

# НАЦИОНАЛЬНАЯ И МЕЖДУНАРОДНАЯ СТАНДАРТИЗАЦИЯ В ОБЛАСТИ КРИПТОГРАФИИ

И.Ф. Качалин, Д.В. Матюхин

ФСБ России

РусКрипто'2017

# О ЧЁМ ЭТОТ ДОКЛАД?

## О ЧЁМ ЭТОТ ДОКЛАД?

- РусКрипто'2016 – секция «Вопросы разработки и применения криптографических требований и стандартов»

## О ЧЁМ ЭТОТ ДОКЛАД?

- РусКрипто'2016 – секция «Вопросы разработки и применения криптографических требований и стандартов»
- Были озвучены результаты, текущие проекты, планы на будущее

## О ЧЁМ ЭТОТ ДОКЛАД?

- РусКрипто'2016 – секция «Вопросы разработки и применения криптографических требований и стандартов»
- Были озвучены результаты, текущие проекты, планы на будущее
- В какой мере они реализовались за прошедший год?

## О ЧЁМ ЭТОТ ДОКЛАД?

- РусКрипто'2016 – секция «Вопросы разработки и применения криптографических требований и стандартов»
- Были озвучены результаты, текущие проекты, планы на будущее
- В какой мере они реализовались за прошедший год?
- Что ещё предстоит сделать?

## О ЧЁМ ЭТОТ ДОКЛАД?

- РусКрипто'2016 – секция «Вопросы разработки и применения криптографических требований и стандартов»
- Были озвучены результаты, текущие проекты, планы на будущее
- В какой мере они реализовались за прошедший год?
- Что ещё предстоит сделать?
- Какие новые направления появились в данной области?





2015 – завершено обновление *базовых стандартов*

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

- 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), о котором подробно рассказано на РусКрипто'2016

## 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), о котором подробно рассказано на РусКрипто'2016
- 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), о котором подробно рассказано на РусКрипто'2016
- перед утверждением Росстандартом, как правило, апробируются в качестве *методических рекомендаций ТК 26*
- доступны для ознакомления на <http://tc26.ru/standard/rs/>





Рекомендации по стандартизации, рекомендованные ТК 26 к утверждению Росстандартом

- Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации (отдельный доклад в программе Рускрипто'2017)

Рекомендации по стандартизации на основе утверждённых в 2016 году методических рекомендаций ТК 26

Рекомендации по стандартизации на основе утверждённых в 2016 году методических рекомендаций ТК 26

- 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

Рекомендации по стандартизации на основе утверждённых в 2016 году методических рекомендаций ТК 26

- 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

тексты которых доступны на <http://tc26.ru/methods/recommendation/>

Рекомендации по стандартизации, разработанные ПК 3 ТК 26  
«Криптографические алгоритмы и механизмы в национальной  
платёжной системе Российской Федерации»

Рекомендации по стандартизации, разработанные ПК 3 ТК 26 «Криптографические алгоритмы и механизмы в национальной платёжной системе Российской Федерации»

- Использование функции диверсификации для формирования производных ключей платежного приложения
- Использование режимов алгоритма блочного шифрования в протоколе защищенного обмена сообщениями в процессе эмиссии платежных карт
- Использование алгоритмов согласования ключа и блочного шифрования при офлайн-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
- два доклада в программе Рускрипто'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
- два доклада в программе Рускрипто'2017
- дискуссия «Блокчейн: ожидания рынка и мнения экспертов» в программе СТСCrypt 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
- два доклада в программе Рускрипто'2017
- дискуссия «Блокчейн: ожидания рынка и мнения экспертов» в программе СТСCrypt 2017

### КРИПТОГРАФИЯ В ЦИФРОВЫХ КОНТРОЛЬНЫХ УСТРОЙСТВАХ

### 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
- два доклада в программе Рускрипто'2017
- дискуссия «Блокчейн: ожидания рынка и мнения экспертов» в программе СТСCrypt 2017

### КРИПТОГРАФИЯ В ЦИФРОВЫХ КОНТРОЛЬНЫХ УСТРОЙСТВАХ

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

### 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
- два доклада в программе Рускрипто'2017
- дискуссия «Блокчейн: ожидания рынка и мнения экспертов» в программе СТCrypt 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 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 «Кессак», 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 «Кессак», получила поддержку 15 из 16 национальных органов по стандартизации, принявших участие в голосовании
- создан технический комитет TC 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 «Кессак», получила поддержку 15 из 16 национальных органов по стандартизации, принявших участие в голосовании
- создан технический комитет TC 307 «Технологии цепной записи данных (блокчейн) и распределённых реестров»
  - в состав экспертов TC 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 «Кессак», получила поддержку 15 из 16 национальных органов по стандартизации, принявших участие в голосовании
- создан технический комитет TC 307 «Технологии цепной записи данных (блокчейн) и распределённых реестров»
  - в состав экспертов TC 307 вошли 12 российских специалистов
  - первое заседание TC 307 – 3-5 апреля

### 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 «Кессак», получила поддержку 15 из 16 национальных органов по стандартизации, принявших участие в голосовании
- создан технический комитет TC 307 «Технологии цепной записи данных (блокчейн) и распределённых реестров»
  - в состав экспертов TC 307 вошли 12 российских специалистов
  - первое заседание TC 307 – 3-5 апреля
  - Россия предложила создать в TC 307 исследовательскую группу по безопасности и взять на себя организацию её работы

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 ожидает публикации)

### 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 ожидает публикации)
- 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 ожидает публикации)
- 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 ожидает публикации)
- 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