Развитие системы стандартов в области криптографической защиты информации

Бондаренко Александр

bondarenko_ai@tc26.ru

Национальные стандарты в области криптографической защиты информации

- ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи».
  - Электронной цифровой подписи, которая может быть представлена в виде двоичного вектора длиной 512 или 1024 бита;
- ГОСТ Р 34.11-2012 «Информационная технология. Криптографическая защита информации. Функция хэширования».
  - Две функции хэширования с длиной хэш-кода 256 и 512 бит;
- ГОСТ Р 34.12-2015 «Информационная технология. Криптографическая защита информации. Блочные шифры».
  - Два блочных шифра: «Магма» - длина блока 64 бита, «Кузнечик» - длина блока 128 бит;
- ГОСТ Р 34.13-2015 «Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров».
  - Шесть режимов работы блочных шифров, включая один режим выработки имитовставки.

Рекомендации по стандартизации

- 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»;
- 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».

Программа национальной стандартизации на 2017 год

- Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации;
- Криптографические алгоритмы выработки ключей шифрования информации и аутентификационных векторов, предназначенные для реализации в аппаратных модулях доверия для использования в подвижной радиотелефонной связи;
- Схемы выработки общего ключа с аутентификацией на основе открытого ключа;
- Механизмы выработки псевдослучайных последовательностей;
- Допустимые объёмы материала для обработки на одном ключе при использовании некоторых вариантов режимов работы блочных шифров в соответствии с ГОСТ Р 34.13-2015.

Безопасное взаимодействие с использованием банковских карт

- Использование функции диверсификации для формирования производных ключей платёжного приложения;
- Использование режимов алгоритма блочного шифрования в протоколе защищённого обмена сообщениями в процессе эмиссии платёжных карт;
- Использование алгоритмов согласования ключа и блочного шифрования при офлайновой проверке PIN;
- Использование алгоритмов имитозащиты блочного шифрования при формировании прикладных криптограмм в платёжных системах;
- Использование алгоритмов блочного шифрования при формировании проверочного значения платёжной карты и проверочного значения PIN;
- Использование режимов алгоритма блочного шифрования и имитозащиты в защищённом обмене сообщениями между эмитентом и платёжным приложением.

Блокчейн

- Целесообразность стандартизации данных технологий;
- Описать предметную область стандартизации с точки зрения криптографии;
- Отдельный круглый стол.

Перспективы

- Криптографические механизмы, обеспечивающие одновременно шифрование и аутентификацию данных;
- Развитие постквантовых криптографических механизмов и протоколов;
- Развитие криптографических протоколов, реализующих безопасный обмен информацией в глобальных информационно-телекоммуникационных системах и сетях связи.

Межгосударственный совет по стандартизации, метрологии и сертификации

- На 50-ом заседании Межгосударственного совета по стандартизации, метрологии и сертификации (МГС) утверждена актуализированная на 2017 год «Программа работ по межгосударственной стандартизации на 2016-2018 гг.»;
- Разработка четырех межгосударственных стандартов в области криптографической защиты информации на основе российских стандартов, определяющих базовые криптографические алгоритмы;
- Разработка первых редакций - конец 2017 года;
- Представление в МГС окончательных редакций - 2018 год.

27-ой подкомитет 1-го объединённого ТК Международной организации по стандартизации

- Опубликован стандарт ISO/IEC 10118-1:2016, определяющий общие требования к функциям хэширования и разработанный российскими специалистами;
- Стандарт ISO/IEC 10118-3, включающий описание хэш-функций, определяемых стандартом ГОСТ Р 34.11-2012 переведён на стадию финального голосования на уровне национальных комитетов и планируется к утверждению и публикации в 2018 году;
- Начат комплекс мероприятий по включению алгоритма блочного шифрования «Кузнечик» в стандарт ISO/IEC 18033-3.

Инженерный совет Интернета (IETF)

- Март 2016 – RFC 7801 «GOST R 34.12-2015: Block Cipher “Kuznyechik”» описывает определяет блочный шифр «Кузнечик»;
- Март 2016 – RFC 7836 «Guidelines on the Cryptographic Algorithms to Accompany the Usage of Standards GOST R 34.10-2012 and GOST R 34.10-2012» описывает криптографические алгоритмы, сопутствующие применению алгоритмов электронной цифровой подписи и функции хэширования, определенные рекомендациями по стандартизации Р 50.1.113-2016;
- Март 2016 – RFC 8133 «The Security Evaluated Standardized Password-Autenticated Key Exchange (SESPAKE) Protocol» описывает протокол выработки общего ключа с аутентификацией на основе пароля, определенный рекомендациями по стандартизации Р 50.1.115-2016.

307 ТК
Международной организации по стандартизации

- Создана исследовательская группа по безопасности соответствующих технологических решений, которую возглавил специалист из Российской Федерации.

Вопросы???