Лунин Анатолий Васильевич
Секретариат технического комитета по стандартизации
«Криптографическая защита информации»
ОАО «ИнфоТеКС»
tc26@infotecs.ru

Процессы стандартизации криптографических методов защиты информации

На наш взляд, одной из самых значимых проблем на пути продвижения российских IT-решения на зарубежные рынки в случае использования в 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» (ISO/IEC 15408:2005 Information technology -- Security techniques -- Evaluation criteria for IT security), в случае проведения сертификации не в России, а за рубежом, как это имело место в BSI (Германия). Сертификационные органы настаивают на замене российских криптографических алгоритмов на привычные и признанные у них технологии. Эта позиция, как минимум, требует со стороны российских производителей дополнительных затрат в части материальных и человеческих ресурсов, а также отодвигает сроки выхода на международные рынки.

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 рекомендация, но не запрет, использования криптографических алгоритмов и протоколов, определенных национальными стандартами. Постановлением Правительства Российской Федерации от 29 декабря 2007 г. № 957 в лицензионных требованиях и условиях при осуществлении разработки, производства шифровальных (криптографических) средств прописана необходимость реализации криптографических алгоритмов, рекомендованных лицензирующим органом.

Таким образом, особую актуальность приобретает задача придания национальным стандартам статуса международных стандартов для обеспечения справедливой конкуренции на российском и международных рынках. И в этом отношении особенно важными становятся вопросы координации и взаимодействия государства и бизнеса.

К российским криптографическим стандартам относятся следующие:

- ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования;
- ГОСТ 34.10-2001. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи;
- ГОСТ 34.11-94. Информационная технология. Криптографическая защита информации. Функция хэширования.

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

Первое. Комитет IETF (Internet Engineering Task Force) утвердил и опубликовал новые стандарты RFC 4490 «Using the GOST 28147-89, GOST R 34.11-94, GOST R 34.10-94, and GOST R 34.10-2001 Algorithms with Cryptographic Message Syntax (CMS)», RFC 4491 «Using the GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms with the Internet X.509 Public Key Infrastructure Certificate and CRL Profile», которые описывают применение российских криптографических стандартов в Инфраструктуре открытых ключей (PKI – Public Key Infrastructure) и электронной почте. Кроме того, принят документ RFC 4357 «Additional Cryptographic Algorithms for Use with GOST 28147-89, GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms» в статусе Informational. К сожалению, работа была выполнена в

инициативном порядке, поэтому до настоящего времени остаются вопросы о качестве выбора отдельных параметров криптографических алгоритмов в данных рекомендациях. Эта проблема была обозначена, в частности, на одной из секций конференции «Методы и технические средства обеспечения безопасности информации», состоявшейся в Стрельне в июне 2007 года.

Второе. В конце августа 2006 года состоялось первое заседание рабочей группы, объединяющей как разработчиков СКЗИ, так и разработчиков информационных систем. Целью создания инициативной группы явилось проведение работ по расширению спецификации базового стандарта PKCS#11: RSA Laboratories. Cryptographic Token Interface Standard механизмами и атрибутами российских криптографических алгоритмов. Работа проводится с согласия и в координации с RSA Security Lab (Магнус Нистром).

Целесообразность проработки дополнений и расширений стандарта PKCS#11 обусловлена необходимостью обеспечить возможность унифицированного использования криптографических примитивов ГОСТ на основе этого программного интерфейса в широком спектре приложений и сервисов, что поможет реально обеспечить признание отечественных стандартов на международном уровне. Кроме того, следование стандарту позволит упорядочить процедуры проверки корректности применения (встраивания) СКЗИ при проведении тематических исследований продуктов. Работа проводиться по согласованию и при координации со стороны уполномоченного органа – ФСБ России.

Можно констатировать, что полтора года спустя готов не один, а два новых профиля для российских стандартов. Сейчас идет процесс апробации и согласования, в т.ч. и с компетентными организациями. До конца 2008 года предстоит провести процедуру регистрации у держателя линейки стандартов, компании RSA

Третье. В настоящее время создан в системе Ростехрегулирования новый технический комитет по стандартизации «Криптографическая защита информации» (ТК 26), основными направлениями работы которого будут как разработка стандартов Российской Федерации, так и участие в разработке международных стандартов в области защиты информации с использованием российских криптографических примитивов. Функции его секретариата будет выполнять ОАО «ИнфоТеКС».

Целью создания технического комитета является обеспечение в Российской Федерации координации работ по организации разработки, принятию и применению документов по стандартизации шифровальных (криптографических) средств защиты информации, а также вопросов их применения в защищенных системах. Технический комитет будет уполномочен рассматривать на своих заседаниях вопросы стандартизации продукции и услуг, классифицируемые в соответствии с кодом Общероссийского классификатора стандартов 35.040 «Наборы знаков и кодирование информации, включая методы обеспечения безопасности ИТ, шифрование и т.д.» и 35.160 «Микропроцессорные системы, включая персональные ЭВМ и т.д.», относящиеся к методам шифрования (криптографического преобразования) информации, способам их реализации, а также методам обеспечения безопасности информационных технологий с использованием криптографического преобразования информации, включая аутентификацию, имитозащиту и электронную цифровую подпись.

В мае 2007 года впервые в России состоялось заседание 27-го Подкомитета Совместного технического комитета № 1 ИСО. В качестве первого шага российская делегация, сформированная национальным комитетом по стандартизации ТК 22 «Информационные технологии», вышла с предложением подготовить дополнение к стандарту ISO/IEC 14888-3:2006(E) «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». 27-ым Подкомитетом было принято положительное решение, российской стороне поручено подготовить необходимые материалы, редактором проекта назначен представитель ОАО «ИнфоТеКС». Такие материалы были подготовлены в установленные сроки, прошло их обсуждение в каждой из стран-членов ИСО. Очередное очное слушание состоится на весеннем заседании ПК27, в Японии, в апреле 2008

года. Мы надеемся, что в ближайшее время удастся осуществить аналогичную процедуру и в отношении остальных российских криптографических стандартов.

Одной из основных причин, подтолкнувших компанию к участию в данной работе, явилось стремление создать равные условия для распространения на международном рынке средств защиты конфиденциальной информации средств российского и зарубежного производства. Следует выразить признательность за поддержку данной инициативы со стороны российских регулирующих и координирующих органов – в первую очередь, ФСБ России, а также Ростехрегулирования и Росинформтехнологии.

В ходе работ по стандартизации в рамках ИСО выявилась еще одна проблема, требующая решения на государственном уровне. Это связано с распределением т.н. объектных идентификаторов – Object Identifiers (OIDs). Следую сложившийся в ИСО практике, а также нашему убеждению, что алгоритмы, принятые в качестве стандартов на национальном уровне, не могут регистрироваться от имени частных компаний, нами было принято решение о регистрации российского дополнения к стандарту 14888-3 на верхнем уровне дерева OID. Тем не менее проблема осталась. Сейчас за Россией закреплено две ветви, одна из них от имени ИСО закреплена за Ростехрегулированием, но именно ее поддержку взяло на себя Росинформтехнологии. Вторая ветвь, практически не развивающаяся, уже от имени МСЭ закреплена за Мининформсвязи России.

Надеемся, что по всем указанным направлениям работа будет продолжатся и далее. Результаты совместных усилий бизнеса и государства будут 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.