УДК 681

СТАНДАРТИЗАЦИЯ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ В РЕСПУБЛИКЕ БЕЛАРУСЬ: ОСОБЕННОСТИ И НЕУЧТЕННЫЕ ФАКТОРЫ

Лебедев А.Н. [1], Афоненко А.А. [2]
[1]Московский государственный технический университет им. Н.Э. Баумана
[2]ЗАО «Аладдин Р.Д.»
Москва, Российская Федерация

С 2011 г. в Республике Беларусь начался переход на новые стандарты крипто алгоритмов: хэширования, шифрования, выработки и проверки электронной подписи, согласования общего ключа и др. Поскольку в крипто протоколах, применяемых на практике (SSL/TLS, почтовые протоколы на основе CMS), для идентификации алгоритмов используются ASN.1-структуры, встал вопрос стандартизации структур данных, описывающих новые криптографические алгоритмы.

По этой причине новые белорусские стандарты содержат раздел, описывающий ASN.1-структуры и идентификаторы (OID) Они применяются при использовании крипто алгоритмов. Для алгоритмов, действовавших ранее (ГОСТ 28147-89, СТБ 1176.1-99, СТБ 1176.2-99), выпущен документ (имеет статус предварительного стандарта) СТБ П 34.101.50 "Информационные технологии и безопасность. Правила регистрации объектов информационных технологий". Однако, формальное описание белорусских структур ASN.1 имеет неоднозначности. Эти неоднозначности присутствуют в описании структур для алгоритмов, сейчас напрямую не используемых в популярных крипто протоколах, и могут стать препятствием для реализации криптографических приложений только при расширении вариантов применения алгоритмов.

СТБ 34101.31-2011. “Информационные технологии и безопасность. Защита информации. Криптографические алгоритмы шифрования и контроля целостности”.

В документе описываются следующие основные крипто алгоритмы: шифрование, выработка имитовставки, одновременно шифрование и имитозащита данных, одновременно шифрование и имитозащита ключа, хэширование, а также вспомогательные крипто алгоритмы расширения ключа и преобразования ключа (последний называется диверсификацией ключа в терминологии, принятой в РФ).

Суть одновременно шифрования и имитозащиты заключается в выполнении шифрования и вычисления имитовставки за время меньшее, чем O(2n), где n-объем данных. Эти алгоритмы встречаются в академической литературе, однако не имеют собственной структуры в CMS, что затрудняет их применение в почтовых протоколах. С натяжкой для указанных целей можно использовать структуру *EncryptedData*, применяемую для описания шифрованных данных, при внедрении имитовставки в состав шифрованных данных с проверкой ее при расшифровании. Белорусский стандарт одновременно шифрования и имитозащиты имеет следующую отличительную особенность - в нем защищаемое сообщение делится на две части: критическое сообщение X (которое предстоит зашифровать и учесть при вычислении имитовставки) и открытое сообщение I (которое используется только при вычислении имитовставки). При таком подходе непонятно как использовать структуру *EncryptedData* для этого алгоритма: в ней нет отдельных полей для X и I. Можно предположить, что в таком случае I должно быть параметром (не входными данными) самого алгоритма, и включаться в структуру *AlgorithmIdentifier* его описания (вместе с параметром синхропосылки). Однако в стандарте про это не говорится ни слова.

Алгоритмы одновременно шифрования и имитозащиты ключа являются разновидностью алгоритмов защиты ключа (KeyWrap), при которой используется шифрование для сокрытия ключа и выработка имитовставки для контроля его целостности. Алгоритмы имеют прямое преобразование (в стандарте СТБ 34101.31-2011 оно называется алгоритмом установки защиты) и обратное (алгоритм снятия защиты). Диверсификация ключа (преобразование ключа в белорусской формулировке) предназначена для порождения нового ключа на основе старого и дополнительной информации, называемой UKM (User Keying Material). В алгоритмах защиты и диверсификации ключа он представляется только своим значением (например, в алгоритмах шифрования). Белорусские стандарты имеют особенность: в алгоритме одновременно шифрования и имитозащиты ключ определяется не только значением X, но и заголовком I, а в алгоритме диверсификации еще и уровнем D. Сразу встают вопросы:

1) Если ключ шифрования определяется тройкой (D, I, X), то как восстановить уровень ключа D после снятия защиты ключа, если параметр D вообще не фигурирует? Значит ли это, что уровень D должен быть параметром алгоритма снятия защиты ключа? Далее, алгоритм снятия защиты ключа требует априорного знания заголовка I ключа для проверки его целостности. Значит ли это, что заголовок I также должен быть параметром алгоритма снятия защиты ключа?

2) Если ключ шифрования определяется парой (I, X), то уровень D ключа должен быть параметром алгоритма диверсификации ключа. Однако в этом случае не совсем корректно говорить именно о параметре D как об уровне ключа. Скорее, это уже параметр ключевой системы. Кроме того, вопрос о заголовке I как параметре алгоритма снятия защиты ключа остается актуальным.

3) Если ключ шифрования определяется только своим значением X, то для алгоритма защиты ключа заголовок I должен быть параметром алгоритма, а для алгоритма диверсификации такими параметрами должны быть заголовок I и уровень ключа D. Это не выглядит правильным, поскольку параметр I (в меньшей степени D) является атрибутом ключа, а не алгоритма.

Эти соображения влияют на то, какие параметры содержатся в структуре *AlgorithmIdentifier* описания алгоритмов одновременно шифрования и имитозащиты (прямого и обратного преобразования) и диверсификации ключа. В стандарте СТБ 34101.31-2011 сказано, что при указании параметров I и D в структуре *AlgorithmIdentifier*, они должны представляться в виде ASN.1-типа *OCTET STRING*, этого недостаточно (при одновременном использовании непонятен порядок следования).

СТБ 34101.45-2013. “Информационные технологии и безопасность. Алгоритмы электронной цифровой подписи и транспорта ключа на основе эллиптических кривых”.

В документе описываются основные крипто алгоритмы: выработка и проверка электронной подписи и алгоритм транспорта ключа. Транспорт ключа имеет прямое преобразование (в СТБ 34101.45-2013 называется алгоритмом создания токена ключа) и обратное (разбор токена ключа). Частью алгоритма транспорта ключа является алгоритм одновременно шифрования и имитозащиты ключа. Поэтому вопросы, связанные с интерпретацией ключа шифрования из предыдущего раздела, актуальны и в контексте транспорта ключа. Поскольку описание транспорта ключа в структуре *AlgorithmIdentifier* для почтовых приложений и протокола SSL/TLS является критичным, в стандарте СТБ 34101.45-2013 во избежание неоднозначности явно указывается, что *“поле parameters должно равняться NULL, а заголовок I транспортируемого ключа полагаться равным 0…0”*.

Поэтому встают следующие вопросы:

1) Если ключ шифрования определяется тройкой (D, I, X) или парой (I, X), то формулировка ограничивает использование алгоритма транспорта для почтовых приложений и протокола SSL/TLS ключами с нулевым заголовком. Как в первом варианте восстановить уровень ключа D после выполнения алгоритма разбора токена ключа, если в нем параметр D вообще не фигурирует?

2) Если ключ шифрования определяется только значением X, то заголовок I ключа должен быть параметром транспорта и формулировка ограничивает использование параметра I алгоритма транспорта в почтовых приложениях и протоколе SSL/TLS только нулевыми значениями.

На наш взгляд, более логично было бы в поле parameters структуры AlgorithmIdentifier помещать не NULL, а структуру AlgorithmIdentifier для одновременно шифрования и имитозащиты ключа (естественно, после ее формального описания, не допускающего неоднозначностей).

В заключение заметим, что исправление указанных недостатков было бы проще произвести, если бы белорусские стандарты описывали только криптографические алгоритмы, а их ASN.1-структуры и использование в рамках криптографических протоколов было бы описано в отдельном документе (стандарте или RFC).

УДК 535.24

СОЗДАНИЕ НАЦИОНАЛЬНОЙ ЭТАЛОННОЙ БАЗЫ БЕЛАРУСИ ДЛЯ СПЕКТРОРАДИОМЕТРИЧЕСКОЙ КАЛИБРОВКИ ОПТИЧЕСКОЙ АППАРАТУРЫ ДИСТАНЦИОННОГО ЗОНДИРОВАНИЯ ЗЕМЛИ

Длугунович В.А. [1], Никоненко С.В. [1], Беляев Ю.В. [2], Кучинский П.В.[2], Попков А.П.[2], Цикман И.М.[2], Скумс Д.В.[3], Тарасова О.Б.[3]

[1]Институт физики НАН Беларуси

[2]НИИПФП имени А.Н. Севченко БГУ

[3]Белорусский государственный институт метрологии

Минск, Республика Беларусь

Выполнение национальной космической программы и развитие Белорусской космической системы дистанционного зондирования (ДЗ) Земли выдвигают задачи метрологического обеспечения спектрально-энергетических калибровок аэрокосмических систем. Это обусловлено тем, что спектрорадиометрические и радиометрические измерения играют значимую роль среди методов и средств измерений, используемых в ДЗ (геоинформационные системы, производственно-хозяйственная инфраструктура, сельское и лесное хозяйство, экология, мониторинг и контроль