Алгоритмы ГОСТ в массовой криптографии: настоящее и будущее

Смышляев Станислав Витальевич, к.ф.-м.н.,
директор по информационной безопасности

РусКрипто'2019

Актуальные задачи в области массовой криптографии (1)

- Пр-1380 и «Цифровая экономика»:
  - Поручение Президента от 16 июля 2016 года № Пр-1380 «Об обеспечении разработки и реализации комплекса мероприятий, необходимых для перехода органов власти на использование российских криптографических алгоритмов и средств шифрования»
  - Создание Национального удостоверяющего центра (НУЦ)
  - Разработка дорожной карты «Российская криптография в российском сегменте Интернет»

Актуальные задачи в области массовой криптографии (2)

- Единая биометрическая система (ЕБС): 482-ФЗ от 31.12.2017 и 4-МР ЦБ от 14.02.2019:
  - Криптографическая защита канала между пользователем и банком при удаленной аутентификации через ЕБС.
  - Браузер и мобильное приложение.
  - Использование сертифицированных по КС1 средств.
- В ближайшие годы:
  - «Цифровой профиль».
  - Объединение технологий облачной подписи с удаленным получением сертификатов через ЕБС.

Актуальные задачи в области массовой криптографии (3)

- Пр-1380 и «Цифровая экономика»
- Единая биометрическая система (ЕБС)
- «Цифровой профиль»
- Облачная ЭП с удаленным получением сертификатов через ЕБС.

— всюду массовое СКЗИ требуется для одного и того же: установления защищенного соединения по TLS с ГОСТ.

СКЗИ у массового пользователя

- Браузеры, поддерживающие клиентскую часть TLS.
- Мобильные приложения на телефоне, обеспечивающие защищенный по TLS канал с сервером.
- Почтовые клиенты, обеспечивающие защиту сообщений (S/MIME — CMS).
- Приложения для защищенного использования «облачных» сервисов.

— TLS (клиентская часть, односторонняя аутентификация), CMS, безопасная аутентификация.

1. Стандартизированные в России механизмы
2. Связь с международной стандартизацией
3. Требуемые компоненты
4. Существующие решения
5. Опыт внедрения
6. Актуальные задачи

Где стандартизируются российские криптографические механизмы

- Технический комитет по стандартизации “Криптографическая защита информации” (ТК 26): стандартизация алгоритмов; рабочие группы по сопутствующим криптографическим алгоритмам и протоколам и TLS, по IPsec, по PKCS#11.
- Эксперты ТК 26 в ISO/JTC1/SC27, в том числе в WG2 “Cryptography and security mechanisms”.
- Эксперты ТК 26 в IETF: CFRG, TLS, CMS, сопутствующие механизмы.

Протоколы «массовой» криптографии и стандартизация в России

Существующие документы ТК 26

- Механизмы и протоколы с использованием ГОСТ 28147-89
  - МР 26.2.001-2013 «Использование наборов алгоритмов шифрования на основе ГОСТ 28147-89 для протокола безопасности транспортного уровня (TLS)»
  - МР 26.2.002-2013 «Использование алгоритмов ГОСТ 28147-89, ГОСТ Р 34.10 и ГОСТ Р 34.11 в криптографических сообщениях формата CMS»

Протоколы «массовой» криптографии и стандартизация в России

Существующие документы ТК 26

- Механизмы и протоколы с использованием действующих ГОСТ Р 34.1x
  - Р 50.1.113–2016 «Криптографические алгоритмы, сопутствующие применению алгоритмов электронной цифровой подписи и функции хэширования»
  - Р 1323565.1.017-2018 «Криптографические алгоритмы, сопутствующие применению алгоритмов блочного шифрования»
  - Р 1323565.1.020-2018 «Использование криптографических алгоритмов в протоколе безопасности транспортного уровня (TLS 1.2)»

Протоколы «массовой» криптографии и стандартизация в России

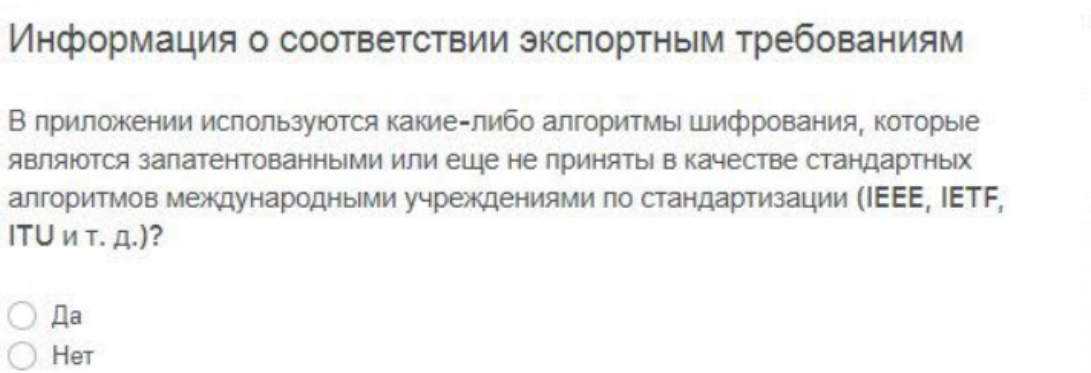
Разрабатываемые документы ТК 26

- Механизмы и протоколы с использованием действующих ГОСТ Р 34.1x
  - «Форматы сообщений, защищенных криптографическими методами» (план: апрель 2019)
  - «Режимы работы блочных шифров, реализующие аутентифицированное шифрование» (план: апрель 2019)
  - «Использование криптографических алгоритмов в протоколе безопасности транспортного уровня (TLS 1.3)» (план: сентябрь 2019)

Связь с международной стандартизацией (1)

- Встраивание российской криптографии в ОС Windows: трудности с подменой жестко зафиксированных алгоритмов (например, SHA-1).
- Существенные трудности с корректировкой архитектуры ключевой системы протокольных решений.
- Крайне желательно иметь согласованные с международными организациями идентификаторы („codepoints“), в т.ч. идентификаторы криптонаборов TLS.

Публикация (экспортных) СКЗИ в магазинах приложений



Связь с международной стандартизацией (2)

Необходимые условия для возможности использования ГОСТ в международных протоколах

Непрерывное участие в работах по международной стандартизации для эффективного внедрения в массовом ПО российских криптоалгоритмов на территории РФ с целью обеспечить:

- Собственно международные документы, специфицирующие алгоритмы и параметры.
- Вариабельность алгоритмов и параметров — “crypto agility”.
- Общая архитектура протоколов не должна противоречить российским требованиям по безопасности.

Российские эксперты в ISO и IETF

- ISO/IEC:
  - Официальный представитель SC27/JTC1 в TC 307.
  - Соруководитель совместной рабочей группы SC27/JTC1 и TC 307.
- IETF:
  - Эксперт Crypto Review Panel.
  - Эксперт IANA по AEAD-режимам.
  - Соруководитель РГ uta.
  - Рецензент secdir.

Российские эксперты в ISO и IETF

- ISO/IEC:
  - Официальный представитель SC27/JTC1 в TC 307.
  - Соруководитель совместной рабочей группы SC27/JTC1 и TC 307.
- IETF:
  - Эксперт Crypto Review Panel.
  - Эксперт IANA по AEAD-режимам.
  - Соруководитель РГ uta.
  - Рецензент secdir.

Российские механизмы в ISO и IETF

- ISO/IEC:
  - ГОСТ Р 34.10-2012 в ISO/IEC 14888-3.
  - ГОСТ Р 34.11-2012 в ISO/IEC 10118-3:2018.
  - Перспективы ГОСТ Р 34.12-2015 в ISO/IEC 18033-3.
  - Перспективы Р 1323565.1.017-2018 в ISO/IEC 10116 и ISO/IEC 19772.
- IETF:
  - ГОСТ Р 34.10-2012 в RFC 7091.
  - ГОСТ Р 34.11-2012 в RFC 6986.
  - ГОСТ Р 34.12-2015 в RFC 7801.
  - Р 50.1.113-2016, Р 50.1.114-2016 в RFC 7836.
  - Р 50.1.115-2016 в RFC 8133.
  - Перспективы Р 1323565.1.017-2018 в draft-irtf-cfrg-re-keying.

Российские механизмы в ISO и IETF

- ISO/IEC:
  - ГОСТ Р 34.10-2012 в ISO/IEC 14888-3.
  - ГОСТ Р 34.11-2012 в ISO/IEC 10118-3:2018.
  - Перспективы ГОСТ Р 34.12-2015 в ISO/IEC 18033-3.
  - Перспективы Р 1323565.1.017-2018 в ISO/IEC 10116 и ISO/IEC 19772.
- IETF:
  - ГОСТ Р 34.10-2012 в RFC 7091.
  - ГОСТ Р 34.11-2012 в RFC 6986.
  - ГОСТ Р 34.12-2015 в RFC 7801.
  - Р 50.1.113-2016, Р 50.1.114-2016 в RFC 7836.
  - Р 50.1.115-2016 в RFC 8133.
  - Перспективы Р 1323565.1.017-2018 в draft-irtf-cfrg-re-keying.

Идентификаторы IANA для TLS с ГОСТ

Март 2018: РусКрипто'2018

«Крайне желательно иметь согласованные с международными организациями идентификаторы („codepoints“), в т.ч. идентификаторы криптонаборов TLS.»

- Устранение опасности блокировки TLS с ГОСТ из-за захвата номеров другими криптонаборами (напр., KHP).
- Легитимизация поддержки российских криптонаборов в свободном ПО, в т.ч. OpenSSL.
- Снижение опасности конфликтов с эволюционными изменениями TLS в IETF.
- Поддержка сторонним по отношению к реализациям TLS ПО, в т.ч. Wireshark.

Работы велись 16 лет, с 2003 года

Идентификаторы IANA для TLS с ГОСТ

Март 2018: РусКрипто'2018

«Крайне желательно иметь согласованные с международными организациями идентификаторы („codepoints“), в т.ч. идентификаторы криптонаборов TLS.»

Идентификаторы IANA для TLS с ГОСТ

Март 2018: РусКрипто'2018

«Крайне желательно иметь согласованные с международными организациями идентификаторы („codepoints“), в т.ч. идентификаторы криптонаборов TLS.»

Февраль 2019: внесение криптонаборов ГОСТ в реестр IANA

7 февраля 2019 года IANA одобрила внесение российских криптонаборов протокола TLS в реестр IANA.

0xC1,0x00	TLS_GOSTR341112_256_WITH_KUZNYECHIK_CTR_OMAC	[draft-smyshlyaev-tls12-gost-suites]
0xC1,0x01	TLS_GOSTR341112_256_WITH_MAGMA_CTR_OMAC	[draft-smyshlyaev-tls12-gost-suites]
0xC1,0x02	TLS_GOSTR341112_256_WITH_28147_CNT_IMIT	[draft-smyshlyaev-tls12-gost-suites]

Требуемые компоненты

- Браузеры с поддержкой TLS с ГОСТ.
- TLS-сервера требуемого класса защиты с одновременной поддержкой ГОСТ и зарубежных криптонаборов (по итогам обсуждения на РусКрипто'2018).
- Почтовые клиенты со встроенной поддержкой S/MIME с CMS по ГОСТ.
- SDK для создания мобильных приложений с поддержкой TLS с ГОСТ.
- Средства УЦ для выдачи TLS-сертификатов (ГОСТ).
- Вспомогательные средства PKI для TLS-сертификатов (ГОСТ).
- Клиентские и серверные решения для "облачной" подписи.

Существующие компоненты (1)

- Браузеры с поддержкой TLS с ГОСТ.
  - Браузер “Спутник”: КС1, КС2.
  - Браузеры в составе ОС Astra Linux и ОС ALT Linux: Chromium GOST, Firefox GOST
  - Яндекс.Браузер
  - Модули для Internet Explorer, Edge: КС1, КС2, КС3.
- TLS-сервера требуемого класса защиты с одновременной поддержкой ГОСТ и зарубежных криптонаборов.
  - Вплоть до класса КС3: TLS_GOSTR341112_256_WITH_28147_CNT_IMIT и основные современные зарубежные криптонаборы.
- Почтовые клиенты со встроенной поддержкой S/MIME с CMS по ГОСТ.
  - Модули для MS Outlook: КС1, КС2, КС3.

Существующие компоненты (2)

- SDK для создания мобильных приложений с поддержкой TLS с ГОСТ.
  - Для ОС iOS, Android: КС1.
- Средства УЦ для выдачи TLS-сертификатов (ГОСТ).
  - Без изменений подходят средства УЦ для СКПЭП: КС1, КС2, КС3.
- Вспомогательные средства PKI для TLS-сертификатов (ГОСТ).
  - OCSP-сервера есть; средств Certificate Transparency и ACME нет.
- Клиентские и серверные решения для “облачной” подписи
  - HSM КВ2, серверные решения КС3, клиентские решения КС1, КС2, КС3.

CRYPTOPRO

1 Стандартизированные в России механизмы

2 Связь с международной стандартизацией

3 Требуемые компоненты

4 Существующие решения

5 Опыт внедрения

6 Актуальные задачи

Демонстрационные стенды

Осень 2018: тестовые TLS-сервера с поддержкой ГОСТ (только)

- https://crypto.cs.msu.ru
- https://gost.norsi-trans.ru
- https://gost.cryptopro.ru
- https://gost.kryptonite.ru

— доступ обеспечивается только в случае поддержки ГОСТ на стороне браузера клиента.

Действующие сайты с поддержкой ГОСТ

Поддержка ГОСТ

- https://lkul.nalog.ru
- https://eruz.zakupki.gov.ru/auth/

Поддержка ГОСТ и RSA

- https://cryptopro.ru
- https://smile.rambler.ru
- https://www.nic.ru
- https://agregatoreat.ru

— в случае поддержки ГОСТ на стороне браузера клиента работают по ГОСТу, иначе работают “стандартным” образом по зарубежному TLS.

1. Стандартизированные в России механизмы
2. Связь с международной стандартизацией
3. Требуемые компоненты
4. Существующие решения
5. Опыт внедрения
6. Актуальные задачи

Актуальные задачи: стандартизация

Разработка криптонаборов TLS 1.3

- В 2018 году TLS 1.3 утвержден в IETF: RFC 8446. Главный протокол защиты соединений в Интернете на ближайшее десятилетие.
  - Разработка проекта Р «Использование криптографических алгоритмов в протоколе безопасности транспортного уровня (TLS 1.3)» и анализ стойкости завершены в ТК 26, до августа будет проходить экспертиза. Плановый срок утверждения — осень 2019.
- Для TLS 1.3 необходимо использование AEAD.
  - Разработан режим MGM (Обоснование стойкости: Cryptology ePrint Archive: Report 2019/123).
  - Окончательная редакция Р «Режимы работы блочных шифров, реализующие аутентифицированное шифрование» направлена в Росстандарт.

Актуальные задачи: ISO и IETF

IETF

- IETF: разработка документа “Multilinear Galois Mode (MGM)”, draft-smyshlyaev-mgm.
- IETF: разработка документа “GOST Cipher Suites for TLS 1.2”, draft-smyshlyaev-tls12-gost-suites.
- IETF: разработка нового документа по криптонаборам для TLS 1.3.
- IANA: получение идентификаторов для криптонаборов TLS 1.3 с ГОСТ.

ISO

- ISO: стандартизация CTR-ACPKM.
- ISO: стандартизация GCM-ACPKM.
- ISO: стандартизация MGM.

Актуальные задачи: программные решения

Клиентские компоненты

- Браузеры с упрощенной установкой криптографических компонент (без регистрации).
- Законченные мобильные приложения на основе существующих SDK с TLS с ГОСТ для решения прикладных задач.

Сопутствующие компоненты PKI

- Сервера ACME — для автоматизированной выдачи ГОСТовых TLS-сертификатов.
- Сервера Certificate Transparency — для обеспечения прозрачности множества сертификатов, выданных каждому из сайтов.

Актуальные задачи: инфраструктура

- До появления нормативной базы НУЦ: начало внедрения серверов с TLS с ГОСТ с получением сертификатов от УЦ, корневые сертификаты которых уже распространяются с СКЗИ.
- Создание НУЦ и подчиненных УЦ, в том числе коммерческих для сайтов, не относящихся к Пр-1380.
- Для НУЦ: учет существующего опыта распространения корневых сертификатов вместе с клиентскими СКЗИ (распространять корневые сертификаты отдельно от клиентских СКЗИ бессмысленно).
- Создание подчиненных УЦ с поддержкой ACME.
- Создание реестра сертификатов (Certificate Transparency).

CRYPTOPRO

Спасибо за внимание!

Вопросы?

- Материалы, вопросы, комментарии:
  - svs@cryptopro.ru