А. В. Л у н и н (Москва, ИнфоТеКС)**. Вопросы формирования набора российских криптографических стандартов.**

В связи со значительным применением в России разработанных за рубежом информационных технологий становится практически неизбежным использование внедренных в них на этапе разработки средств информационной безопасности, включая и средства криптографической защиты информации.

Для разработчиков средств информационной безопасности, как правило, общепринятым считается использование механизмов, соответствующих международным стандартам. Базовый набор подобных стандартизованных криптографических механизмов разрабатывается и принимается в рамках 27-го Подкомитета «Информационная безопасность» 1-го Совместного технического комитета «Информационные технологии» международной организации по стандартизации ИСО.

К основным международно признанным криптографическим механизмам относятся следующие группы стандартов ИСО:

1) криптографические протоколы (Entity Authentication, Key Mgt, Non-Repudiation, Time Stamping Services);

2) аутентификация сообщений (Hash Functions, Message Authentication Codes, Check Character Systems);

3) электронная цифровая подпись (Cryptographic Techniques based on Elliptic Curves, Signatures giving Msg Recovery, Signatures with Appendix);

4) шифрование и режимы шифрования (Biometric Template Protection, Authenticated Encryption, Modes of Operation, Encryption, CryptoSign);

5) выработка параметров (Random Bit Generation, Prime Number Generation).

В Российской Федерации имеются лишь следующие национальные криптографические стандарты.

А) ГОСТ 28147 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования»;

Б) ГОСТ Р 34.10 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи»;

В) ГОСТ Р 34.11 «Информационная технология. Криптографическая защита информации. Функция хэширования».

Из криптографических стандартов ИСО в России принят только один: ГОСТ Р ИСО/МЭК 10116 «Информационная технология. Режимы работы для алгоритма n-разрядного блочного шифрования». Однако он уже утратил свою актуальность.

Сложившиеся положение требует принятия следующих неотложных мер: а) определение базового набора криптографических механизмов российской разработки, согласованных по функционалу и параметрам со стандартами ИСО; б) принятие оставшейся части криптографических стандартов ИСО в качестве национальных стандартов; в) организация взаимодействия технических комитетов по стандартизации Ростехрегулирования друг с другом и с другими организациями по стандартизации (в первую очередь, с ITU-T и IETF) с целью подготовки и согласования криптографических механизмов для таких конкретных приложений, как финансовые услуги, оказание государственных услуг, использование интеллектуальных карт, управления правами и др.