Национальная, межгосударственная и международная стандартизация в области криптографии

Бондаренко А.И.

ФСБ России

XXIII научно-практическая конференция
«Комплексная защита информации»

О чём этот доклад?

Национальная/межгосударственная/международная стандартизация в области криптографической защиты информации

- Текущее состояние
- Ближайшие перспективы
- Новые направления

Уровни стандартизации

Национальная/межгосударственная/международная стандартизация в области криптографической защиты информации

- Базовые алгоритмы
- Общие конструкции
- Спецификации для конкретных сфер применения

Национальная стандартизация. Стандарты

ГОСТ Р 34.10-2012 – Процессы формирования и проверки ЭЦП

- Может быть представлена в виде двоичного вектора длиной 512 или 1024 бита

ГОСТ Р 34.11-2012 – Функция хэширования

- Две функции хэширования с длиной хэш-кода 256 и 512 бит

ГОСТ Р 34.12-2015 – Блочные шифры

- Два блочных шифра: «Магма» - длина блока 64 бита, «Кузнечик» - длина блока 128 бит

ГОСТ Р 34.13-2015 – Режимы работы блочных шифров

- Шесть режимов работы блочных шифров, включая один режим выработки имитовставки

Криптографические исследования базовых алгоритмов и исследования их эксплуатационных характеристик

- www.tc26.ru/events/publikatcii-i-izdaniia/
- www.eprint.iacr.org
- www.ctcrypt.ru
- www.ruscrypto.ru
- www.itsec.ru
- www.xakep.ru

Национальная стандартизация. Рекомендации по стандартизации

- Обеспечивают применение базовых криптографических стандартов при разработке средств криптографической защиты информации
- Разрабатываются и проходят всестороннюю экспертизу в рамках деятельности Технического комитета по стандартизации «Криптографическая защита информации» (ТК 26), членами которого являются более 60 организаций
- Перед утверждением Росстандартом, как правило, апробируются в течение года в качестве методических рекомендаций ТК 26
- Доступны для ознакомления на www.tc26.ru или tc26@tc26.ru (по запросу)

Национальная стандартизация. Рекомендации по стандартизации – 2016

- Р 50.1.110–2016 – Контейнер хранения ключей
- Р 50.1.111–2016 – Парольная защита ключевой информации
- Р 50.1.112–2016 – Транспортный ключевой контейнер
- Р 50.1.113–2016 – Криптографические алгоритмы, сопутствующие применению алгоритмов электронной цифровой подписи и функции хэширования *(HMAC, PRF, DH, KDF)*
- Р 50.1.114–2016 – Параметры эллиптических кривых для криптографических алгоритмов и протоколов
- Р 50.1.115–2016 – Протокол выработки общего ключа с аутентификацией на основе пароля

Национальная стандартизация. Рекомендации по стандартизации – 2017

- Р 1323565.1.003-2017 – Криптографические алгоритмы выработки ключей шифрования информации и аутентификационных векторов, предназначенные для реализации в аппаратных модулях доверия для использования в подвижной радиотелефонной связи
- Р 1323565.1.004-2017 – Схемы выработки общего ключа с аутентификацией на основе открытого ключа
- Р 1323565.1.005-2017 – Допустимые объемы материала для обработки на одном ключе при использовании некоторых вариантов режимов работы блочных шифров
- Р 1323565.1.006-2017 – Механизмы выработки псевдослучайных последовательностей
- Р 1323565.1.012-2017 – Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации

Национальная стандартизация. Рекомендации по стандартизации – 2017. Национальная платёжная система

- Р 1323565.1.007-2017 – Использование алгоритмов блочного шифрования при формировании проверочного значения платежной карты и проверочного значения PIN
- Р 1323565.1.008-2017 – Использование режимов алгоритма блочного шифрования и имитозащиты в защищенном обмене сообщениями между эмитентом и платежным приложением
- Р 1323565.1.009-2017 – Использование алгоритмов имитозащиты блочного шифрования при формировании прикладных криптограмм в платежных системах
- Р 1323565.1.010-2017 – Использование функции диверсификации для формирования производных ключей платежного приложения

Национальная стандартизация. Рекомендации по стандартизации – 2017-18. Национальная платёжная система

- Р 1323565.1.011-2017 – Использование алгоритмов согласования ключа и блочного шифрования при оффлайновой проверке PIN
- Р 1323565.1.013-2017 – Использование режимов алгоритма блочного шифрования в протоколе защищенного обмена сообщениями в процессе эмиссии платежных карт
- Р 1323565.1.015-2018 – Задание параметров алгоритмов электронной подписи и функции хэширования в профиле EMV сертификатов открытых ключей платежных систем
- Р 1323565.1.016-2018 – Использование режимов алгоритма блочного шифрования, алгоритмов электронной подписи и функции хэширования в процедуре оффлайновой аутентификации платежного приложения

Национальная стандартизация. Программа национальной стандартизации на 2018 год

Проекты документов

- Использование алгоритмов, определенных национальными стандартами, в сообщениях формата CMS
- Функции выработки производного ключа
- Режимы работы блочных шифров, реализующие аутентифицированное шифрование
- Использование российских криптографических алгоритмов в протоколе безопасности транспортного уровня (TLS 1.2)
- Протокол защищенного обмена для индустриальных систем

Национальная стандартизация. Рекомендации по стандартизации – 2018

- Р 1323565.1.017-2018 – Криптографические алгоритмы, сопутствующие применению алгоритмов блочного шифрования
- Р 1323565.1.018-2018 – Криптографические механизмы аутентификации в контрольных устройствах для автотранспорта

Действующие межгосударственные стандарты

- ГОСТ 28147-89 – блочный шифр (присоединились: Белоруссия, Казахстан, Молдавия, Россия, Украина)
- ГОСТ 34.311-95 – функция хэширования, на базе ГОСТ Р 34.11-94 (присоединились: Азербайджан, Армения, Белоруссия, Казахстан, Кыргызстан, Молдавия, Россия, Таджикистан, Туркменистан)
- ГОСТ 34.310-2004 – электронная цифровая подпись, на базе ГОСТ Р 34.10-2001 (присоединились: Азербайджан, Армения, Казахстан, Кыргызстан, Молдавия, Россия, Таджикистан, Туркменистан, Узбекистан)

Межгосударственные стандарты и национальные стандарты РФ

- ГОСТ 28147-89 (блочный шифр и режимы его работы) действует одновременно с ГОСТ Р 34.12-2015 (два блочных шифра, в том числе определенный ГОСТ 28147-89 – «Магма») и ГОСТ Р 34.13-2015 (режимы работы блочных шифров)
- ГОСТ Р 34.10-2001 выведен из действия и заменен на ГОСТ Р 34.10-2012
- ГОСТ Р 34.11-94 выведен из действия и заменен на ГОСТ Р 34.11-2012
- Планомерный переход на новые стандарты, определяющие процессы формирования и проверки ЭП и функцию хэширования
- Использование схем подписи ГОСТ 34.10-2001 для формирования подписи после 31 декабря 2018 года не допускается

Программа работ по межгосударственной стандартизации на 2016-2018 гг. (актуализация 2017 г.)

- Принята решением 50-го заседания Межгосударственного совета по стандартизации, метрологии и сертификации в декабре 2016
- Включает разработку межгосударственных стандартов в области криптографической защиты информации на базе ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012, ГОСТ Р 34.12-2015, ГОСТ Р 34.13-2015
- Заинтересованные государства – все члены МГС

Программа работ по межгосударственной стандартизации на 2016-2018 гг. (актуализация 2017 г.)

- Октябрь 2017 – подготовлены первые редакций проектов стандартов
- Получены отзывы от пяти российских организаций
- Получены отзывы от Белоруссии и Кыргызстана
- Осуществляется подготовка сводок отзывов и корректировка проектов
- Июнь 2018 – представление окончательных редакций проектов
- Ноябрь 2018 – направление проектов в Бюро МГС на принятие

Международная организация по стандартизации

- опубликован стандарт ISO/IEC 10118-1:2016, определяющий общие требования к функциям хэширования – первый стандарт ISO в области криптографии, полностью разработанный российскими специалистами
- подготовленная новая редакция международного стандарта ISO/IEC 10118-3, включающая функции хэширования «Стрибог», определяемые национальным стандартом ГОСТ Р 34.11-2012, переведена на предфинальную стадию
- подготовленный проект дополнения к международному стандарту ISO/IEC 18033-3, содержащий описание алгоритма блочного шифрования «Кузнечик», определяемого национальным стандартом ГОСТ Р 34.12-2015, переведен на предфинальную стадию

План мероприятий по направлению «Информационная безопасность»

- информационно-аналитическое обеспечение и координация участия российских экспертов по криптографии и информационной безопасности в деятельности основных международных организаций
- обеспечение непрерывного и скоординированного участия российских экспертов по криптографии и информационной безопасности в разработке, научном обосновании и экспертизе (проектов) международных стандартов
- поддержка механизмов участия российских экспертов, представляющих национальные интересы Российской Федерации, в деятельности основных международных организаций

Вместо заключения: актуальные направления

- криптографические механизмы, перспективные для реализации в современных информационно-телекоммуникационных протоколах
- использование российских криптографических механизмов в протоколе TLS 1.3
- стандартизация постквантовых криптографических механизмов