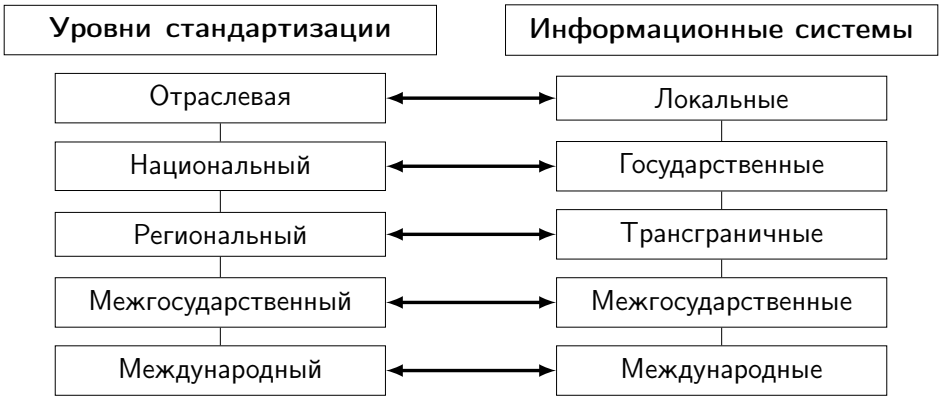
О вопросах национальной, межгосударственной и международной стандартизации в области криптографической защиты информации

Александр Бондаренко,
Антон Гуселев

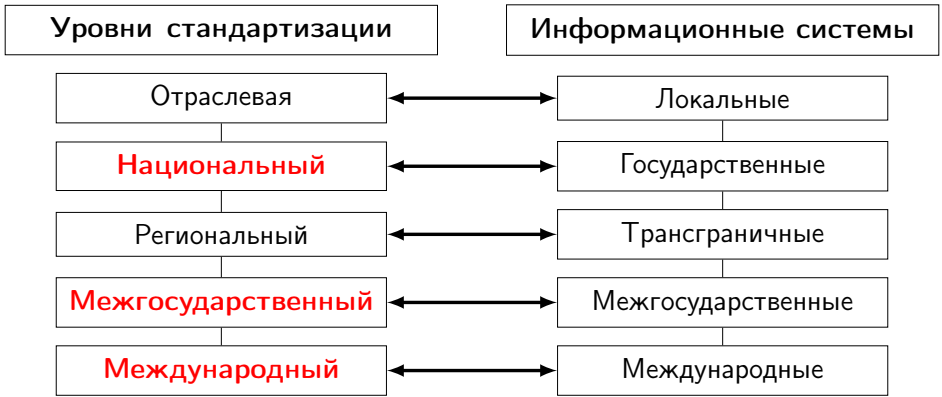
– PKI-Форум Россия 2018 –

Концепция стандартизации



*Соблюдение интересов Российской Федерации на всех уровнях – основа безопасности информационных систем

Концепция стандартизации



*Соблюдение интересов Российской Федерации на всех уровнях – основа безопасности информационных систем

Технический комитет по стандартизации «Криптографическая защита информации» (ТК 026)

«ТК 026 является формой сотрудничества заинтересованных организаций, органов власти и физических лиц при проведении работ по ***национальной***, ***межгосударственной*** *и* ***международной*** *стандартизации в закрепленной сфере деятельности...»*

Положение о ТК 026

За ТК 026 среди прочего закреплены *«...объекты стандартизации, относящиеся к методам шифрования (криптографического преобразования) информации, способам их реализации, а также методам обеспечения безопасности информационных технологий с использованием криптографического преобразования информации, включая аутентификацию, имитозащиту и электронную цифровую подпись...»*

Приказ Росстандарта от 09.06.2017 № 1319

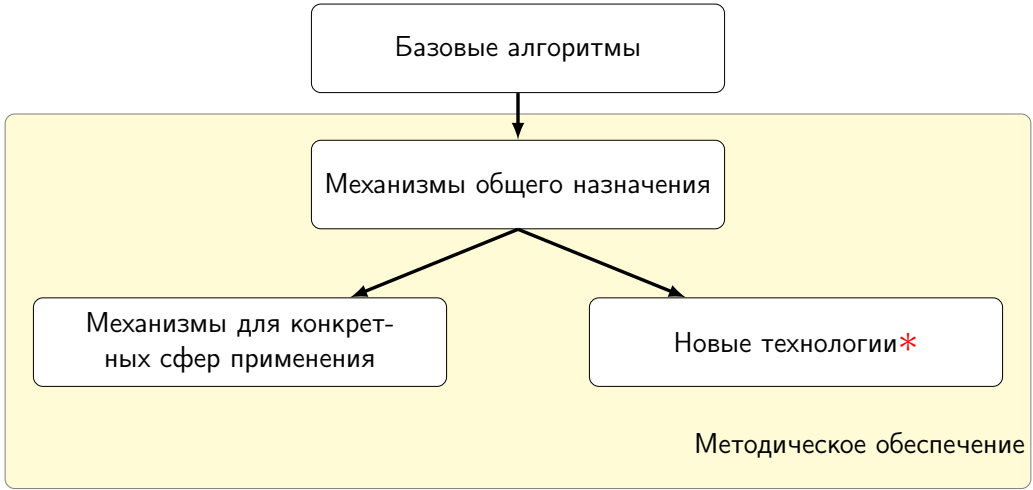
Структура ТК 026

Состав: более 60 организаций участников

Подкомитет № 1	Подкомитет № 2	Подкомитет № 3	Подкомитет № 4	Рабочая группа № 1
«Криптографические алгоритмы и протоколы для применения в ... шифровальных (криптографических) средствах защиты информации, содержащей сведения, составляющие государственную тайну»	«Криптографические алгоритмы и протоколы для применения в ... шифровальных (криптографических) средствах защиты информации, содержащей сведения ... ограниченного доступа»	«Криптографические алгоритмы и механизмы в национальной платежной системе Российской Федерации»	«Российские шифровальные (криптографические) средства защиты информации, не содержащей сведений, составляющих государственную тайну или ... информации ограниченного доступа, а также зарубежные шифровальные (криптографические) средства защиты информации...»	«Процедуры и регламенты ТК 026»
	Рабочая группа 2.1 Рабочая группа 2.2 Рабочая группа 2.3 Рабочая группа 2.4	Рабочая группа 3.1	Рабочая группа 4.1 Рабочая группа 4.2 Рабочая группа 4.3 Рабочая группа 4.4	

*Основная особенность стандартизации – экспертиза документов только вместе с анализом безопасности

Основные направления стандартизации



*Разработка не только криптографических механизмов, удовлетворяющих современным требованием, но и создание понятийного аппарата, в случае его отсутствия

Национальная стандартизация. Стандарты

4 национальных стандарта
(обновление «старых» завершено в 2015 году)

- Процессы формирования и проверки электронной цифровой подписи
  (Длина подписи 512 или 1024 бита)
- Функция хэширования
  (Длина хэш-кода 256 и 512 бит)
- Блочные шифры
  («Магма» – длина блока 64 бита, «Кузнечик» – длина блока 128 бит)
- Режимы работы блочных шифров
  (6 режимов работы блочных шифров)

«Документ, содержащий советы организационно-методического характера, которые касаются проведения работ по стандартизации и способствуют применению основополагающего национального стандарта или содержат положения, которые целесообразно предварительно проверить на практике до их установления в основополагающем национальном стандарте»

ГОСТ Р 1.12-2004

Национальная стандартизация. Рекомендации по стандартизации

Текущее состояние:

Утверждено 23 рекомендации по стандартизации
(6 – 2016, 11 – 2017, 6 – 2018)

Из них 2017 и 2018 годах:

- 3 – механизмы общего назначения
  (датчик, выработка общего ключа, режимы)
- 2 – методическое обеспечение
  (объемы материала и принципы разработки и модернизации)
- конкретные сферы:
  - 8 – национальная система платежных карт *(альтернатива RSA)*
  - 1 – мобильные системы связи *(замена Milenage и Tuak)*
  - 1 – транспорт (тахографы) *(новая разработка)*
  - 1 – контрольно-кассовая техника *(новая разработка)*
  - 1 – системы интернет взаимодействия *(TLS 1.2)*

Национальная стандартизация. Методические рекомендации и Технические спецификации

Методические рекомендации используются для апробации рекомендаций по стандартизации перед утверждением Росстандартом.

Опубликовано 2 методических рекомендаций

Технические спецификации устанавливает определенные технические требования к изготавливаемым изделиям (обязательно к исполнению только в случае договоренности)

Утверждено 6 технических спецификаций

Ближайшая перспектива

Стандартизация на 2018 год *(рекомендации по стандартизации)*

- Использование национальных стандартов в сообщениях формата CMS *(Cryptographic Message Syntax)*
- Использования алгоритмов ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012 в инфраструктуре открытых ключей X.509
- Функции выработки производного ключа *(KDF)*
- Режимы работы блочных шифров, реализующие имитозащищенное шифрование *(AEAD)*

Исследования в перспективных областях *(методические рекомендации)*

- Термины и определения в области технологий цепной записи данных (блокчейн) и распределенных реестров

Межгосударственная стандартизация. Действующие стандарты

- **Блочный шифр** – ГОСТ 28147-89
  («входит» в состав ГОСТ Р 34.12-2015)
- **Функция хэширования** – ГОСТ 34.311-95
  (идентичен ~~ГОСТ 34.11-94~~ $\Longrightarrow$ заменен ГОСТ Р 34.11-2012)
- **Подпись** – ГОСТ 34.310-2004
  (идентичен ~~ГОСТ 34.10-2001~~ $\Longrightarrow$ заменен ГОСТ Р 34.10-2012)

*Инициатива Российской Федерации

Межгосударственная стандартизация. Обновление стандартов

Головной орган:
Межгосударственный совет по стандартизации, метрологии и сертификации *(страны СНГ и Грузия)*

«Программа работ по межгосударственной стандартизации на 2016-2018 гг.» *(актуализация 2017 г.)*: разработка 4 межгосударственных стандартов в области криптографической защиты информации на основе российских стандартов *(инициатива Российской Федерации)*

Уже

1. подготовлены первые редакции проектов межгос стандартов
2. проведена процедура их обсуждения
3. стандарты доработаны по результатам обсуждения и подготовлены окончательные редакции межгос стандартов
4. проекты переданы в совет для проведения процедуры голосования

однако к настоящему моменту отзывов получено не было

Международная стандартизация. Направления работы

Международная организация по стандартизации
(International Organization for Standardization, ISO)

Инженерный совет интернета
(Internet Engineering Task Force, IETF)

Organization for the Advancement of Structured Information Standards, OASIS

WiFi Alliance

Международная стандартизация. ISO

В соответствии с Приказом Росстандарта от 09.06.2017 № 1319 за ТК 026 закреплено проведение работы по направлениям

- подкомитет 27 «Методы защиты ИТ» 1 объединенного технического комитета ИСО «Информационные технологии»
  (ISO/JTC1/SC27 «Cryptography and security mechanisms»)
- технический комитет ИСО 307 «Технологии цепной записи данных и распределенных реестров»
  (ICO TC 307 «Blockchain and electronic distributed ledger technologies»)

Международная стандартизация. ISO. Текущие результаты

1. **подготовлена** новая редакция стандарта ISO/IEC 10118-3
   включает хэш-функцию из ГОСТ Р 34.11-2012,
   !!! заключительная стадия *(принятие ожидается в 2018 году)* !!!
2. **подготовлен** проект дополнения к стандарту ISO/IEC 18033-3 включает блочный шифр «Кузнечик» из ГОСТ Р 34.12-2015
   !!! прошел процедуру голосования однако принято решение включить данное дополнение в основной текст стандарта $\Longrightarrow$
   подготовка нового документа *(принятие возможно 2019-2020 годах)* !!!
3. **подготовлен** проект новой редакции стандарта ISO/IEC 9797-2
   включает механизмы выработки имитовставок из Р 50.1.113-2016
4. **начато изучения возможности** принятия документа ISO, определяющего механизмы из Р 1323565.1.017-2018
   (смена ключа во время работы режима шифрования).

Международная стандартизация. ISO. Текущие результаты

Методические рекомендаций ТК 026, определяющие терминологию в области цепной записи данных (блокчейн), использованы при формировании экспертной позиции Российской Федерации по соответствующему вопросу повестки международного комитета ИСО ТК 307

Заседание комитета ИСО ТК 307 пройдет в Москве 22-25 октября 2018 года – участники уполномоченные представители Росстандарта

26 октября – Международный форум о практике применения блокчейн-технологий «Блокчейн в цифровой экономике»
– участники все желающие

Текущее состояние:

12 спецификаций с описанием отечественных решений

(в некоторых из них описаны устаревшие стандарты)

При этом в

- 3 из них *(RFC 6986, RFC 7091, RFC 7801)* описаны действующие стандарты ГОСТ + 1 RFC с описанием ГОСТ 28147-89
- 2 из них *(RFC 7836, RFC 8133)* описаны действующие рекомендации по стандартизации

Международная стандартизация

OASIS – **подготовлена** 1 спецификация с описанием применения национальных стандартов

WiFi Alliance – эксперты ТК 026 вошли в состав экспертов занимающихся анализом безопасности базового протокола WiFi

План мероприятий по направлению «Информационная безопасность»:

«Создать эффективные механизмы государственного регулирования и поддержки в области информационной безопасности при интеграции национальной цифровой экономики в международную экономику»

«Национальные стандарты в области информационной безопасности гармонизированы с международными, региональными и отраслевыми стандартами с учетом интересов Российской Федерации»

Актуальные направления стандартизации

- Развитие криптографических протоколов, реализующих безопасный обмен информацией в глобальных информационно-телекоммуникационных системах и сетях связи, в том числе протокола TLS 1.3, реализующего российские криптографические механизмы
- Развитие постквантовых криптографических механизмов и протоколов
- Развитие криптографических механизмов и протоколов для определенных функциональных областей (отраслей) применения, например, транспорт, энергетика, медицина и т.д.

СПАСИБО ЗА ВНИМАНИЕ!

Вопросы?