Национальная и международная стандартизация в области криптографии

Д.В. Матюхин

ФСБ России

VI Форум АЗИ
«Актуальные вопросы информационной безопасности»

О чём этот доклад?

О чём этот доклад?

Национальная/межгосударственная/международная стандартизация в области криптографической защиты информации

О чём этот доклад?

Национальная/межгосударственная/международная стандартизация в области криптографической защиты информации

- Основные события за период с апреля 2016 года

О чём этот доклад?

Национальная/межгосударственная/международная стандартизация в области криптографической защиты информации

- Основные события за период с апреля 2016 года
- Что ещё предстоит сделать?

О чём этот доклад?

Национальная/межгосударственная/международная стандартизация в области криптографической защиты информации

- Основные события за период с апреля 2016 года
- Что ещё предстоит сделать?
- Какие новые направления появились?

Национальная стандартизация

Национальная стандартизация

2015 – завершено обновление *базовых стандартов*

Национальная стандартизация

2015 – завершено обновление *базовых стандартов*

2016 – Росстандартом утверждены *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 *(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

Рекомендации по стандартизации

Рекомендации по стандартизации

- обеспечивают применение базовых стандартов при разработке средств криптографической защиты информации

Рекомендации по стандартизации

- обеспечивают применение базовых стандартов при разработке средств криптографической защиты информации
- разрабатываются в рамках деятельности Технического комитета по стандартизации «Криптографическая защита информации» (ТК 26)

Рекомендации по стандартизации

- обеспечивают применение базовых стандартов при разработке средств криптографической защиты информации
- разрабатываются в рамках деятельности Технического комитета по стандартизации «Криптографическая защита информации» (ТК 26)
- перед утверждением Росстандартом, как правило, апробируются в качестве *методических рекомендаций ТК 26*

Рекомендации по стандартизации

- обеспечивают применение базовых стандартов при разработке средств криптографической защиты информации
- разрабатываются в рамках деятельности Технического комитета по стандартизации «Криптографическая защита информации» (ТК 26)
- перед утверждением Росстандартом, как правило, апробируются в качестве *методических рекомендаций ТК 26*
- доступны для ознакомления на http://tc26.ru/standard/rs/, http://tc26.ru/methods/recommendation/

Программа разработки национальных стандартов - 2017

Программа разработки национальных стандартов - 2017

Проекты рекомендаций по стандартизации, рекомендованные ТК 26 к утверждению Росстандартом, разработанные ФСБ России

Программа разработки национальных стандартов - 2017

Проекты рекомендаций по стандартизации, рекомендованные ТК 26 к утверждению Росстандартом, разработанные ФСБ России

- 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

Программа разработки национальных стандартов - 2017

Проекты рекомендаций по стандартизации, рекомендованные ТК 26 к утверждению Росстандартом, разработанные ПК 3 «Криптографические алгоритмы и механизмы в национальной платёжной системе РФ»

Программа разработки национальных стандартов - 2017

Проекты рекомендаций по стандартизации, рекомендованные ТК 26 к утверждению Росстандартом, разработанные ПК 3 «Криптографические алгоритмы и механизмы в национальной платёжной системе РФ»

- Использование функции диверсификации для формирования производных ключей платежного приложения
- Использование алгоритмов согласования ключа и блочного шифрования при офлайновой проверке PIN
- Использование алгоритмов имитозащиты блочного шифрования при формировании прикладных криптограмм в платежных системах
- Использование алгоритмов блочного шифрования при формировании проверочного значения платежной карты и проверочного значения PIN
- Использование режимов алгоритма блочного шифрования и имитозащиты в защищенном обмене сообщениями между эмитентом и платежным приложением

Национальная стандартизация: новые направления

Технологии цепной записи данных (блокчейн) и распределённых реестров

Технологии цепной записи данных (блокчейн) и распределённых реестров

- целесообразность и предметная область стандартизации с точки зрения криптографии?

Технологии цепной записи данных (блокчейн) и распределённых реестров

- целесообразность и предметная область стандартизации с точки зрения криптографии?
- ноябрь 2016 – в ТК 26 создана временная рабочая группа по безопасности технологий ЦЗД и РР

Технологии цепной записи данных (блокчейн) и распределённых реестров

- целесообразность и предметная область стандартизации с точки зрения криптографии?
- ноябрь 2016 – в ТК 26 создана временная рабочая группа по безопасности технологий ЦЗД и РР
  - проект терминологического справочника – ноябрь 2017

Технологии цепной записи данных (блокчейн) и распределённых реестров

- целесообразность и предметная область стандартизации с точки зрения криптографии?
- ноябрь 2016 – в ТК 26 создана временная рабочая группа по безопасности технологий ЦЗД и РР
  - проект терминологического справочника – ноябрь 2017
  - проект документа по общим моделям безопасности – март 2018

Технологии цепной записи данных (блокчейн) и распределённых реестров

- целесообразность и предметная область стандартизации с точки зрения криптографии?
- ноябрь 2016 – в ТК 26 создана временная рабочая группа по безопасности технологий ЦЗД и РР
  - проект терминологического справочника – ноябрь 2017
  - проект документа по общим моделям безопасности – март 2018
- дискуссия «Блокчейн: ожидания рынка и мнения экспертов» в программе CTCrypt 2017

Национальная стандартизация: новые направления

Технологии цепной записи данных (блокчейн) и распределённых реестров

- целесообразность и предметная область стандартизации с точки зрения криптографии?
- ноябрь 2016 – в ТК 26 создана временная рабочая группа по безопасности технологий ЦЗД и РР
  - проект терминологического справочника – ноябрь 2017
  - проект документа по общим моделям безопасности – март 2018
- дискуссия «Блокчейн: ожидания рынка и мнения экспертов» в программе CTCrypt 2017

Криптография в цифровых контрольных устройствах

Национальная стандартизация: новые направления

Технологии цепной записи данных (блокчейн) и распределённых реестров

- целесообразность и предметная область стандартизации с точки зрения криптографии?
- ноябрь 2016 – в ТК 26 создана временная рабочая группа по безопасности технологий ЦЗД и РР
  - проект терминологического справочника – ноябрь 2017
  - проект документа по общим моделям безопасности – март 2018
- дискуссия «Блокчейн: ожидания рынка и мнения экспертов» в программе CTCrypt 2017

Криптография в цифровых контрольных устройствах

- ноябрь 2016 – в ТК 26 создана рабочая группа по использованию криптографических механизмов в ЦКУ

Национальная стандартизация: новые направления

Технологии цепной записи данных (блокчейн) и распределённых реестров

- целесообразность и предметная область стандартизации с точки зрения криптографии?
- ноябрь 2016 – в ТК 26 создана временная рабочая группа по безопасности технологий ЦЗД и РР
  - проект терминологического справочника – ноябрь 2017
  - проект документа по общим моделям безопасности – март 2018
- дискуссия «Блокчейн: ожидания рынка и мнения экспертов» в программе CTCrypt 2017

Криптография в цифровых контрольных устройствах

- ноябрь 2016 – в ТК 26 создана рабочая группа по использованию криптографических механизмов в ЦКУ
- РГ представила 2 проекта рекомендаций по стандартизации

Межгосударственная стандартизация

Межгосударственная стандартизация

- Межгосударственный совет по стандартизации, метрологии и сертификации (МГС) объединяет страны СНГ и Грузию

Межгосударственная стандартизация

- Межгосударственный совет по стандартизации, метрологии и сертификации (МГС) объединяет страны СНГ и Грузию
- В настоящее время действуют 3 межгосударственных стандарта в области криптографической защиты информации:

Межгосударственная стандартизация

- Межгосударственный совет по стандартизации, метрологии и сертификации (МГС) объединяет страны СНГ и Грузию
- В настоящее время действуют 3 межгосударственных стандарта в области криптографической защиты информации:
  - шифрования ГОСТ 28147-89 (присоединились: Белоруссия, Казахстан, Молдавия, Россия, Украина)

Межгосударственная стандартизация

- Межгосударственный совет по стандартизации, метрологии и сертификации (МГС) объединяет страны СНГ и Грузию
- В настоящее время действуют 3 межгосударственных стандарта в области криптографической защиты информации:
  - шифрования ГОСТ 28147-89 (присоединились: Белоруссия, Казахстан, Молдавия, Россия, Украина)
  - функции хэширования на базе ГОСТ Р 34.11-94 (присоединились: Азербайджан, Армения, Белоруссия, Казахстан, Кыргызстан, Молдавия, Россия, Таджикистан, Туркменистан)

Межгосударственная стандартизация

- Межгосударственный совет по стандартизации, метрологии и сертификации (МГС) объединяет страны СНГ и Грузию
- В настоящее время действуют 3 межгосударственных стандарта в области криптографической защиты информации:
  - шифрования ГОСТ 28147-89 (присоединились: Белоруссия, Казахстан, Молдавия, Россия, Украина)
  - функции хэширования на базе ГОСТ Р 34.11-94 (присоединились: Азербайджан, Армения, Белоруссия, Казахстан, Кыргызстан, Молдавия, Россия, Таджикистан, Туркменистан)
  - электронной цифровой подписи на базе ГОСТ Р 34.10-2001 (присоединились: Азербайджан, Армения, Казахстан, Кыргызстан, Молдавия, Россия, Таджикистан, Туркменистан, Узбекистан)

Межгосударственная стандартизация

- Межгосударственный совет по стандартизации, метрологии и сертификации (МГС) объединяет страны СНГ и Грузию
- В настоящее время действуют 3 межгосударственных стандарта в области криптографической защиты информации:
  - шифрования ГОСТ 28147-89 (присоединились: Белоруссия, Казахстан, Молдавия, Россия, Украина)
  - функции хэширования на базе ГОСТ Р 34.11-94 (присоединились: Азербайджан, Армения, Белоруссия, Казахстан, Кыргызстан, Молдавия, Россия, Таджикистан, Туркменистан)
  - электронной цифровой подписи на базе ГОСТ Р 34.10-2001 (присоединились: Азербайджан, Армения, Казахстан, Кыргызстан, Молдавия, Россия, Таджикистан, Туркменистан, Узбекистан)
- Из указанных ГОСТов в качестве национального стандарта РФ действует только ГОСТ 28147-89 (одновременно с ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015) – ГОСТ Р 34.11-94 и ГОСТ Р 34.10-2001 заменены на ГОСТ Р 34.11-2012 и ГОСТ Р 34.10-2012

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

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

- Принята решением 50-го заседания МГС 8 декабря 2016 г.

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

- Принята решением 50-го заседания МГС 8 декабря 2016 г.
- 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

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

- Принята решением 50-го заседания МГС 8 декабря 2016 г.
- 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.)

- Принята решением 50-го заседания МГС 8 декабря 2016 г.
- 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
  - Рассылка первых редакций проектов – октябрь 2017

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

- Принята решением 50-го заседания МГС 8 декабря 2016 г.
- 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
  - Рассылка первых редакций проектов – октябрь 2017
  - Представление окончательных редакций проектов – июнь 2018

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

- Принята решением 50-го заседания МГС 8 декабря 2016 г.
- 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
  - Рассылка первых редакций проектов – октябрь 2017
  - Представление окончательных редакций проектов – июнь 2018
  - Направление проектов в Бюро МГС на принятие – ноябрь 2018

Международная стандартизация

Международная организация по стандартизации (ISO)

Международная организация по стандартизации (ISO)

- опубликован стандарт ISO/IEC 10118-1:2016, определяющий общие требования к функциям хэширования – первый стандарт ISO в области криптографии, полностью разработанный российскими специалистами

Международная организация по стандартизации (ISO)

- опубликован стандарт ISO/IEC 10118-1:2016, определяющий общие требования к функциям хэширования – первый стандарт ISO в области криптографии, полностью разработанный российскими специалистами
- новая редакция стандарта ISO/IEC 10118-3, включающая хэш-функции ГОСТ Р 34.11-2012 «Стрибог» и FIPS 202 «Keccak», получила поддержку 15 из 16 национальных органов по стандартизации, принявших участие в голосовании

Международная организация по стандартизации (ISO)

- опубликован стандарт ISO/IEC 10118-1:2016, определяющий общие требования к функциям хэширования – первый стандарт ISO в области криптографии, полностью разработанный российскими специалистами
- новая редакция стандарта ISO/IEC 10118-3, включающая хэш-функции ГОСТ Р 34.11-2012 «Стрибог» и FIPS 202 «Keccak», получила поддержку 15 из 16 национальных органов по стандартизации, принявших участие в голосовании
- создан технический комитет ТС 307 «Технологии цепной записи данных (блокчейн) и распределённых реестров»

Международная организация по стандартизации (ISO)

- опубликован стандарт ISO/IEC 10118-1:2016, определяющий общие требования к функциям хэширования – первый стандарт ISO в области криптографии, полностью разработанный российскими специалистами
- новая редакция стандарта ISO/IEC 10118-3, включающая хэш-функции ГОСТ Р 34.11-2012 «Стрибог» и FIPS 202 «Keccak», получила поддержку 15 из 16 национальных органов по стандартизации, принявших участие в голосовании
- создан технический комитет ТС 307 «Технологии цепной записи данных (блокчейн) и распределённых реестров»
  - в состав экспертов ТС 307 вошли 12 российских специалистов

Международная организация по стандартизации (ISO)

- опубликован стандарт ISO/IEC 10118-1:2016, определяющий общие требования к функциям хэширования – первый стандарт ISO в области криптографии, полностью разработанный российскими специалистами
- новая редакция стандарта ISO/IEC 10118-3, включающая хэш-функции ГОСТ Р 34.11-2012 «Стрибог» и FIPS 202 «Keccak», получила поддержку 15 из 16 национальных органов по стандартизации, принявших участие в голосовании
- создан технический комитет ТС 307 «Технологии цепной записи данных (блокчейн) и распределённых реестров»
  - в состав экспертов ТС 307 вошли 12 российских специалистов
  - на первом заседании ТС 307 (3-5 апреля) по инициативе российской делегации создана исследовательская группа по безопасности, которую возглавил российский специалист

Инженерный совет Интернета (IETF)

Инженерный совет Интернета (IETF)

- продвижение российских криптографических механизмов

Инженерный совет Интернета (IETF)

- продвижение российских криптографических механизмов
  - блочный шифр ГОСТ Р 34.11-2015 «Кузнечик» (RFC 7801)

Инженерный совет Интернета (IETF)

- продвижение российских криптографических механизмов
  - блочный шифр ГОСТ Р 34.11-2015 «Кузнечик» (RFC 7801)
  - Р 50.1.113–2016 Криптографические алгоритмы, сопутствующие применению алгоритмов электронной цифровой подписи и функции хэширования (RFC 7836)

Инженерный совет Интернета (IETF)

- продвижение российских криптографических механизмов
  - блочный шифр ГОСТ Р 34.11-2015 «Кузнечик» (RFC 7801)
  - Р 50.1.113–2016 Криптографические алгоритмы, сопутствующие применению алгоритмов электронной цифровой подписи и функции хэширования (RFC 7836)
  - Р 50.1.115–2016 Протокол выработки общего ключа с аутентификацией на основе пароля (RFC 8133)

Инженерный совет Интернета (IETF)

- продвижение российских криптографических механизмов
  - блочный шифр ГОСТ Р 34.11-2015 «Кузнечик» (RFC 7801)
  - Р 50.1.113–2016 Криптографические алгоритмы, сопутствующие применению алгоритмов электронной цифровой подписи и функции хэширования (RFC 7836)
  - Р 50.1.115–2016 Протокол выработки общего ключа с аутентификацией на основе пароля (RFC 8133)
- октябрь 2016 – создан экспертный совет IETF по криптографии, одним из 7 членов которого стал российский специалист

Инженерный совет Интернета (IETF)

- продвижение российских криптографических механизмов
  - блочный шифр ГОСТ Р 34.11-2015 «Кузнечик» (RFC 7801)
  - Р 50.1.113–2016 Криптографические алгоритмы, сопутствующие применению алгоритмов электронной цифровой подписи и функции хэширования (RFC 7836)
  - Р 50.1.115–2016 Протокол выработки общего ключа с аутентификацией на основе пароля (RFC 8133)
- октябрь 2016 – создан экспертный совет IETF по криптографии, одним из 7 членов которого стал российский специалист
- ноябрь 2016 – опубликован PROPOSED STANDARD RFC 8019 «Защита реализаций протокола IKEv2 от DDOS-атак», одним из двух авторов которого является российский специалист

Инженерный совет Интернета (IETF)

- продвижение российских криптографических механизмов
  - блочный шифр ГОСТ Р 34.11-2015 «Кузнечик» (RFC 7801)
  - Р 50.1.113–2016 Криптографические алгоритмы, сопутствующие применению алгоритмов электронной цифровой подписи и функции хэширования (RFC 7836)
  - Р 50.1.115–2016 Протокол выработки общего ключа с аутентификацией на основе пароля (RFC 8133)
- октябрь 2016 – создан экспертный совет IETF по криптографии, одним из 7 членов которого стал российский специалист
- ноябрь 2016 – опубликован PROPOSED STANDARD RFC 8019 «Защита реализаций протокола IKEv2 от DDOS-атак», одним из двух авторов которого является российский специалист
- ноябрь 2016 – российский специалист возглавил разработку RFC по механизмам смены ключей

Вместо заключения: что обсуждать и над чем работать?

Вместо заключения: что обсуждать и над чем работать?

- проекты криптографических механизмов, обеспечивающих одновременно шифрование и аутентификацию

Вместо заключения: что обсуждать и над чем работать?

- проекты криптографических механизмов, обеспечивающих одновременно шифрование и аутентификацию
- использование российских криптографических механизмов в протоколе TLS 1.3

Вместо заключения: что обсуждать и над чем работать?

- проекты криптографических механизмов, обеспечивающих одновременно шифрование и аутентификацию
- использование российских криптографических механизмов в протоколе TLS 1.3
- стандартизация постквантовых криптографических механизмов