# Расширен перечень нацстандартов, определяющих криптографические алгоритмы и протоколы

jurliga.ligazakon.ua/news/2015/2/16/124401.htm

Это событие имеет существенное влияние на введение единых требований для применения криптографических механизмов в Украине

Министерство экономического развития и торговли приказом от 30 декабря 2014 года № 1493 методом подтверждения приняло европейские и международные нормативные документы как **национальные стандарты Украины**.

**С 1 января 2016 года** в Украине вступают в силу **55** международных и европейских стандартов. Среди них 32 определены Перечнем международных и европейских стандартов, других актов технического регулирования для гармонизации с целью реформирования, развития и обеспечения интероперабельности системы электронной цифровой подписи, утвержденным приказом Министерства юстиции и Администрации Госспецсвязи от 25 декабря 2014 года № 2170/5/703. Из них 15 принято повторно в связи с изменением международных стандартов-оригиналов. Речь идет о наиболее распространенных в мире криптографических алгоритмах и протоколах - RSA, DSA, KCDSA, ECDSA, EC KCDSA, EC-GDSA т.д.

Это событие имеет существенное влияние на введение единых требований для применения криптографических механизмов, в частности, в ключевых элементах инфраструктуры открытых ключей ЭЦП в Украине.

В 2014 году Минэкономразвития принято еще два национальные стандарты, которыми определяются

криптографические алгоритмы украинской разработки:

**-** функция хеширования (ГОСТ 7564:2014, разработан на заказ Госспецсвязи во исполнение приказа Минэкономразвития от 2 декабря 2014 года № 1431, вступает в силу **с апреля 2015 года**),

**-** алгоритм симметричного блочного преобразования (ГОСТ 7624:2014, разработан на заказ Госспецсвязи во исполнение приказа Минэкономразвития от 29 декабря 2014 года № 1484, вступает в силу **с июля 2015 года**).

Криптографические алгоритмы, определяемые этими стандартами, являются гибкими, поддерживают размер блока и длины ключа от 128 до 512 бит, что является уникальным в мире. Криптографические преобразования, применяемые в алгоритмах, соответствующих современным требованиям относительно уровня криптографической стойкости и быстродействия. Алгоритмы разработаны с учетом существующих и потенциальных угроз, необходимости их активного использования в течение нескольких следующих десятилетий, учитывая интенсивное развитие информационных технологий. ГОСТ 7624:2014 определяет десять различных режимов работы (применения), которые широко распространены в соответствии с международным стандартом ISO/IEC 10116:2006.

Госспецсвязи после официальной публикации текстов вышеуказанных стандартов будет готова проводить подтверждение соответствия средств КЗИ национальным стандартам, в том числе гармонизированным с европейскими и международными.

Вместе с тем Госспецсвязи продолжит развивать стандартизацию отечественных криптографических алгоритмов и протоколов, не ограничивая применение гармонизированных стандартов в продуктах для защиты конфиденциальной информации, а также сосредоточит усилия на использовании лучших практик их применения для защиты информации, требование относительно защиты которой установлена законом.

Комментариев ()