А. В. Л у н и н (ОАО «ИнфоТеКС»)**. Стандартизация российских криптографических методов защиты информации.**

Одной из самых значимых проблем на пути продвижения российских IT-решений на зарубежные рынки в случае использования средств криптографической защиты информации до последнего времени являлся тот факт, что отечественные криптографические стандарты не являются общепризнанными в мире и относятся к категории национальных. К сожалению, это не только препятствует экспорту, но и делает невозможным сертификацию, в частности, по «Общим критериям» в случае проведения сертификации не в России, а за рубежом, как это, например, имело место в BSI (Германия). Сертификационные органы настаивают на замене российских криптографических алгоритмов на привычные и признанные у них технологии.

Вступление России в ВТО и, особенно, присоединение России к соглашению о взаимном признании сертификатов соответствия «Общим критериям» может привести к существенному изменению на российском рынке средств криптографической защиты конфиденциальной информации. В основном документе, регулирующем разработку, распространение и реализацию СКЗИ — Положении ПКЗ-2005 — есть лишь рекомендация, но не запрет, использования криптографических алгоритмов и протоколов, определенных национальными стандартами.

Таким образом, особую актуальность приобретает задача придания национальным стандартам статуса международных стандартов для обеспечения справедливой конкуренции на российском и международном рынках.

В настоящее время благодаря усилиям российских разработчиков средств криптографической защиты информации ситуация постепенно меняется в лучшую сторону.

Во-первых, комитет IETF утвердил и опубликовал новые стандарты RFC 4490 и RFC 4491, которые описывают применение российских криптографических стандартов в PKI и электронной почте.

Во-вторых, в конце августа 2006 г. состоялось первое заседание рабочей группы по расширению спецификации базового стандарта PKCS#11 механизмами и атрибутами российских криптографических алгоритмов. Работа проводится с согласия и в координации с RSA Security Lab.

В-третье, в настоящее время идет процесс создания в системе Ростехрегулирования нового технического комитета по стандартизации «Криптографическая защита информации».

В мае 2007г. в России состоялось очередное заседание ПК 27 СТК 1 ИСО. На нем была одобрена российская инициатива подготовить дополнение к стандарту ISO/IEC 14888-3 «Information technology–Security techniques–Digital signatures with appendix–Part 3: Discrete logarithm based mechanisms» на основе российского национального стандарта ГОСТ Р 34.10-2001 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи». В настоящее время подготовлена и направлена в секретариат первая редакция указанного дополнения.

По всем указанным направлениям работа будет продолжаться и далее. Ее результаты должны способствовать укреплению позиций российских компаний на зарубежных рынках, увеличению экспорта российских средств криптографической защиты информации, а также защите интересов отечественных разработчиков на национальном рынке при вступлении России в ВТО.