Работы по стандартизации сопутствующих криптографических алгоритмов и криптографических протоколов

Смышляев С.В.
Алексеев Е.К., Ошкин И.Б., Попов В.О.

- Курс на импортозамещение.
- Требования к СКЗИ, СЭП, УЦ.
- Российские криптографические стандарты.

- Необходимость совместимой работы в рамках, задаваемых международными стандартами и де-факто стандартами.
- Встраивание в Windows, массовое прикладное ПО.
- Наработки международного научного сообщества в области криптографии.
- Согласование с существующими стандартами и RFC и создание новых.

VII Уральский форум „Информационная безопасность банков“, доклад В.М. Простова „Создание национальной системы платежных карт с использованием отечественных HSM.“:

- Первый этап: функционал импортных аналогов с использованием отечественных криптоалгоритмов только в автономных режимах.
- Второй этап: реализация инфраструктуры с использованием импортных и отечественных криптоалгоритмов.
- Третий этап: Разработка и внедрение спецификаций и приложений с поддержкой отечественных криптоалгоритмов.

Спецификации и рекомендации по стандартизации по использованию российских алгоритмов в:

- IKE, ESP, AH;
- TLS;
- X.509;
- CMS;
- CAdES, PAdES, XAdES;
- EKE, SM;
- PKCS#11, PKCS#12, PKCS#15.

Спецификации и рекомендации по стандартизации по использованию российских алгоритмов в:

- IKE, ESP, AH;
- TLS;
- X.509;
- CMS;
- CAdES, PAdES, XAdES;
- EKE, SM;
- PKCS#11, PKCS#12, PKCS#15.

Технический комитет 26 „Криптографическая защита информации“. Рекомендации по стандартизации.

- Задание узлов замены блока подстановки алгоритма шифрования ГОСТ 28147-89.
- Использование криптографических алгоритмов, сопутствующих применению стандартов ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012.
- Использование алгоритмов ГОСТ 28147-89, ГОСТ Р 34.11 и ГОСТ Р 34.10 в криптографических сообщениях формата CMS.
- Использование наборов алгоритмов на основе ГОСТ 28147-89 для протокола безопасности транспортного уровня (TLS).
- Задание параметров эллиптических кривых в соответствии с ГОСТ Р 34.10-2012.
- Задание параметров скрученных эллиптических кривых Эдвардса в соответствии с ГОСТ Р 34.10-2012.

Технический комитет 26 „Криптографическая защита информации“. Технические спецификации.

- Использование ГОСТ 28147-89, ГОСТ Р 34.11-94 и ГОСТ Р 34.10-2001 при согласовании ключей в протоколах IKE и ISAKMP.
- Использование ГОСТ 28147-89 при шифровании вложений в протоколе IPsec ESP.
- Использование ГОСТ Р 34.11-94 при обеспечении целостности в протоколах IPsec AH и ESP.
- Использование алгоритмов ГОСТ Р 34.10, ГОСТ Р 34.11 в профиле сертификата и в списке отзыва сертификатов (CRL) инфраструктуры открытых ключей x.509.

Технический комитет 26 „Криптографическая защита информации“. Проекты.

- Протокол аутентификации на основе пароля с выработкой общего ключа.
- Использование ГОСТ 28147-89, ГОСТ Р 34.11-2012 и ГОСТ Р 34.10-2012 при согласовании ключей в протоколах IKE и ISAKMP.
- Использование рекомендуемых узлов замены ГОСТ 28147-89 для шифрования вложений IPsec ESP.
- Элементы режимов работы блочного шифра ГОСТ 28147-89.

Согласованность с международными стандартами

- HMAC, KDF, PRF;
- IKE, ESP, AH;
- X.509, CMS;
- TLS.

Соответствие требованиям ФСБ России к СКЗИ, специфика российских стандартов

- CMS, TLS — работа в отсутствии криптосистемы с открытым ключом;
- VKO — меры защиты при многократном использовании пары долговременных ключей;
- ESP — ограничение нагрузки на ключи, преобразование ключей, ключевые деревья;
- EKE — специфика работы со смарт-картами;
- KDFTREE — обеспечение работы на едином корневом симметричном ключе.

- Обоснование решений путем сведения вопросов об их стойкости к стойкости базовых алгоритмов, составляющих государственные стандарты.
- Оценка влияния результатов известных в открытой литературе методов анализа алгоритмов и протоколов на стойкость предлагаемых решений.
- Обсуждение результатов анализа на конференциях, публикации по результатам анализа.
- Обеспечение совместимости решений с партнерами на этапе подготовки документов и контрольных примеров.
- Обеспечение работы тестовых стендов открытого доступа.
- Соответствие "Порядку оформления документов, содержащих проекты методических рекомендаций по вопросам, относящимся к стандартизации в области криптографической защиты информации".

Спасибо за внимание!