существующих алгоритмов шифрования не дают достаточной степени защиты информации. Поэтому, в наше время, для защиты данных используются NGN методы. Это комплексный подход, представляющий собой комбинирование нескольких алгоритмов защиты данных.

Алгоритмы, составленные NGE являются результатом более чем 30 лет мирового прогресса и эволюции в области криптографии. Каждый составляющий компонент NGE имеет свою историю. NGE состоит из множества всемирно используемых алгоритмов, протестированных на протяжении многих лет, и публично доступных алгоритмов.

При проектировании системы NGN стоит придерживаться еще одного правила: криптостойкость алгоритма должна определяться только криптостойкостью ключей шифрования. Все остальное, например техническое описание самого алгоритма, методы построения системы защиты, должны заведомо считаться известными потенциальному противнику.

Таким образом, система защиты данных, способная обеспечить достаточную защиту от современных угроз, должна представлять собой комплексную систему из различных элементарных методов проверки:

– шифрование с использованием сильного алгоритма и ключа большой длины;
– безопасный обмен ключами;
– аутентификация пользователя;
– авторизация пользователя;
– проверка целостности данных;
– проверка наличия чужого вмешательства;
– сокрытие канала передачи.

Литература

1. Cisco Systems – Next Generation Encryption [Электронный ресурс] — Режим доступа: http://www.cisco.com/web/about/security/intelligence/nextgen_crypto.html#ftn2

2. Super Cryptography: The Next Generation Encryption [Электронный ресурс] — Режим доступа: http://thehackernews.com/2011/11/super-cryptography-next-generation.html

3. CNG Features [Электронный ресурс] — Режим доступа: https://msdn.microsoft.com/en-us/library/windows/desktop/bb204775(v=vs.85).aspx

ВОПРОСЫ ОБЕСПЕЧЕНИЯ СТОЙКОСТИ КЛЮЧЕЙ ПРИ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЕ ИНФОРМАЦИИ

Г.А. Власова, А.И. Букштынова

Известно, что стойкость криптографической системы определяется стойкостью ключа. Развитие средств вычислительной техники приводит к необходимости увеличения длины ключей для обеспечения требуемого уровня криптостойкости.

До 2002 года стойкими считались RSA-ключи длиной 64 бит (в 1997 г. удалось взломать RSA-шифр с длиной ключа 56 бит за 250 дней). В 2009 году был взломан шифр с длиной ключа 768 бит, а уже в 2010 году — 1024 бит, на что потребовалось всего 100 ч.

В 2015 году появилась информация об успешном взломе 4096-битных RSA-ключей. Однако в дальнейшем было показано, что взломать удалось лишь отдельные отбракованные ключи. Таким образом, на сегодняшний день RSA-ключи длиной 4096 бит можно считать криптостойкими.

Согласно [1], одинаковую криптостойкость имеют ключи симметричных систем с длиной 80 бит и ключи асимметричных систем с длиной 768 бит; ключи длиной 128 бит и 2304 бит соответственно. Анализируя тенденции взлома ключей асимметричного алгоритма RSA, можно сделать вывод, что для симметричного алгоритма AES ключи длиной 128 бит использовать не следует.

Отметим, что наряду с устройствами криптографической защиты по ГОСТ 28147-89 и AES256, встречаются коммерческие предложения с длиной ключа, не обеспечивающие достаточный уровень безопасности (AES128), либо вовсе без информации о длине ключа. Поэтому выбор условий функционирования средств криптографической защиты, в том числе длины ключа, становится необходимым условием обеспечения безопасной работы систем хранения, обработки и передачи информации.

Литература

1. *Деднев М.А., Дыльнов Д.В., Иванов М.А.* Защита информации в банковском деле и электронном бизнесе. М., 2004.