Российские криптоалгоритмы в международных протокольных решениях: история, задачи, перспективы

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

РусКрипто'2018

Стандартизация российских криптографических механизмов

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

Не только престиж — прямая практическая необходимость.

Стандартизация российских криптографических механизмов

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

Не только престиж — прямая практическая необходимость.

Разработка собственного изолированного стека протоколов (включая форматы, инфраструктуру, прикладное ПО) для массового прикладного ПО на практике трудна
$\Rightarrow$ требуется работа в рамках существующих протокольных решений: TLS, IPsec, CMS и пр.

Альтернатива: КНР

- Широкая деятельность по собственному набору протокольных решений и реализаций ПО как системного, так и прикладного.
- Пример: Сиань, лаборатория NELWS — разработка своих решений для широчайшего множества беспроводных протоколов, свои программные и аппаратные реализации.
- Но: параллельно ведут работу по содействию встраивания своих алгоритмов в основные международные протокольные решения.

Разработка собственного изолированного стека протоколов (включая форматы, инфраструктуру, прикладное ПО) для массового прикладного ПО на практике трудна
$\Rightarrow$ требуется работа в рамках существующих протокольных решений: TLS, IPsec, CMS и пр.

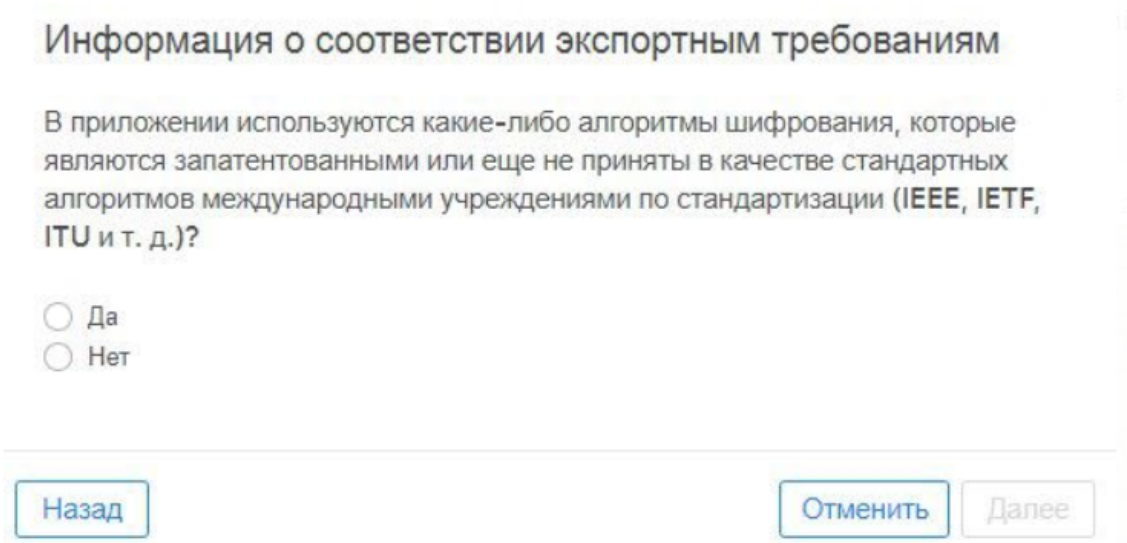
Альтернатива: КНР

- Широкая деятельность по собственному набору протокольных решений и реализаций ПО как системного, так и прикладного.
- Пример: Сиань, лаборатория NELWS — разработка своих решений для широчайшего множества беспроводных протоколов, свои программные и аппаратные реализации.
- Но: параллельно ведут работу по содействию встраивания своих алгоритмов в основные международные протокольные решения.

- 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.

- 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



Включение в документы IETF

- Не влечет формальных обязательств по поддержке в ПО.
- Зачастую требуется для фактической совместимости и поддержки.
- Открытые стандарты — влечет возможность поддержки в открытых сообществах.
- Необходимо для получения идентификаторов IANA.

Включение в стандарты ISO

- Не влечет формальных обязательств по поддержке в ПО.
- Стандарты малодоступны для открытых сообществ.
- Повышает статус алгоритмов до международных.
- Может убирать формальные препятствия (в т.ч. в IETF).

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.

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.

Проблемы использования международных протоколов в российских СКЗИ

Недопустимость изменений фундаментальной структуры протокола

Порядок сообщений, форматы данных, правила обработки ошибок.

- Блокирование возможности согласования в IETF при коренных изменениях протокола.
- Существенные трудности изменений любых элементов протокола при совмещении с существующими реализациями (пример: TLS в ОС Windows).
- Важность не потерять преимущества от работы в рамках существующего стека реализаций протокола.

Проблемы использования международных протоколов в российских СКЗИ

Разница в подходах к синтезу и анализу протоколов

- Различия в существующей базе фактически доступных для использования типов криптографических механизмов.
- Другая степень ориентированности на быстродействие, а также (после 2013 года) на защиту анонимности и невозможности депонирования ключей.
- Российские требования к криптостандартам и к СКЗИ в существенной части аспектов строже общепринятых.

Пример: нагрузка на ключ

- Жесткие ограничения по нагрузке на ключ не свойственны для международных протокольных решений.
- Ситуация начала меняться только с 2016 года, после атак Sweet32 на криптонаборы TLS с шифрами с блоком 64 бита.
- Но большинство дискуссий — про запрет шифров с малой длиной блока, а не про ограничение нагрузки на ключ (все еще актуальное для блока 128 бит, если учитывать атаки по побочным каналам).
- В протокольных решениях до TLS 1.3 данный вопрос вовсе не рассматривался.
- В РФ в ESP, TLS, CMS с ГОСТ 28147-89 данную проблему приходилось решать, не меняя структуру протокола.

Пример: нагрузка на ключ

- Жесткие ограничения по нагрузке на ключ не свойственны для международных протокольных решений.
- Ситуация начала меняться только с 2016 года, после атак Sweet32 на криптонаборы TLS с шифрами с блоком 64 бита.
- Но большинство дискуссий — про запрет шифров с малой длиной блока, а не про ограничение нагрузки на ключ (все еще актуальное для блока 128 бит, если учитывать атаки по побочным каналам).
- В протокольных решениях до TLS 1.3 данный вопрос вовсе не рассматривался.
- В РФ в ESP, TLS, CMS с ГОСТ 28147-89 данную проблему приходилось решать, не меняя структуру протокола.

Пример: нагрузка на ключ

Ограничение нагрузки на ключ в ESP

- Два режима: 4M и 1K (по предельному объему зашифровываемых на одном ключе данных).
- 1K: ключ на пакет, прозрачная смена ключа (internal re-keying, key meshing по RFC 4357) внутри пакета.
- 4M: ключ на несколько пакетов, внешняя смена ключа (external re-keying с использованием диверсификации по RFC 4357):

$$
\begin{aligned}
&\qquad\qquad\qquad\qquad\qquad\quad \text{RootKey} \\
&\qquad\qquad\qquad\quad \text{Divers(} \quad \text{RootKey} \quad \text{,i\&Mask1)} \\
&\qquad\qquad\quad \text{Divers(} \quad \text{Divers(} \quad \text{RootKey} \quad \text{,i\&Mask1)} \quad \text{,i\&Mask2)} \\
\text{Key[i]} = \text{Divers(} \quad &\text{Divers(} \quad \text{Divers(} \quad \text{RootKey} \quad \text{,i\&Mask1)} \quad \text{,i\&Mask2)} \quad \text{,i\&Mask3)}
\end{aligned}
$$

Пример: нагрузка на ключ

Ограничение нагрузки на ключ в TLS 1.2

- Два криптонабора: TLS_GOSTR341112_256_WITH_MAGMA_CTR_OMAC и ..._WITH_KUZNYECHIK_CTR_OMAC.
- Магма: смена ключа по CTR-ACPKM один раз в 1КБ, лист ключевого дерева на 4096 сообщений.
- Кузнечик: смена ключа по CTR-ACPKM один раз в 4КБ, лист ключевого дерева на 64 сообщения.
- В криптонаборе с Кузнечиком нагрузка на ключ строго ограничена в целях возможности использования данного криптонабора при обеспечении безопасности соединений в СКЗИ высоких классов.

Пример: нагрузка на ключ

Ограничение нагрузки на ключ в TLS 1.2

- Два криптонабора: TLS_GOSTR341112_256_WITH_MAGMA_CTR_OMAC и ..._WITH_KUZNYECHIK_CTR_OMAC.
- Магма: смена ключа по CTR-ACPKM один раз в 1КБ, лист ключевого дерева на 4096 сообщений.
- Кузнечик: смена ключа по CTR-ACPKM один раз в 4КБ, лист ключевого дерева на 64 сообщения.
- В криптонаборе с Кузнечиком нагрузка на ключ строго ограничена в целях возможности использования данного криптонабора при обеспечении безопасности соединений в СКЗИ высоких классов.

Специфика разработки механизмов в ТК 26

Технический комитет по стандартизации “Криптографическая защита информации” (ТК 26):

- Требование проведения самодостаточного анализа безопасности “с нуля”, экспертиза документов только вместе с анализом безопасности.
- Как в парадигме доказуемой стойкости, так и по отношению к известным методам.
- Строгие требования по теоретической стойкости — отсутствие толерантности к теоретическим уязвимостям, для которых пока не найдено практических путей применения.

Пример: криптонаборы для TLS с ГОСТ

- 2003: первые версии draft-chudov-cryptopro-cptls — с CFB.
- 2004: работы Барда и Воденея о теоретических уязвимостях TLS 1.0.
- 2009: draft-chudov-cryptopro-cptls-04, а позже разрабатываемые и внедряемые в РФ на его основе Методические рекомендации ТК 26 — на основе режима гаммирования.
- 2011: BEAST, POODLE, Lucky13 — практические уязвимости, необходимость срочно усекать перечень поддерживаемых криптонаборов.
- 2011-2018: TLS по МР ТК 26 — необходимости в изменениях нет, обнаруженные уязвимости не применимы.
- 2018: Планируется принятие Рекомендаций по Стандартизации по TLS 1.2 с ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015.

Что сделано по каждому из направлений

Необходимые условия для возможности использования ГОСТ в международных протоколах

Направления работы:

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

Современные российские алгоритмы в международных стандартах

- Действующие ГОСТ Р в документах IETF: RFC 6986, RFC 7091, RFC 7801
- Действующие Рекомендации ТК 26: RFC 7836, RFC 8133.
- ГОСТ Р 34.10-2012 в ISO/IEC 14888-3.
- ГОСТ Р 34.11-2012 и ГОСТ Р 34.12-2015 в проектах документов ISO.

Примеры: crypto agility

- Криптографическая экспертиза документов IETF в качестве члена Crypto Review Panel IETF (примеры: документ CFRG “Hash-Based Signatures”, использование любой стойкой хэш-функции, не только SHA-2; документы КНР, позиция по вопросам национальной криптографии).
- IETF: долгие дискуссии о поддержке нац. криптографии в TLS 1.3, в том числе после отклонения draft-chudov-cryptopro-cptls. В политику IANA внесены изменения, криптонаборы могут быть не только “рекомендованными”, но и “определенными” — для целей российских алгоритмов этого достаточно.
- Wi-Fi Device Provisioning Protocol — в первых версиях явно зафиксированы SHA-256, AES и параметры эл. кривых NIST; на конкурсной основе удалось получить проведение работ по экспертизе, замечания были учтены.

Примеры: crypto agility

- Криптографическая экспертиза документов IETF в качестве члена Crypto Review Panel IETF (примеры: документ CFRG “Hash-Based Signatures”, использование любой стойкой хэш-функции, не только SHA-2; документы КНР, позиция по вопросам национальной криптографии).
- IETF: долгие дискуссии о поддержке нац. криптографии в TLS 1.3, в том числе после отклонения draft-chudov-cryptopro-cptls. В политику IANA внесены изменения, криптонаборы могут быть не только “рекомендованными”, но и “определенными” — для целей российских алгоритмов этого достаточно.
- Wi-Fi Device Provisioning Protocol — в первых версиях явно зафиксированы SHA-256, AES и параметры эл. кривых NIST; на конкурсной основе удалось получить проведение работ по экспертизе, замечания были учтены.

Примеры: crypto agility

- Криптографическая экспертиза документов IETF в качестве члена Crypto Review Panel IETF (примеры: документ CFRG “Hash-Based Signatures”, использование любой стойкой хэш-функции, не только SHA-2; документы КНР, позиция по вопросам национальной криптографии).
- IETF: долгие дискуссии о поддержке нац. криптографии в TLS 1.3, в том числе после отклонения draft-chudov-cryptopro-cptls. В политику IANA внесены изменения, криптонаборы могут быть не только “рекомендованными”, но и “определенными” — для целей российских алгоритмов этого достаточно.
- Wi-Fi Device Provisioning Protocol — в первых версиях явно зафиксированы SHA-256, AES и параметры эл. кривых NIST; на конкурсной основе удалось получить проведение работ по экспертизе, замечания были учтены.

Примеры: влияние на структуру

Полезно, когда выработанные в РФ принципиальные подходы к использованию криптоалгоритмов заблаговременно обсуждаются в широком сообществе.

- Строгие требования к ограничению нагрузки на ключ (примеры: ISO SC 27, NIST, ограничение материала на 3DES до 8 МБ только в 2017) — процедуры смены ключей.
- Резервный источник случайности на случай сбоев основного пула; подходы к постквантовой криптографии.
- Оптимизация работы IPsec (В.А. Смыслов).
- Подходы к работе с PKI (Д.М. Белявский).
- Соответствие протоколов и их модельных версий в обоснованиях — пример с TLS, влияние на разрабатываемые в CFRG PAKE (Е.К. Алексеев).
- Проведение работ по экспертизе.

Основные массовые протоколы и ГОСТ

Документы ТК 26

- TLS, IPsec, CMS с ГОСТ 28147-89, ГОСТ Р 34.1x-2012 — действуют.
- TLS, CMS с ГОСТ Р 34.1x-2015 — работы в ТК 26 на заключительном этапе.
- IPsec с ГОСТ Р 34.1x-2015 — работы в процессе.
- IPsec, CMS, TLS 1.2, TLS 1.3 — охватываются текущими работами системы стандартизации.
- SRTP, OAuth, Kerberos — существуют происследованные проприетарные решения.
- DTLS, XMLDsig, XMLEnc — в ТК 26 начато проведение работ, важно довести до конца.
- SSH, QUIC — требуется проведение работ.

Основные массовые протоколы и ГОСТ

Документы ТК 26

- TLS, IPsec, CMS с ГОСТ 28147-89, ГОСТ Р 34.1x-2012 — действуют.
- TLS, CMS с ГОСТ Р 34.1x-2015 — работы в ТК 26 на заключительном этапе.
- IPsec с ГОСТ Р 34.1x-2015 — работы в процессе.

- IPsec, CMS, TLS 1.2, TLS 1.3 — охватываются текущими работами системы стандартизации.
- SRTP, OAuth, Kerberos — существуют происследованные проприетарные решения.
- DTLS, XMLDsig, XMLEnc — в ТК 26 начато проведение работ, важно довести до конца.
- SSH, QUIC — требуется проведение работ.

Разработка криптонаборов TLS 1.3

- Работа вне РГ и ТК 26: цикл научных семинаров в МГУ.
- Протокол не обязательно должен быть разработан в России, чтобы удовлетворять всем требованиям — анализ Handshake TLS 1.3 в свете принципиальных качеств протокола “Эхинацея”.
- Для TLS 1.3 крайне важно использовать AEAD-режим блочного шифра.
- Разработка AEAD-режима в ТК 26 в кратчайшие сроки — включен в ПНС на 2018 год.
- Основной вариант в проработке — режим MGM (представлен в 2017 году на CTCrypt В.И. Ноздруновым).
- Продвижение MGM в IETF, несмотря на трудности из-за CAESAR (запланирован доклад на IETF 102 в Монреале).

Разработка криптонаборов TLS 1.3

- Работа вне РГ и ТК 26: цикл научных семинаров в МГУ.
- Протокол не обязательно должен быть разработан в России, чтобы удовлетворять всем требованиям — анализ Handshake TLS 1.3 в свете принципиальных качеств протокола “Эхинацея”.
- Для TLS 1.3 крайне важно использовать AEAD-режим блочного шифра.
- Разработка AEAD-режима в ТК 26 в кратчайшие сроки — включен в ПНС на 2018 год.
- Основной вариант в проработке — режим MGM (представлен в 2017 году на CTCrypt В.И. Ноздруновым).
- Продвижение MGM в IETF, несмотря на трудности из-за CAESAR (запланирован доклад на IETF 102 в Монреале).

Использование российских алгоритмов в самостоятельных протокольных решениях

- РГ по ЦКУ — использование механизмов из Р 50.1.113-2016/RFC 7836; планы использования механизмов безопасности TLS с ГОСТ;
- РГ по НСПК — благодаря переиспользованию элементов анализа механизмов ТК 26, разработанных для CMS, TLS и IPsec (в т.ч. VKO из RFC 4357), в кратчайшие сроки удалось покрыть существенную часть потребности в механизмах для платежных систем

— при том, что изначально при синтезе и анализе механизмов данные приложения не рассматривались как области применения.

CRYPTOPRO

Спасибо за внимание!

Вопросы?

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