Некоторые особенности международной стандартизации в области криптографии

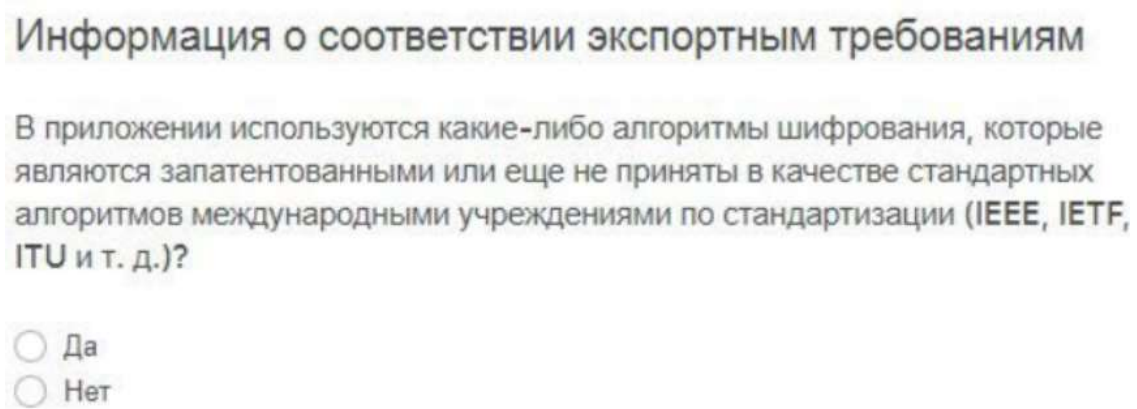
Смышляев Станислав Витальевич,
заместитель генерального директора КриптоПро

КРИПТОПРО

Состояние и перспективы развития ИКТ-инфраструктуры при обеспечении доверия и безопасности

Целесообразность международной стандартизации в области криптографии

- Встраивание российской криптографии в массовое ПО (например, в ОС Windows): трудности с подменой жестко зафиксированных алгоритмов.
- Существенные трудности с корректировкой криптографической архитектуры протокольных решений с учетом российских требований.
- Согласованные с международными организациями идентификаторы («codepoints»), например, для криптонаборов протокола TLS.
- Проблемы с публикацией приложений в AppStore/Google Play с использованием механизмов, не представленных в документах IETF/ISO.



Целесообразность международной стандартизации в области криптографии

- Признание отечественных механизмов безопасности на уровне номеров международных организаций:
  - Устраняет вероятность блокировки российских механизмов зарубежными.
  - Обеспечивает гарантию поддержки наших механизмов в свободном ПО.
  - Снижает вероятность конфликтов при эволюционном развитии технологий.
  - Позволяет достичь согласованности при работе со сторонним ПО (например, Wireshark и TLS).
- Для использования в отраслевых протоколах крайне полезен статус у криптографического механизма «международного стандарта».

ISO/IEC JTC1 SC27 WG2

- Рабочая группа ISO по криптографии и механизмам безопасности.
- Активное участие российских экспертов.
- Присутствие российских алгоритмов в стандартах ISO – в ряде случаев необходимо для применения в протоколах (массовых/отраслевых).
- Продвижение интересов России невозможно без активного вовлечения во все процессы РГ: в частности, для формирования объективных критериев по включению механизмов в документы.

ГОСТы в документах ISO/IEC JTC1 SC27 WG2

- ГОСТ Р 34.10-2012 в ISO/IEC 14888-3.
- ГОСТ Р 34.11-2012 в ISO/IEC 10118-3.
- Работы по продвижению ГОСТ Р 34.12-2015. Дискуссии и политика.
- Российские режимы шифрования со сменой ключа ACPKM в проекте дополнения к ISO/IEC 10116:2017.

Целесообразность международной стандартизации в IETF

- Непрерывное участие российских экспертов в работах IETF позволяет влиять на развитие важнейшей современной технологии – сети Интернет:
  - добиваться соблюдения принципа вариабельности механизмов безопасности (не допускать жесткого фиксирования каких-либо алгоритмов);
  - влиять на фундаментальные принципы построения протоколов безопасности (например, ключевую систему);
  - добиваться учета российских требований к построению криптографических механизмов (например, нагрузка на ключ).

Текущие и перспективные направления работ в IETF

- Документы IETF с российской криптографией:
  - Действующие ГОСТ Р:
  - RFC 6986 – ГОСТ Р 34.11-2012
  - RFC 7091 – ГОСТ Р 34.10-2012
  - RFC 7801 – ГОСТ Р 34.12-2015
- Действующие Рекомендации ТК26:
  - RFC 7836 – алгоритмы, сопутствующие применению ГОСТ Р 34.11-2012 и ГОСТ Р 34.10-2012
  - RFC 8133 – протокол SESPAKE
  - RFC 8645 – плановый документ CFRG, механизмы смены ключей.

Российские эксперты в IETF

- Станислав Смышляев в январе 2020 назначен соруководителем CFRG в IETF (взамен Кенни Патерсона).
- Валерий Смыслов – в составе Security Area Directorate в IETF.
- Российские режимы шифрования со сменой ключа ACPKM в RFC 8645.
- Доклад Лео Перрена на IETF 105 в Монреале о необходимости запрета использования российских криптоалгоритмов в протоколах IETF, дискуссия.

Особенности

- Как в российских, так и в международных организациях по стандартизации, в случае криптографии необходимо проведение анализа безопасности решений.
- Влияние политики на процесс:
  - После Сноудена и скандала со стандартизацией ПДСЧ в NIST, пониженное доверие к представителям государств.
  - Исключение представителя АНБ из руководства CFRG в IETF.
  - Ход дискуссий при включении «Кузнечика» в стандарт ISO.
  - Регулярно возникающие предложения о «запрете» национальной криптографии в международных протоколах.
- Надежный фундамент, научная база и активная вовлеченность в процессы для обеспечения их гибкости – необходимые условия для успешной работы.

Спасибо за внимание!

svs@cryptopro.ru