А. В. Л у н и н (Москва, ИнфоТеКС)**. О текущем положении дел в области стандартизации криптографичкских методов защиты информации.**

Дается обзор текущего положения дел в области стандартизации криптографических методов защиты информации на национальном, региональном и международном уровнях с учетом следующих знаковых мероприятий, состоявших в текущем году.

24 июня 2010 года в г. Москве, Россия, прошло очередное заседание технического комитета по стандартизации (ТК26) «Криптографическая защита информации» [1], среди рассматривавшихся вопросов был также вопрос включения в Программу разработки национальных стандартов на 2011 год нового стандарта на криптографическую функцию хэширования и соответствующей корректировки действующего стандарта электронной цифровой подписи.

С 1 по 4 июня 2010 года в г. Иркутске, Россия, состоялся первый Байкальский форум «Россия и Беларусь в информационном сообществе», на котором рассматривались актуальные проблемы информационного взаимодействия и информационной безопасности Беларуси и России и пути их решения в Союзном государстве. В рамках данного мероприятия обсуждались в том числе и вопросы стандартизации как в каждом из государств, так и рамках Союзного государства [2].

С 19 по 23 апреля 2010 года в г. Малаке, Малайзия, прошло 40-е заседание WG 2 Cryptography and Security Mechanisms / SC 27 Security Techniques / JTC 1 Information Technology / ISO International Organisation for Standardisation [3]. В ходе заседания продолжилось обсуждение предложений о включении алгоритма ГОСТ 28147-89 в перечень алгоритмов блочного шифрования, являющихся стандартами ИСО.

4 июня 2010 года успешно завершился начатый еще в 2007 году проект, в результате которого алгоритм выработки и проверки цифровой подписи по ГОСТ Р 34.10-2001, предложенный российскими специалистами в качестве дополнения к международному стандарту ISO/IEC 14888-3:2006(E), получил официальное признание и вступил в силу [4].

СПИСОК ЛИТЕРАТУРЫ

1. Протокол заседания технического комитета по стандартизации (ТК26) «Криптографическая защита информации» от 24 июня 2010 года, www.tc26.ru.
2. Комплексная защита информации. Материалы XV Международной конференции 1–4 июня 2010 года, Иркутск (Россия). М.: 2010, 170 с.
3. Resolutions of the 40th meeting of SC 27/WG 2, April 2010, Melaka, Malaysia ISO/IEC JTC 1/SC 27 N8789.
4. ISO/IEC 14888-3:2006/Amd 1:2010. Elliptic Curve Russian Digital Signature Algorithm, Schnorr Digital Signature Algorithm, Elliptic Curve Schnorr Digital Signature Algorithm, and Elliptic Curve Full Schnorr Digital Signature Algorithm.