Развитие нормативной базы для разработки средств криптографической защиты информации

А.С. Кузьмин (ФСБ России)

26 марта 2014 года

Основные направления развития нормативной базы разработки СКЗИ на современном этапе

- определение порядка перехода к использованию стандарта электронной цифровой подписи ГОСТ Р 34.10-2012 в случаях, подлежащих регулированию со стороны ФСБ России

- разработка новой редакции «Требований к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну»

- обновление стандарта шифрования ГОСТ 28147-89

О переходе к использованию ГОСТ Р 34.10-2012

- Стандарт введен в действие 1 января 2013 года вместе с новым стандартом хэш-функции ГОСТ Р 34.11-2012, разработка порядка перехода велась с октября 2012 года

- январь 2013 года – разработан порядок перехода для сертифицированных средств ЭП Банка России

- ноябрь 2013 года – общий проект порядка перехода (на основе порядка для ЦБ) опубликован на сайте ТК 26 для дополнительного обсуждения

- январь 2014 года – порядок перехода доработан и утвержден

Порядок перехода на ГОСТ Р 34.10-2012
(основные положения, полный текст на `tc26.ru`)

- Для средств ЭП, ТЗ на разработку которых утверждено после 31 декабря 2012 года, должна быть *предусмотрена* реализация функций средства по ГОСТ Р 34.10-2012 (это *не исключает* использования в них ГОСТ Р 34.10-2001)

- после 31 декабря 2013 года не осуществлять подтверждение соответствия «Требованиям к средствам электронной подписи» средств ЭП, в которых такая реализация не предусмотрена (есть исключения – см. полный текст)

- Использование ГОСТ Р 34.10-2001 для *формирования подписи* после 31 декабря 2018 года не допускается

О новой редакции Требований

- традиционная корректировка используемых числовых значений параметров и характеристик с течением времени

- предложения разработчиков по упрощению Требований путем исключения неиспользуемых классов СКЗИ

- необходимость упорядочения ситуации с сертификацией СКЗИ, использующих сертифицированные криптобиблиотеки (подробнее в докладе В.М. Простова)

Подготовлен проект новой редакции, утвержден в качестве временных Требований и будет доработан по результатам «опытной эксплуатации» и обсуждения

Об обновлении стандарта ГОСТ 28147-89

В 2014 году предполагается разработать и представить на утверждение в Росстандарт проекты национальных стандартов:

- «Информационная технология. Криптографическая защита информации. Блочные шифры» на основе ГОСТ 28147-89 с фиксированным набором подстановок и перспективного шифра с длиной блока 128 бит (доклад на Рускрипто 2013)

- «Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров» (будут выделены в отдельный стандарт, подробнее – в докладе В.А. Шишкина на секции «Криптография и криптоанализ»)

Спасибо за внимание!