

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

к проекту предварительного государственного стандарта
СТБ П 34.101.XX «Информационные технологии и безопасность. Правила
регистрации объектов информационных технологий»

1. Основание для разработки государственного стандарта

Проект стандарта был разработан в соответствии с Планом государственной стандартизации Республики Беларусь на 2011 год в ходе выполнения работ по договору №0312/2010/605Д от 23.12.2010г. между Национальным банком Республики Беларусь и ЗАО «АВЕСТ»

2. Цели и задачи разработки государственного стандарта

Целью разработки государственного стандарта является установка правил определения идентификаторов объектов информационных технологий, определяемых в соответствии с положениями ГОСТ 34.973-91, в том числе порядок формирования дерева идентификаторов объектов информационных технологий, используемых в Республике Беларусь, определения организаций, ответственных за присвоение значений компонентов данных идентификаторов.

Разрабатываемый государственный стандарт направлен на решение задачи назначения идентификаторов объектов информационных технологий при разработке систем управления открытыми ключами (инфраструктуры открытых ключей), систем, использующих стандартизованные форматы данных, криптографические алгоритмы и протоколы, определенные в технических нормативных правовых актах Республики Беларусь.

Разрабатываемый государственный стандарт обеспечит необходимую нормативную базу для решения задач развертывания и функционирования Государственной системы управления открытыми ключами Республики Беларусь.

Для достижения поставленной цели необходимо решить следующие задачи:

- 1) определить иерархическую структуру дерева идентификаторов объектов Республики Беларусь;
- 2) определить основные организации Республики Беларусь, выступающие в роли регистрационных служб;
- 3) разработать идентификаторы для основных категорий объектов информационных технологий, используемых в системах криптографической защиты информации, управления открытыми ключами;
- 4) оформить стандарт в соответствии с требованиями ТКП 1.5-2004 «Система технического нормирования и стандартизации Республики Беларусь. Правила построения, изложения, оформления и содержания технических кодексов установившейся практики и государственных стандартов».

3. Характеристики объекта стандартизации

Во многих стандартизованных форматах данных (например, формате сертификатов открытых ключей, форматах данных, используемых в электронной почте и т.д.) применяются идентификаторы алгоритмов, а также указываются используемые в этих алгоритмах параметры (в составе структуры, стандартизуемой вместе с идентификатором алгоритма — указанный

идентификатор в этом случае можно также считать и идентификатором структуры параметров).

Многие отечественные алгоритмы не имеют зафиксированных публично идентификаторов, которые можно использовать в стандартизированных форматах данных. Более того, у алгоритмов с опубликованными идентификаторами не стандартизированы соответствующие структуры данных, что снова не позволяет их встраивать в высокоуровневые системы. Поэтому при выпуске приложений, описывающих использование отечественных алгоритмов в стандартизированных форматах данных, следует приводить идентификаторы алгоритмов и соответствующие им структуры параметров.

Необходимо обратить внимание на несколько моментов:

1. Структура параметров алгоритмов СТБ 1176.2 и Проекта РД «Банковские технологии. Протоколы формирования общего ключа», используемая внутри формата X.509 сертификатов открытых ключей, регламентируется РД РБ 07040.1206-2004, однако в этом документе не указаны идентификаторы алгоритмов. При выпуске приложений, описывающих использование указанных алгоритмов в сертификатах открытых ключей X.509, следует устранить указанный недостаток.
2. Идентификаторы, структура параметров и способ использования алгоритма ГОСТ 28147-89 применительно к форматам данных Интернет (RFC 3852) предложены российской компанией CryptoPro и регламентируются Интернет-стандартами RFC 4357 и RFC 4490. Отметим, что приведенный способ использования алгоритма ГОСТ 28147-89 в указанных стандартах является достаточно специфичным:
 - в некоторых случаях применяется нестандартизированный режим сцепления блоков;
 - в некоторых случаях производится смена ключа шифрования данных (способом, описанным в RFC 4357) после обработки определенного объема данных;
 - используется контроль целостности ключа шифрования данных (не требуемый стандартом RFC 3852).

4. Взаимосвязь проекта государственного стандарта с другими документами

Проект стандарта ссылается на ГОСТ 34.973-91 «Информационная технология. Взаимосвязь открытых систем. Спецификация абстрактно-синтаксической нотации версии 1 (ASN.1)».

Внесения изменений в другие государственные стандарты Республики Беларусь не потребуются.

5. Предполагаемый срок введения стандарта: 01 января 2012 года.

6. Источники информации

В качестве источников информации выступают:

- 1) СТБ 1176.1-99 «Информационная технология. Защита информации. Функция хэширования»;
- 2) СТБ 1176.2-99 «Информационная технология. Защита информации. Процедуры выработки и проверки электронной цифровой подписи»;
- 3) Проект СТБ 34.101.19-2011 «Информационные технологии. Форматы сертификатов и списков отозванных сертификатов инфраструктуры открытых ключей»;

- 4) СТБ 34.101.31-2011 «Информационные технологии. Защита информации. Криптографические алгоритмы шифрования и контроля целостности»;
- 5) ГОСТ 28147-89 «Система обработки информации. Защита криптографическая. Алгоритм криптографического преобразования»;
- 6) РД РБ 07040.1206-2004 «Банковские технологии. Формат сертификатов открытых ключей и списков отозванных сертификатов»;
- 7) RFC 3852 «Cryptographic Message Syntax (CMS)»;
- 8) RFC 4357 «Additional Cryptographic Algorithms for Use with GOST 28147-89, GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms».
- 9) RFC 4490 «Using the GOST 28147-89, GOST R 34.11-94, GOST R 34.10-94, and GOST R 34.10-2001 Algorithms with Cryptographic Message Syntax (CMS)».

Директор ЗАО «АВЕСТ»

А.Н.Скобов

ИСПОЛНИТЕЛИ

Начальник отдела разработки
программных средств защиты
информации ЗАО «АВЕСТ»

Д.В.Шпилевский

Начальник группы контроля качества ЗАО
«АВЕСТ»

С.В.Степченков

Бухгалтер-экономист ЗАО «АВЕСТ»

Е.И.Ковальчук