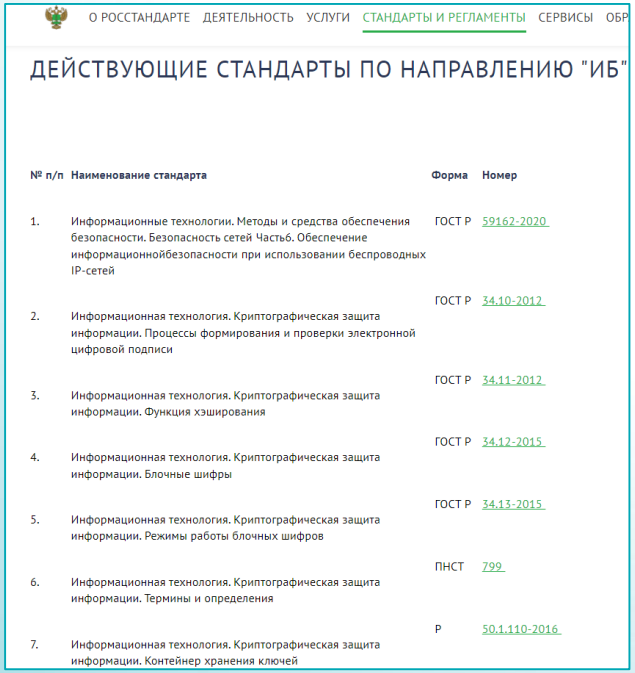
Ссылка – https://fstec.ru/tk-362/standarty



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, включая национальные стандарты и рекомендации по стандартизации

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

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

Опубликование документов по стандартизации в области ИБ

Неясно по каким критериям отбирались документы по стандартизации в области ИБ для публикации на сайте Росстандарта и кто это делал

Общее количество документов по стандартизации, разработанных в рамках деятельности ТК362 и ТК26, составляет более 150 документов, из них на сайте Росстандарта размещено только 89 документов по стандартизации

Организационная и процедурная основы разработки стандартов в области ИБ на профильных площадках

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 срез)

Предпочтительно проведение НИР силами компании-лицензиата ФСТЭК России / ФСБ России (или с участием такой организации) с публикацией и апробацией результатов и как итог - 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 которой 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 …

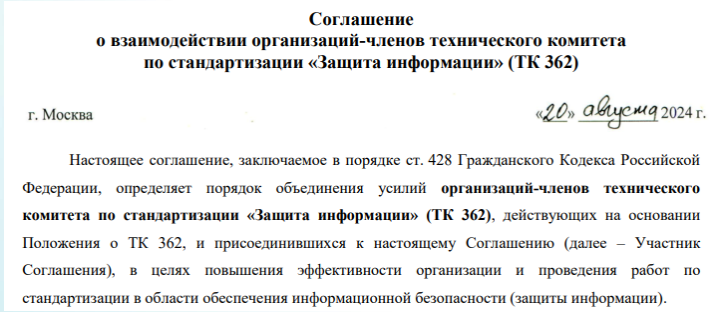
……

7) Результаты сторонних криптографических исследований

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

Из материалов заседания ТК26. Маршалко Г.Б.

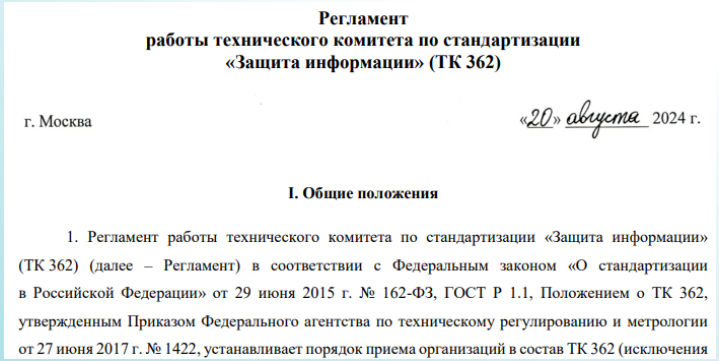
Процедурная основа работ по ТК362 «ЗИ». С 2024 г. Регламент и Соглашение



Соглашение
о взаимодействии организаций-членов технического комитета по стандартизации «Защита информации» (ТК 362)

г. Москва «20» августа 2024 г.

Настоящее соглашение, заключаемое в порядке ст. 428 Гражданского Кодекса Российской Федерации, определяет порядок объединения усилий **организаций-членов технического комитета по стандартизации «Защита информации» (ТК 362)**, действующих на основании Положения о ТК 362, и присоединившихся к настоящему Соглашению (далее – Участник Соглашения), в целях повышения эффективности организации и проведения работ по стандартизации в области обеспечения информационной безопасности (защиты информации).



Регламент
работы технического комитета по стандартизации «Защита информации» (ТК 362)

г. Москва «20» августа 2024 г.

I. Общие положения

1. Регламент работы технического комитета по стандартизации «Защита информации» (ТК 362) (далее – Регламент) в соответствии с Федеральным законом «О стандартизации в Российской Федерации» от 29 июня 2015 г. № 162-ФЗ, ГОСТ Р 1.1, Положением о ТК 362, утвержденным Приказом Федерального агентства по техническому регулированию и метрологии от 27 июня 2017 г. № 1422, устанавливает порядок приема организаций в состав ТК 362 (исключения

Соглашение определяет:

- цели и содержание деятельности ТК362;
- принципы присоединения участников к Соглашению;
- форму Согласия на присоединение к Соглашению.

(https://fstec.ru/tk-362/dokumenty-tk362/soglashenie-o-vzaimodejstvii-organizatsij-chlenov-tk-362-ot-20-avgusta-2024-g)

Регламент устанавливает порядок приема организаций в состав ТК362 (исключения из состава ТК362), основные правила организации деятельности ТК362, а также порядок обеспечения доступа к информации о деятельности ТК362.

(https://fstec.ru/tk-362/dokumenty-tk362/reglament-raboty-tk-362-ot-20-avgusta-2024-g)

Процедурная основа работ по ТК362 «ЗИ». Включение в план работ

В соответствии с п. 22 Регламента ТК362 осуществляет работу в соответствии с ежегодными планами своей деятельности, а также перспективным планом работы ТК362 на среднесрочный период, утверждаемыми председателем ТК362.

В соответствии с п. 24 Регламента организации-члены ТК362 направляют в секретариат ТК362 предложения по работам, предлагаемым к включению в план, по форме приложения №2 к Регламенту.

Предложения в программу (план) работ по стандартизации в области защиты информации включают:

1. Наименование предлагаемого к разработке (пересмотру) документа по стандартизации.
2. Цель проведения работ по разработке (пересмотру) документа по стандартизации;
3. Обоснование актуальности проведения работ по разработке (пересмотру) документа по стандартизации, в том числе;

…

Почему возникли вопросы о стандартизации требований ИБ? Продолжаем тему 1-го дня

Ошибки разработки проектов стандартов в части требований ИБ

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

2020 год. Примеры [не]«удачных» проектов национальных стандартов

Проект ГОСТ Р 58603-2019 (MQTT v3.1.1)

Цитаты из стандарта: «*Реализация может потребовать соответствия определённым отраслевым стандартам безопасности, таким как **NIST Cyber Security Framework, PCI-DSS, FIPS 140-2** и **NSA Suite B***», «*Широко применяется **Улучшенный стандарт шифрования (AES)** и **Стандарт шифрования данных (DES)***»

Был издан приказ Росстандарта от 16 октября 2019 № 1005-ст о введении в действие с 01.01.2021. Но уже в ноябре 2020 года издан приказ Росстандарта от 17.11.2020 № 1113-ст об отмене приказа от 16.10.2019 № 1005-ст о введении в действие ГОСТ Р 58603-2019 с 01.01.2021. Стандарт **не успел вступить в действие**!

Матюхин Д.В. Вопросы криптографической защиты информации в интернете вещей и индустриальных системах. URL: https://www.ruscrypto.ru/resource/archive/rc2020/files/01_matyukhin.pdf

2020 год. Примеры [не]«удачных» проектов национальных стандартов

Проект ГОСТ Р ИСО/МЭК 27033-6 по безопасности телекоммуникаций в частности беспроводных сетей

Проект упоминает в качестве допустимых, рекомендуемых и даже обязательных к использованию большое число криптографических механизмов, не определяемых документами (проектами документов) национальной системы стандартизации в области криптографической защиты информации

Отрицательный отзыв ТК26 на первую редакцию проекта дан в конце января 2020 года

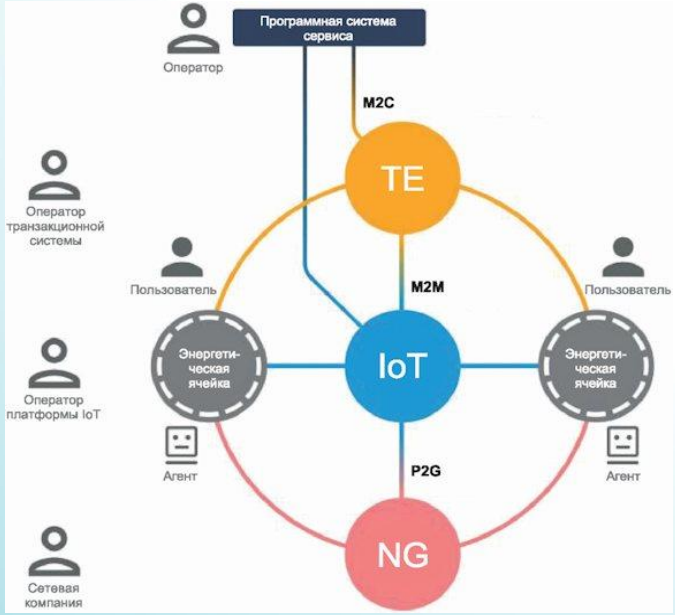
Сводка отзывов и окончательная редакция **не опубликованы**

Матюхин Д.В. Вопросы криптографической защиты информации в интернете вещей и индустриальных системах. URL: https://www.ruscrypto.ru/resource/archive/rc2020/files/01_matyukhin.pdf

Причины ошибок в проектах стандартов в части требований ИБ

- Проекты стандартов разрабатываются непрофильными ТК (ТК22, ТК164, ТК194 и др.). Разработчики (организации-члены непрофильных ТК) проектов документов зачастую не обладают необходимыми знаниями и компетенциями.
- Слабое взаимодействие между профильными ТК (ТК26 и ТК362) и непрофильными ТК. Заключены соглашения с отдельными ТК, но нет системной работы.
- Отсутствует экспертиза проектов стандартов, содержащих требования ИБ, проводимая профильными ТК (осуществляется в инициативном порядке, при обращении в секретариат профильного ТК).
- В 2020 году заинтересованными ТК инициированы работы по развитию института экспертизы требований ИБ. В 2024 году работы еще не завершены, проблема продолжает быть актуальной.

Пример 2024 года. Программа «Энерджинет»... Ссылки на источники



«Определены следующие компоненты Интернета энергии:

- транзакционная подсистема (**TE**);
- подсистема межмашинной коммуникации (**IoT**);
- подсистема обеспечения режимов передачи электрической энергии (**NG**);
- программные агенты энергетических ячеек.»

ПНСТ 913-2024, подраздел 5.1 «Общие положения»

Рисунок 1 - Концептуальная модель Интернета энергии

Пример 2024 года. Программа «Энерджинет»... Ссылки на источники

ПНСТ 913-2024 «Информационные технологии. Энергетика умная. Интернет энергии. Типовая архитектура»

Фрагмент требований ИБ (всего требований – отдельный раздел в 4 абзаца):

«...Требования к информационной безопасности при реализации конкретного архитектурного решения Интернета энергии следует применять согласно **ГОСТ Р ИСО/МЭК 27001, ГОСТ Р ИСО/МЭК 27002, ГОСТ Р 52863.** Рекомендуется учитывать положения **ГОСТ Р 56205 и ГОСТ Р МЭК 62443-2-1**.

Дополнительно требования к информационной безопасности системы ТЕ, ее программных интерфейсов и межсоединительных устройств с программным агентом энергетической ячейки и другими системами следует применять согласно **ГОСТ Р ИСО/ТО 13569, ГОСТ Р 57580.1**...»

Пример 2024 года. Программа «Энерджинет»... Ссылки на источники

Стандарты, на которые приведены ссылки в **ПНСТ 913-2024**:

СМИБ

ГОСТ Р ИСО/МЭК 27001-2021 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования
ГОСТ Р ИСО/МЭК 27002-2021 Информационные технологии. Методы и средства обеспечения безопасности. Свод норм и правил применения мер обеспечения информационной безопасности

ГОСТ Р 52863-2007 Защита информации. Автоматизированные системы в защищенном исполнении. Испытания на *устойчивость к преднамеренным силовым электромагнитным воздействиям*. Общие требования (*ПЭМИН «наоборот»*)

АСУ ТП

ГОСТ Р 56205-2014/IEC/TS 62443-1-1:2009 Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 1-1. Терминология, концептуальные положения и модели
ГОСТ Р МЭК 62443-2-12015 Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 2-1. Составление программы обеспечения защищенности (кибербезопасности) системы управления и промышленной автоматики

Банки

ГОСТ Р ИСО/ТО 13569-2007 Финансовые услуги. Рекомендации по информационной безопасности
ГОСТ Р 57580.1-2017 Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер

Изменения к лучшему. Примеры (продолжение)

ГОСТ Р 71844 Аэродромы гражданские. Искусственные покрытия. Искусственный интеллект при распознавании дефектов. Общие положения

Стандарт включает раздел «Обеспечение информационной безопасности», устанавливающий требования ИБ к частным алгоритмам ИИ, применяемым для распознавания дефектов на искусственных покрытиях гражданских аэродромов

На первую редакцию вынуждены были дать отрицательные отзывы ТК362 и ТК26 в июле 2024 года

Окончательная редакция: были учтены замечания экспертов профильных ТК, поступила в сентябре 2024 года – включены ссылки на НПА и документы по стандартизации, устанавливающие требования криптографической ЗИ

Утвержден и введен в действие приказом Росстандарта от 29.11.2024 №1812-ст. **Дата введения – 01.02.2025**

Изменения к лучшему. Примеры (продолжение)

ГОСТ Р 71704 «Информатизация здоровья. Связь с медицинскими приборами индивидуального контроля состояния здоровья. Часть 20701. Сервис – ориентированная архитектура медицинских приборов и привязка протокола»

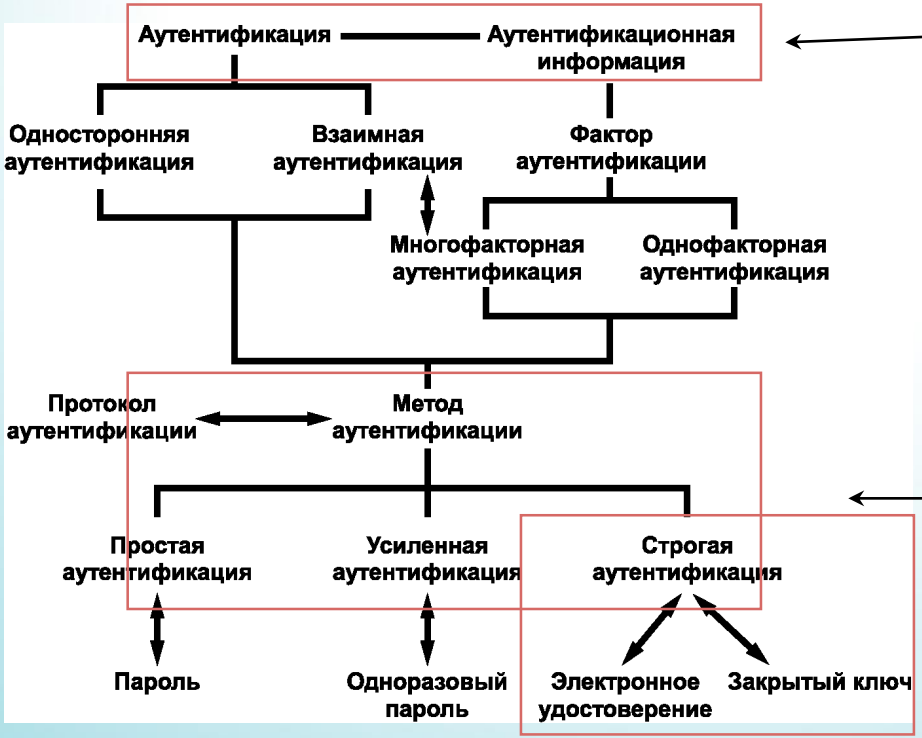
Стандарт включает подраздел «Безопасность информационных технологий», устанавливающий требования *по защите специальной категории персональных данных*, к которой относятся медицинские ПДн

На первую редакцию вынуждены были дать отрицательные отзывы ТК362 и ТК26

Окончательная редакция доработана с учетом замечаний, включены ссылки на действующее законодательство, устанавливающее требования по защите ПДн, а также ссылки на документы по стандартизации, описывающие использование российских криптографических алгоритмов. Форма гармонизации изменена на неэквивалентную в соответствии с замечаниями

Утвержден и введен в действие приказом Росстандарта от Приказ Росстандарта от 17.10.2024 №1465-ст. Дата введения - **01.07.2025**
Неэквивалентный ISO/IEEE 11073-20701:2020

Пример корректного 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

Пример корректного построения научно-технической терминологии

метод аутентификации: Реализуемое при аутентификации предопределенное сочетание факторов, организации обмена и обработки аутентификационной информации, а также соответствующих данному сочетанию протоколов аутентификации, [**п.3.27**]

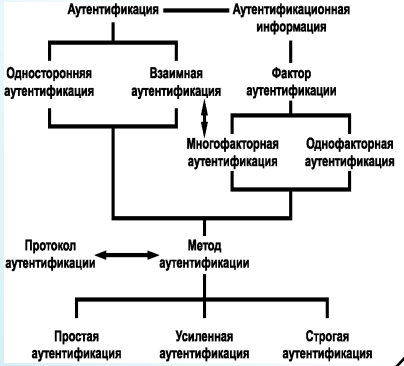
простая аутентификация: Аутентификация с применением метода (*ближайшее понятие*) однофакторной односторонней аутентификации и соответствующих данному методу протоколов аутентификации (*отличительный признак*), [**п.3.46**]

усиленная аутентификация: Аутентификация с применением метода (*ближайшее понятие*) многофакторной односторонней или взаимной аутентификации и соответствующих данному методу протоколов аутентификации (*отличительный признак*), [**п.3.59**]

строгая аутентификация: Аутентификация с применением только метода (*ближайшее понятие*) многофакторной взаимной аутентификации и использованием криптографических протоколов аутентификации (*отличительный признак*), [**п.3.54**]

ГОСТ Р 58833-2020 Защита информации. Идентификация и аутентификация. Общие положения, раздел 3

Пример корректного построения научно-технической терминологии



аутентификация: Действия по проверке подлинности субъекта доступа и/или объекта доступа …, [**п.3.4**]

строгая аутентификация: Аутентификация с применением только метода многофакторной взаимной аутентификации и использованием криптографических протоколов аутентификации, [**п.3.54**]

метод аутентификации: Реализуемое при аутентификации предопределенное сочетание факторов …, [**п.3.27**]

многофакторная аутентификация: Аутентификация, при выполнении которой используется не менее двух различных факторов аутентификации, [**п.3.29**]

взаимная аутентификация: Обоюдная аутентификация, обеспечивающая …, [**п.3.10**]

протокол аутентификации: Протокол, позволяющий участникам процесса аутентификации … , [**п.3.47**]

ГОСТ Р 58833-2020 Защита информации. Идентификация и аутентификация. Общие положения, раздел 3

Изменения в ГОСТ Р 1.6 по экспертизе, специализированная экспертиза требований ИБ

Изменение ГОСТ Р 1.6 (специализированная экспертиза ИБ)

В первую редакцию включены следующие изменения, вводящие институт экспертизы ИБ:

- «При оценке соответствия проекта стандарта целям и задачам, установленным в статье 3 Федерального закона «О стандартизации в Российской Федерации» [1], рассматривают:
  ...
  - обеспечение требований в области информационной безопасности в случае применения разрабатываемого стандарта при осуществлении процессов поиска, сбора, хранения, обработки, предоставления, распространения информации», [**п.4.2**];

Изменение ГОСТ Р 1.6 (специализированная экспертиза ИБ)

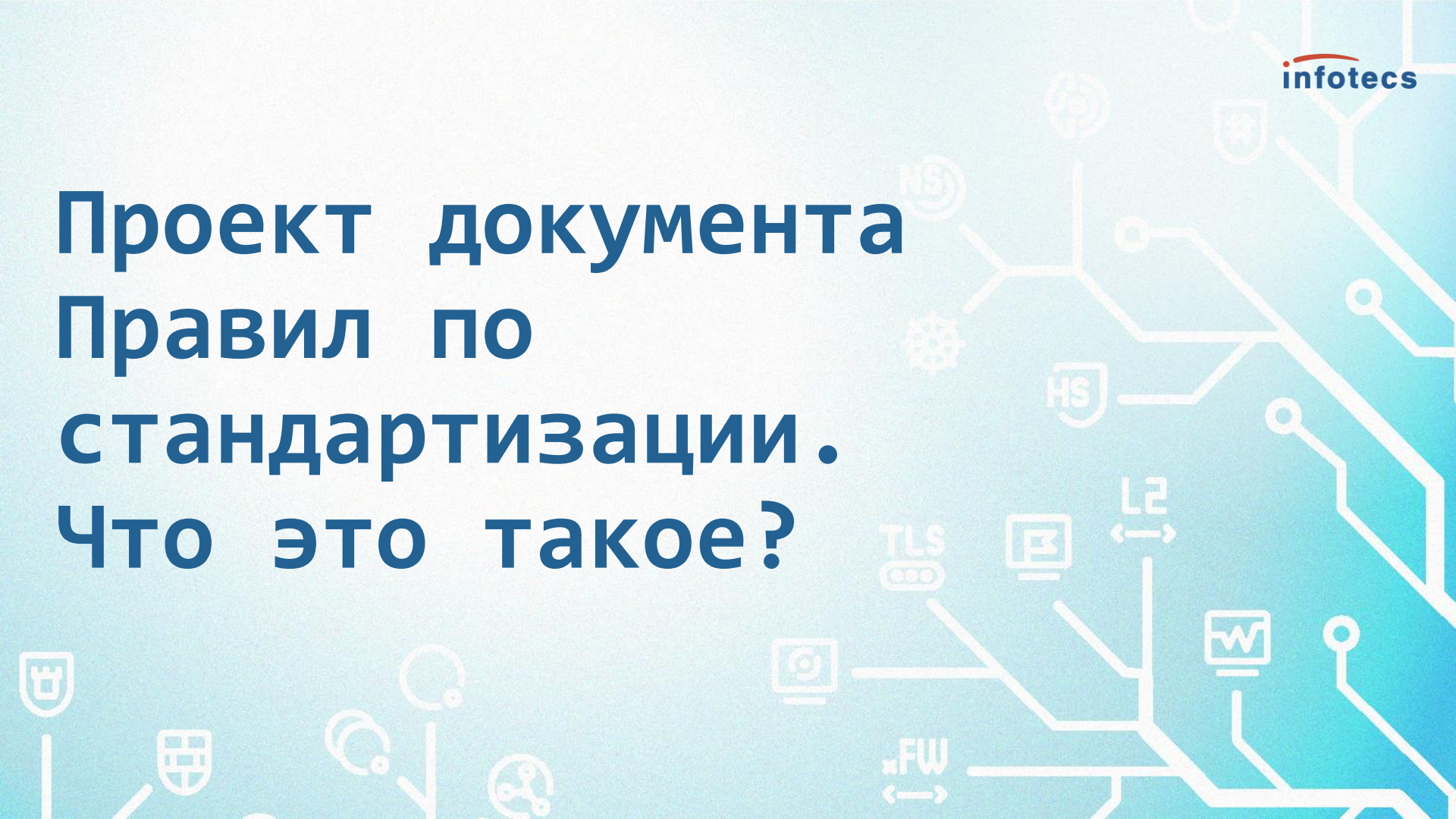
продолжение:

- *«Для оценки проекта стандарта, определяющего порядок разработки, использования и внедрения информационных технологий, содержание которого (**включая термины, их определения, описываемые свойства, методы и механизмы**), а также объект или аспект стандартизации которого содержат вопросы защиты информации или криптографической защиты информации проводится экспертиза в области информационной безопасности в соответствии с установленным порядком.*

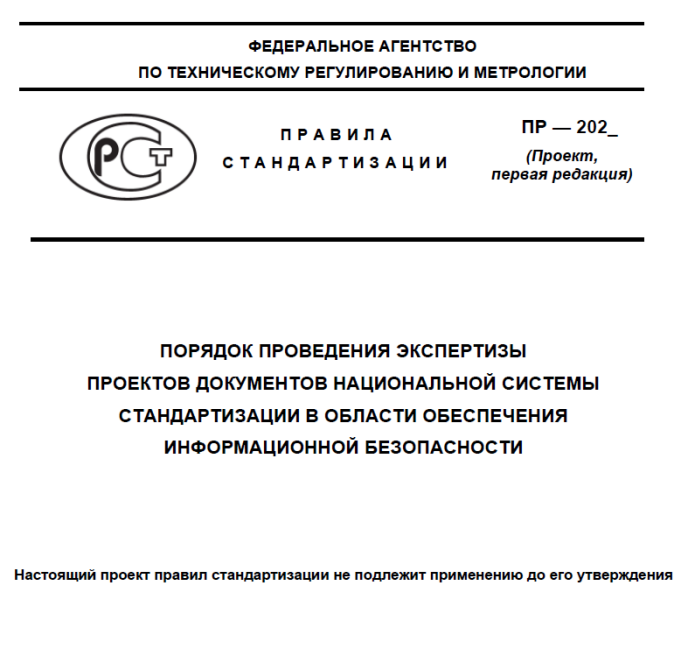
  Экспертиза проводится с целью установления в разрабатываемых стандартах требований, направленных на устойчивость и безопасность информационной инфраструктуры, конкурентоспособность отечественных разработок и технологий информационной безопасности, создание эффективной системы защиты прав и законных интересов государства от угроз безопасности в части применения не доверенных методов защиты информации.

  *Для проведения экспертизы в области информационной безопасности привлекают технические комитеты по стандартизации в области защиты информации и (или) криптографической информации. По результатам такой экспертизы может быть сделано заключение о необходимости проведения дополнительной экспертизы в области информационной безопасности специализированными организациями», [**п.4.7.2**]*

Проект документа Правил по стандартизации. Что это такое?



Необходимость разработки Правил стандартизации



ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

ПРАВИЛА
СТАНДАРТИЗАЦИИ

ПР — 202_
(Проект, первая редакция)

ПОРЯДОК ПРОВЕДЕНИЯ ЭКСПЕРТИЗЫ
ПРОЕКТОВ ДОКУМЕНТОВ НАЦИОНАЛЬНОЙ СИСТЕМЫ
СТАНДАРТИЗАЦИИ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Настоящий проект правил стандартизации не подлежит применению до его утверждения

Разработка правил стандартизации осуществляется во взаимосвязи с проводимыми работами по пересмотру ГОСТ Р 1.6 «Стандартизация в Российской Федерации. Проекты стандартов. Правила организации и проведения экспертизы». Обсуждается изменение ГОСТ Р 1.6, вводящее специализированный вид экспертизы – **экспертиза в области обеспечения информационной безопасности**.

Проект правил стандартизации **определяет порядок проведения и содержание экспертизы** проектов документов национальной системы стандартизации в области обеспечения информационной безопасности.

Проект Правил стандартизации «Организация проведения …»

Раздел 4 «Организация проведения экспертизы в области обеспечения информационной безопасности» проекта Правил стандартизации

4.1 Проведение экспертизы в области обеспечения информационной безопасности проектов документов национальной системы стандартизации включает следующие основные этапы:

1) проверка первой редакции проекта документа национальной системы стандартизации на предмет соответствия критериям необходимости проведения экспертизы в области обеспечения информационной безопасности;

2) экспертиза окончательной редакции проекта документа национальной системы стандартизации в области обеспечения информационной безопасности.

Проект Правил стандартизации «Организация проведения …»

Раздел 4 «Организация проведения экспертизы в области обеспечения информационной безопасности» проекта Правил стандартизации

4.1.1 На первом этапе осуществляется проверка первой редакции проекта документа национальной системы стандартизации, принятие решения о необходимости проведения экспертизы в области обеспечения информационной безопасности, в том числе дополнительной (специализированной) экспертизы в области обеспечения информационной безопасности.

4.1.2 На втором этапе осуществляется:

- экспертиза окончательной редакции проекта документа национальной системы стандартизации в области обеспечения информационной безопасности ТК в области защиты информации и/или криптографической защиты информации;

- дополнительная (специализированная) экспертиза проекта документа национальной системы стандартизации в области обеспечения информационной безопасности специализированными организациями (при необходимости).

Проект Правил стандартизации «Организация проведения …»

Разработка/доработка **первой редакции** документа НСС

Проверка первой редакции, установление необходимости проведения экспертизы в области обеспечения ИБ

необходима экспертиза

Проведение экспертизы проекта документа НСС в области обеспечения ИБ в **ТК362 и/или ТК26** (*необходимость может быть установлена на этапе экспертизы **окончательной редакции***)

обоснование невозможности представления проекта документа на утверждение …

вывод о необходимости проведения **дополнительной (специализированной) экспертизы в области обеспечения ИБ**

мотивированный вывод о **возможности представления проекта документа НСС на утверждение**

необходима доп. экспертиза

необходима доп. экспертиза

Проведение дополнительной (специализированной) экспертизы проекта документа НСС в области обеспечения ИБ **в ТК362 и/или ТК26** (*решение может принять самостоятельно разработчик и/или секретариат ТК на этапе экспертизы **окончательной редакции***)

мотивированный вывод о **соответствии/несоответствии** проекта документа требованиям в области обеспечения ИБ, а также при необходимости конкретные предложения по его доработке, в том числе предложения по устранению выявленных несоответствий (недостатков) по его содержанию и/или структуре в части требований в области обеспечения ИБ

Экспертиза пройдена. Подготовка к голосованию по проекту

Организация проведения экспертизы в области обеспечения ИБ (далее)

Основные критерии принятия решения о необходимости проведения **экспертизы в области обеспечения ИБ** проектов документов национальной системы стандартизации

- в карточке темы в качестве смежных ТК указаны ТК в области ЗИ и/или криптографической ЗИ
- проект устанавливает требования к объектам стандартизации, регулируемым законодательством в области обеспечения ИБ, ЗИ и/или криптографической ЗИИ, обеспечения безопасности КИИ РФ, обеспечения безопасности ПДн
- …

Всего 13 критериев

В соответствии с **п.4.2** проекта Правил …

Основные критерии принятия решения о необходимости проведения **дополнительной (специализированной) экспертизы в области обеспечения ИБ** проектов документов национальной системы стандартизации

- проект документа НСС содержит характеристику или порядок применения методов и средств ЗИ и/или криптографической ЗИ, не содержащиеся в действующих документах НСС в области ЗИ и/или криптографической ЗИ
- установленные в проекте требования к объектам стандартизации (с точки зрения обеспечения ИБ, ЗИ и/или криптографической ЗИ) носят фрагментарный и несистемный характер
- …

Всего 8 критериев

В соответствии с **п.4.3** проекта Правил …

Порядок и правила проведения экспертизы в области обеспечения ИБ

Проверка первой редакции, установление необходимости проведения экспертизы в области обеспечения ИБ

Анализ **первой редакции** проекта документа НСС

Направление проекта документа в секретариаты ТК в области ЗИ и/или КЗИ

Анализ проекта документа НСС и ПЗ к нему

Рассылка проекта документа в организации-члены ТК в области ЗИ и/или КЗИ для рассмотрения

Рассмотрение проекта, подготовка отзывов

Формирование *обобщенного отзыва ТК в области ЗИ и/или КЗИ* по проекту документа НСС

Обобщенный отзыв ТК в области ЗИ и/или КЗИ

обоснованный вывод о необходимости проведения экспертизы окончательной редакции в области обеспечения ИБ …

вывод о необходимости проведения дополнительной (специализированной) экспертизы в области обеспечения ИБ (если такая необходимость установлена)

Направление в адрес разработчика и секретариата ТК, в рамках деятельности которого разработан проект документа НСС

уведомление о необходимости проведения **дополнительной (специализированной) экспертизы** в области обеспечения ИБ

рекомендуемый **перечень организаций** для проведения **дополнительной (специализированной) экспертизы** в области обеспечения ИБ

Порядок и правила проведения экспертизы в области обеспечения ИБ

Экспертиза окончательной редакции проекта документа НСС в области обеспечения ИБ

Направление **окончательной редакции** проекта документа, ПЗ к нему и сводки отзывов по первой редакции в секретариат ТК в области ЗИ и/или криптографической ЗИ

Рассмотрение представленных документов и организация проведения экспертизы окончательной редакции проекта документа НСС в области обеспечения ИБ

(рассылка организациям-членам ТК)

Формирование позиций организациями-членами ТК в области ЗИ и/или криптографической ЗИ по результатам рассмотрения полученных проектов документов, в которых отражается соответствие проекта документа по стандартизации требованиям Правил …, учета разработчиком ранее сформированных замечаний и предложений по первой редакции в части требований в области обеспечения ИБ, ЗИ и/или криптографической ЗИ (при наличии)

мотивированный вывод о **возможности представления проекта документа НСС на утверждение**

либо

обоснование невозможности представления проекта документа на утверждение ввиду его несоответствия требованиям в области обеспечения ИБ, ЗИ и/или криптографической ЗИ, а также конкретные предложения по его доработке

Формирование заключения ТК, отражающего результаты экспертизы в области обеспечения ИБ, направление разработчику и в секретариат ТК, в рамках деятельности которого разработан проект документа НСС

Порядок и правила проведения экспертизы в области обеспечения ИБ

Экспертиза окончательной редакции проекта документа НСС в области обеспечения ИБ

Заключение ТК по результатам экспертизы в области обеспечения ИБ

выводы о целесообразности разработки документа НСС и/или необходимости установления в разрабатываемом или обновляемом документе положений, содержащих требования в области обеспечения ИБ, ЗИ и/или криптографической ЗИ (приложение А проекта Правил …)

…

вывод о необходимости проведения дополнительной (специализированной) экспертизы в области обеспечения ИБ (при установлении необходимости ее проведения) (приложение А проекта Правил …)

мотивированный вывод о возможности представления проекта документа НСС на утверждение, либо обоснование невозможности представления проекта документа на утверждение ввиду его несоответствия требованиям в области обеспечения ИБ, ЗИ и/или криптографической ЗИ, а также конкретные предложения по его доработке, в том числе предложения по устранению выявленных несоответствий (недостатков) по его содержанию и/или структуре в части требований в области обеспечения ИБ (при необходимости) (приложение А проекта Правил …)

Подписи

ответственный секретарь ТК председатель ТК или заместитель председателя ТК

Форма в соответствии с приложением А проекта Правил …

Порядок и правила проведения экспертизы в области обеспечения ИБ

Дополнительная (специализированная) экспертиза документа НСС

Определение одной или нескольких организаций в области деятельности ТК в области ЗИ и/или криптографической ЗИ для проведения дополнительной (специализированной) экспертизы

на основе полученных от ТК в области ЗИ и/или криптографической ЗИ перечней организаций, в которые проект документа может быть направлен для ее проведения

направление проекта документа

Проведение дополнительной (специализированной) экспертизы в области обеспечения ИБ

Оформление заключения по результатам проведения дополнительной (специализированной) экспертизы

Согласование результатов дополнительной (специализированной) экспертизы с секретариатами ТК в области ЗИ и/или КЗИ, при необходимости согласование с ФСБ России или ФСТЭК России

Направление согласованных результатов дополнительной (специализированной) экспертизы разработчику и в секретариат ТК, в области деятельности которого разрабатывается проект документа НСС

Привлечение экспертной организации. Спецэкспертиза

5.4 **Порядок определения организаций** для проведения дополнительной (специализированной) экспертизы в области обеспечения информационной безопасности

...

5.4.5 Взаимодействие разработчика и организации, осуществляющей дополнительную (специализированную) экспертизу, регламентируется их внутренними нормативными актами и иными организационно-распорядительными документами **и Гражданским кодексом Российской Федерации**

Порядок и правила проведения экспертизы в области обеспечения ИБ

Дополнительная (специализированная) экспертиза документа НСС

Заключение по результатам дополнительной (специализированной) экспертизы в области обеспечения ИБ

выводы о целесообразности разработки документа НСС и/или необходимости установления в разрабатываемом или обновляемом документе положений, содержащих требования в области обеспечения ИБ, ЗИ и/или криптографической ЗИ

…

мотивированный вывод о соответствии/несоответствия проекта документа требованиям в области обеспечения ИБ, а также при необходимости конкретные предложения по его доработке, в том числе предложения по устранению выявленных несоответствий (недостатков) по его содержанию и/или структуре в части требований в области обеспечения ИБ

Подпись
руководитель организации, проводившей дополнительную (специализированную) экспертизу в области обеспечения ИБ

Форма в соответствии с приложением Б проекта Правил …

Порядок и правила проведения экспертизы в области обеспечения ИБ

Выводы по результатам экспертизы в области обеспечения ИБ

При отрицательных результатах рассмотрения и экспертизы проекта документа НСС секретариат ТК в области ЗИ и/или криптографической ЗИ

направляет разработчику

предложения по устранению выявленных несоответствий (недостатков) по его содержанию и/или структуре (в части требований в области обеспечения ИБ, ЗИ и/или криптографической ЗИ) и может предложить разработчику доработать проект документа и представить его на рассмотрение в ТК в области ЗИ и/или криптографической ЗИ для повторного проведения экспертизы в области обеспечения ИБ

направляет в национальный орган по стандартизации

уведомление об отрицательных результатах рассмотрения и экспертизы проекта документа НСС

Направление на утверждение проекта документа НСС, соответствующего критериям проведения экспертизы в области обеспечения ИБ, **без положительного заключения** ТК в области ЗИ и/или криптографической ЗИ **не допускается**

Заключение. Резюме

Ожидаемые результаты …

Совершенствование организации работ по стандартизации требований ИБ

- Организация совместной системной работы причастных ТК
- Недопущение разработки и принятия документов НСС, несоответствующих действующему законодательству РФ, НПА и документам по стандартизации в области обеспечения ИБ
- Недопущение применения в Российской Федерации решений, несогласованных с Регуляторами – ФСБ России и ФСТЭК России
- Создание условий для разработки и применения надежных и высокоэффективных отечественных решений (методов и средств) по ЗИ/КЗИ

«… совершенствование деятельности производственных, научных и научно-технических организаций по разработке, производству и эксплуатации средств обеспечения ИБ, оказанию услуг в области обеспечения ИБ», (из документа «***Доктрина информационной безопасности Российской Федерации***», п. 8, перечисление в)

Подписывайтесь
на наши соцсети,
там много интересного

infotecs

Спасибо
за внимание!