УДК 004.7

Обзор белорусских криптографических стандартов

Белова С.В.
Белорусский национальный технический университет

Знание стандартов и спецификаций важно для специалистов в области информационной безопасности по целому ряду причин: 1) необходимость следования некоторым криптографическим стандартам закреплена законодательно; 2) стандарты регулируют требования к программным и аппаратным средствам, методики оценки и сертификации систем; 3) стандарты и спецификации - одна из форм накопления знаний, в них зафиксированы апробированные, высококачественные решения, разработанные наиболее квалифицированными специалистами; 4) стандарты и спецификации являются основным средством обеспечения взаимной совместимости аппаратно-программных систем и их компонентов.

Количество стандартов и спецификаций в области информационной безопасности велико. Существуют международные стандарты, стандарты отдельных фирм, стандарты комитетов и объединений, национальные стандарты. В Республике Беларусь разработаны и утверждены свои государственные стандарты в области информационной безопасности. Официальные редакции стандартов можно найти на сайте www.tnpa.by.

Одним из важнейших является стандарт СТБ 34.101.27-2011 «Информационные технологии и безопасность. Требования безопасности к программным средствам криптографической защиты информации». Данный стандарт устанавливает общие требования безопасности к программным средствам, которые используются для криптографической защиты информации ограниченного распространения. Стандарт предназначен для использования заказчиками, разработчиками, а также экспертами при оценке надежности программных средств криптографической защиты.

Стандарт СТБ 34.101.31-2011 «Информационные технологии. Защита информации. Криптографические алгоритмы шифрования и контроля целостности» определяет семейство криптографических алгоритмов симметричного шифрования, которые используются для защиты информации при ее хранении, передаче и обработке.

Введены в действие стандарты электронной цифровой подписи, алгоритмов генерации псевдослучайных чисел, протокола защиты транспортного уровня (TLS), протокола формирования общего ключа на основе эллиптических кривых, алгоритма хэширования.