**А. В. Уривский** (Москва, ОАО «ИнфоТеКС»). **Проект государственного стандарта на криптографическую хэш-функцию.**

Криптографические функции хэширования являются одним из наиболее важных примитивов, используемых при создании средств криптографической защиты информации. В России действует стандарт на хэш-функцию — ГОСТ Р 34.11-94 [1]. Последние результаты криптоанализа стандарта указывают на его недостатки с теоретической точки зрения. Поэтому имеется потребность в создании новой отечественной криптографически стойкой хэш-функции.

Для стандартизации предлагается хэш-функция «Стрибог» с длинами выхода в 256 и 512 бит со следующими синтезными решениями [2]. Базовая конструкция — стандартная итерационная конструкция Меркля–Дамгорда [3, 4] с процедурой МД-усиления. Дополнительные элементы — завершающее преобразование, состоящее в применении функции сжатия к сумме всех блоков сообщения по модулю $2^{512}$, и использование на каждом шаге хэширования различных функций сжатия, выбор которых зависит от номера блока сообщения. Данные решения служат для уменьшения эффективности ряда известных методов криптоанализа.

Функция сжатия хэш-функции «Стрибог» построена на основе блочного шифра при помощи конструкции Миягучи–Принеля, признанной одной из наиболее стойких. В качестве блочного шифра выбран шифр типа XSL (SP-сеть), длина блока и ключа которого равна 512 битам. Данный тип шифров хорошо изучен и достаточно прост с точки зрения криптоанализа и обоснования свойств.

Разработчики провели экспериментальные исследования производительности хэш-функции «Стрибог». Для 64-битной платформы Intel Xeon E5335 2 ГГц и одном используемом ядре получена производительность порядка 51 такта работы процессора на 1 байт хэшируемых данных или около 40 Мбайт/с, что на 20% больше, чем у ГОСТ Р 34.11-94.

С текстом проекта стандарта можно ознакомиться по адресу http://infotecs.ru/laws/gost/proj/gost3411.pdf.

## СПИСОК ЛИТЕРАТУРЫ

1. ГОСТ Р 34.11-94. Информационная технология. Криптографическая защита информации. Функция хэширования. Введ. 01.01.1995. М.: Изд-во стандартов, 1994, IV, 12 с.
2. *Матюхин Д. В.*, *Шишкин В. А.*, *Рудской В. И.* Перспективный алгоритм хэщирования. — Доклад на коференции РусКрипто'2010, 2010.
3. *Damgård I.* A design principle for hash functions. — In: Proceedings of Advances in Cryptogy — Crypto'89, 1989, p. 416–427.
4. *Merkle R. C.* One Way Hash Functions and DES. — In: Proceedings of Advances in Cryptogy — Crypto'89, 1989, p. 428–446.