

**Информационные технологии и безопасность
Правила регистрации объектов
информационных технологий**

**Інфармацыйныя тэхналогіі і бяспека
Правілы рэгістрацыі аб'ектаў
інфармацыйных тэхналогій**

Настоящий проект предстандарта не подлежит применению до его утверждения



Ключевые слова: абстрактно-синтаксическая нотация версии 1, идентификатор объекта, дерево идентификаторов, регистрация идентификаторов

Предисловие

Цели, основные принципы, положения по государственному регулированию и управлению в области технического нормирования и стандартизации установлены Законом Республики Беларусь «О техническом нормировании и стандартизации».

1 РАЗРАБОТАН Закрытым акционерным обществом «АВЕСТ».
ВНЕСЕН Национальным Банком Республики Беларусь.

2 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ постановлением Госстандарта Республики Беларусь
от _____ № ____

3 ВВЕДЕН ВПЕРВЫЕ

4 Срок предоставления разработчику предстандарта замечаний и предложений, предложений о целесообразности (нецелесообразности) перевода предстандарта в государственный стандарт, до 01.07.2012 г.

Разработчик: Закрытое акционерное общество «АВЕСТ».

Адрес: 220116, г. Минск, пр. газеты имени «Правда», д. 5, пом. 3Н.

Тел.: +375 17 207-99-74, +375 17 207-92-34

E-mail: welcome@avest.by

Настоящий предстандарт не может быть тиражирован и распространен без разрешения Госстандарта Республики Беларусь

Издан на русском языке

Содержание

1 Область применения	1
2 Нормативные ссылки	1
3 Термины и определения	1
4 Общие положения	2
4.1 Назначение	2
4.2 Идентификаторы объектов	2
5 Дерево идентификаторов	2
6 Регистрация	3
6.1 Методы регистрации	3
6.2 Назначение идентификаторов в ТНПА	3
6.3 Назначение идентификаторов регистрирующей организацией	3
Приложение А (рекомендуемое) Идентификаторы регистрирующих организаций	5
Приложение Б (рекомендуемое) Идентификаторы объектов СТБ 1176.1	6
Приложение В (рекомендуемое) Идентификаторы объектов СТБ 1176.2	7
Приложение Г (рекомендуемое) Идентификаторы объектов ГОСТ 28147	15
Приложение Д (рекомендуемое) Идентификаторы объектов Государственной системы управления открытыми ключами	17
Библиография	18

ПРЕДВАРИТЕЛЬНЫЙ ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ БЕЛАРУСЬ

Информационные технологии и безопасность Правила регистрации объектов информационных технологий

Інфармацыйныя тэхналогіі і бяспека Правілы рэгістрацыі аб'ектаў інфармацыйных тэхналогіі

Information technology and security
Procedures for registering information technology objects

Дата введения 201_ _ - _
Дата окончания действия 201_ _ - _

1 Область применения

Настоящий предварительный государственный стандарт (далее – предстандарт) устанавливает правила регистрации объектов информационных технологий. Регистрация состоит в назначении объектам уникальных идентификаторов. Идентификаторы определяются в соответствии с соглашениями абстрактно-синтаксической нотации версии 1 (далее – АСН.1), заданными в ГОСТ 34.973-91. В предстандарте определена структура дерева идентификаторов, определены методы назначения идентификаторов.

Настоящий предстандарт применяется при разработке и эксплуатации информационных систем, в которых используются стандартизированные объекты.

2 Нормативные ссылки

В настоящем предстандарте использованы ссылки на следующие технические нормативные правовые акты в области технического нормирования и стандартизации (далее – ТНПА):

СТБ 1176.1-99 Информационная технология. Защита информации. Функция хэширования

СТБ 1176.2-99 Информационная технология. Защита информации. Процедуры выработки и проверки электронной цифровой подписи

СТБ 34.101.19-2011 Информационные технологии. Форматы сертификатов и списков отозванных сертификатов инфраструктуры открытых ключей

СТБ 34.101.31-2011 Информационные технологии. Защита информации. Криптографические алгоритмы шифрования и контроля целостности

ГОСТ 28147-89 Система обработки информации. Защита криптографическая. Алгоритм криптографического преобразования

ГОСТ 34.973-91 (ИСО 8824-87) Информационная технология. Взаимосвязь открытых систем. Спецификация абстрактно-синтаксической нотации версии 1 (АСН.1)

Примечание - При пользовании настоящим предварительным стандартом целесообразно проверить действие ТНПА по каталогу, составленному на 1 января текущего года, и по соответствующим информационным указателям, опубликованным в текущем году. Если ссылочные ТНПА заменены (изменены), то при пользовании настоящим предстандартом следует руководствоваться замененными (измененными) ТНПА. Если ссылочные ТНПА отменены без замены, то положение, в котором дана ссылка на них, применяется в части, не затрагивающей эту ссылку.

3 Термины и определения

В настоящем предстандарте применяются термины и определения ГОСТ 34.973, а также следующие термины с соответствующими определениями:

3.1 регистр идентификаторов – набор записей (на бумаге или в электронном виде), которым управляет регистрирующая организация. Каждая запись представляет собой описание объекта информационных технологий и идентификатор этого объекта.

3.2 регистрация – назначение объектам информационных технологий уникальных идентификаторов.

3.3 регистрирующая организация, РО – организация, наделенная полномочиями выполнять регистрацию объектов информационных технологий.

4 Общие положения

4.1 Назначение

В настоящем предстандарте определяются правила регистрации объектов информационных технологий. Регистрация состоит в назначении объектам уникальных идентификаторов. Единые идентификаторы объектов обеспечивают унификацию и совместимость различных информационных систем.

В настоящем предстандарте рассматриваются объекты, связанные с безопасностью: форматы криптографических данных, типы ключей, криптографические алгоритмы, параметры алгоритмов и др. В перечень объектов включаются также регистрирующие организации, которые назначают идентификаторы другим объектам, в том числе другим регистрирующим организациям. Таким образом, обеспечивается расширяемость перечня зарегистрированных объектов.

Регистрирующая организация может использовать правила настоящего предстандарта для регистрации объектов, не связанных с безопасностью.

4.2 Идентификаторы объектов

Идентификаторы объектов определяются в соответствии с ГОСТ 34.973. Идентификатор представляет собой последовательность неотрицательных целых чисел. Сначала идет число первого уровня, затем второго и т.д. Числа разделяются пробелами. Вся последовательность окаймляется фигурными скобками. Например, {1 2 112} – идентификатор объекта, составленный из компонентов 1, 2, 112.

Числовым компонентам могут назначаться имена (идентификаторы АСН.1). При задании компонентов могут использоваться либо числа, либо совместно числа и имена, либо только имена:

```
{1 2 112},
{iso(1) member-body(2) belarus(112)},
{iso member-body belarus}.
```

Идентификаторы образуют иерархическую структуру: идентификатор $\{a_1 a_2 \dots a_{n+1}\}$ считается дочерним для $\{a_1 a_2 \dots a_n\}$, идентификатор $\{a_1 a_2 \dots a_n\}$ считается родительским для $\{a_1 a_2 \dots a_{n+1}\}$. Идентификаторы с начальными компонентами a_1, a_2, \dots, a_n считаются порожденными от $\{a_1 a_2 \dots a_n\}$.

Совокупность идентификаторов, порожденных от одного начального (корневого) идентификатора, задает дерево идентификаторов. Вершинами этого дерева являются сами идентификаторы, ребра соединяют родительские вершины с дочерними.

5 Дерево идентификаторов

Корневая вершина дерева идентификаторов определяется следующим образом:

```
{iso(1) member-body(2) belarus(112)}.
```

Корневой вершине назначается имя by:

```
by OBJECT IDENTIFIER ::= {iso(1) member-body(2) belarus(112)}.
```

Корневая вершина имеет две дочерние:

```
{by standard(0)},
{by registration-authority(1)}.
```

Вершина {by standard} определяет ветвь дерева, которая содержит идентификаторы объектов, определяемых в технических нормативных правовых актах.

Вершина {by registration-authority} определяет ветвь дерева, которая содержит идентификаторы регистрирующих организаций, а также объекты, зарегистрированные этими организациями.

Вершина {by standard} имеет четыре дочерние, соответствующие типам ТНПА:

```
{by standard tr(0)},
{by standard tkp(1)},
{by standard std(2)},
{by standard tu(3)}.
```

Вершина {by standard tr} определяет ветвь дерева, которая содержит идентификаторы объектов, определяемых в технических регламентах.

Вершина {by standard tkp} определяет ветвь дерева, которая содержит идентификаторы объектов, определяемых в технических кодексах установившейся практики.

Вершина {by standard std} определяет ветвь дерева, которая содержит идентификаторы объектов, определяемых в стандартах, в том числе государственных стандартах и стандартах организаций.

Вершина {by standard tu} определяет ветвь дерева, которая содержит идентификаторы объектов, определяемых в технических условиях.

Вершина {by standard std} имеет четыре дочерние, соответствующие типам стандартов:

```
{by standard std stb(0)},
```

{by standard std gost(1)},
 {by standard std ist(2)},
 {by standard std sto(3)}.

Вершина {by standard std stb} определяет ветвь дерева, которая содержит идентификаторы объектов, определяемых в государственных стандартах.

Вершина {by standard std gost} определяет ветвь дерева, которая содержит идентификаторы объектов, определяемых в межгосударственных (региональных) стандартах.

Вершина {by standard std ist} определяет ветвь дерева, которая содержит идентификаторы объектов, определяемых в международных стандартах.

Вершина {by standard std sto} определяет ветвь дерева, которая содержит идентификаторы объектов, определяемых в стандартах организаций.

Дерево идентификаторов может расширяться по правилам, описанным в разделе 6 настоящего предстандарта.

6 Регистрация

6.1 Методы регистрации

Регистрация объекта информационных технологий может выполняться тремя методами:

- назначением идентификатора в настоящем предстандарте;
- назначением идентификатора в другом ТНПА;
- назначением идентификатора определенной регистрирующей организацией.

Первый метод реализован включением в настоящий предстандарт приложений А – Е. В этих приложениях определены идентификаторы уполномоченных регистрирующих организаций, идентификаторы объектов ряда действующих криптографических стандартов, а также идентификаторы объектов Государственной системы управления открытыми ключами.

6.2 Назначение идентификаторов в ТНПА

Идентификаторы, назначаемые в ТНПА, должны состоять из двух частей: идентификатор ТНПА и идентификатор конкретного объекта в пределах действия ТНПА.

Идентификатор ТНПА должен определять тип и номер ТНПА. Идентификатор типа должен определяться в соответствии с разделом 5 настоящего предстандарта. Идентификатор номера определяется по регистрационному номеру ТНПА. В регистрационном номере выделяются целочисленные части, разделенные символами «.», «,», «/» и т.д. Последовательность данных целочисленных частей, за исключением даты введения или изменения ТНПА, образует идентификатор номера. При определении идентификатора номера дата введения или изменения ТНПА учитываться не должна.

Например, СТБ 1176.1 должен быть назначен идентификатор {by standard std stb 1176 1}, международному стандарту ИСО/МЭК 15946-2 – идентификатор {by standard std ist 15946 2}.

Идентификаторы объектов в пределах действия ТНПА могут назначаться произвольным образом, на усмотрение разработчика ТНПА.

Идентификаторы объектов ТНПА, определяющего криптографические алгоритмы и протоколы, рекомендуется вводить по следующей схеме (tnpa – идентификатор целевого ТНПА):

- в ветви {tnpa module(1)} регистрировать модули АСН.1 различных версий;
- в ветви {tnpa keys(2)} регистрировать ключи криптографических алгоритмов и протоколов;
- в ветви {tnpa params(3)} регистрировать стандартные параметры криптографических алгоритмов и протоколов;
- алгоритмам и протоколам назначать идентификаторы {tnpa n}, где $n \geq 11$.

При выпуске новых редакций ТНПА может пересматриваться перечень объектов, могут уточняться свойства объектов. Новым или измененным объектам должны назначаться новые идентификаторы.

6.3 Назначение идентификаторов регистрирующей организацией

Регистрирующая организация должна поддерживать регистр идентификаторов. Средства управления регистром могут быть произвольными, выбранными самой РО.

Регистрирующая организация должна выполнять следующие функции:

- 1) Обработка запросов на регистрацию объектов;
- 2) Назначение идентификаторов объектам и соответствующее изменение регистра;
- 3) Распространение копий регистра или представление информации из регистра.

При обработке запросов РО должна проверять, что:

- в запросе содержится достаточно информации для идентификации регистрируемого объекта;
- регистрация объекта находится в компетенции РО;
- указанный в запросе объект еще не зарегистрирован данной РО.

При нарушении указанных условий регистрация не должна выполняться.

СТБ П 34.101.XX-2011

Назначаемые идентификаторы должны быть подчинены идентификатору РО. Могут использоваться идентификаторы, указанные в запросе на регистрацию.

Для распространения регистра может использоваться электронная публикация, выпуск бумажных бюллетеней и др.

Перечень регистрирующих организаций может пополняться. Например, новая организация может быть зарегистрирована уже действующей или может быть расширено приложение А.

Приложение А
(рекомендуемое)
Идентификаторы регистрирующих организаций

Определены следующие регистрирующие организации:

- 1) Государственный комитет по стандартизации Республики Беларусь;
- 2) Министерство связи и информатизации Республики Беларусь;
- 3) Оперативно-аналитический центр при Президенте Республики Беларусь;
- 4) Национальный банк Республики Беларусь.

Данным организациям назначаются соответственно следующие идентификаторы:

```
{by registration-authority gosstandard(0)},  
{by registration-authority mpt(1)},  
{by registration-authority oac(2)},  
{by registration-authority nbrb(3)}.
```

Приложение Б
(рекомендуемое)
Идентификаторы объектов СТБ 1176.1

Б.1 Объекты

Алгоритму хэширования СТБ 1176.1 назначается идентификатор `stb11761-hash`. В алгоритме `stb11761-hash` долговременный параметр L , определенный в п. 5.1 СТБ 1176.1, должен равняться 256, а еще один долговременный параметр H , также определенный в п. 5.1 СТБ 1176.1, должен задаваться дополнительно.

При задании H (целое число) с помощью АСН.1 должен использоваться тип ОСТЕТ STRING. Первый октет значения этого типа должен совпадать с младшим октетом в двоичной записи H, \dots , последний октет значения – со старшим октетом двоичной записи.

При конкретных значениях H алгоритм `stb11761-hash` уточняется следующими 3 способами:

- `stb11761-hash0` алгоритм `stb11761-hash` с $H = 0$;
- `stb11761-hashA` алгоритм `stb11761-hash` с $H = AA\dots A$ (в шестнадцатеричной системе счисления);
- `stb11761-hash4E` алгоритм `stb11761-hash` с $H = 4E4E9C9C\ 9C9C4E4E\ 9C9C4E4E\ 4E4E9C9C\ 9C9C4E4E\ 4E4E9C9C\ 4E4E9C9C\ 9C9C4E4E$ (в шестнадцатеричной системе счисления).

Б.2 Модуль АСН.1

```
Stb11761-module-v1 {1 2 112 0 2 0 1176 1 module(1) ver1(1)}
```

```
DEFINITIONS ::=
```

```
BEGIN
```

```
  stb11761 OBJECT IDENTIFIER ::= {1 2 112 0 2 0 1176 1}
```

```
  stb11761-hash OBJECT IDENTIFIER ::= {stb11761 11}
```

```
  stb11761-hash0 OBJECT IDENTIFIER ::= {stb11761 12}
```

```
  stb11761-hashA OBJECT IDENTIFIER ::= {stb11761 13}
```

```
  stb11761-hash4E OBJECT IDENTIFIER ::= {stb11761 14}
```

```
END
```

Приложение В
(рекомендуемое)
Идентификаторы объектов СТБ 1176.2

В.1 Алгоритмы

Алгоритмам СТБ 1176.2 назначаются следующие идентификаторы:

stb11762-sign	алгоритмы выработки и проверки электронной цифровой подписи (далее – ЭЦП), определенные в пп. 5, 6 СТБ 1176.2;
stb11762pre-sign	алгоритмы выработки и проверки ЭЦП, определенные в пп. 5, 6 СТБ 1176.2, с предварительным хэшированием сообщений в соответствии с СТБ 34.101.31;
stb11762-genparam	алгоритм генерации долговременных параметров, определенный в п. 7 СТБ 1176.2.

Алгоритмы stb11762-sign применяются непосредственно к сообщению, ЭЦП которого вырабатывается или проверяется. В пп. 5.1.2, 6.1.2 СТБ 1176.2 данное сообщение определяется как последовательность $M = (m_1, m_2, \dots, m_z)$, где m_i – октеты.

В алгоритмах stb11762pre-sign выполняется предварительное хэширование сообщения с помощью алгоритма, определенного в СТБ 34.101.31. В качестве M используется полученное хэш-значение. При этом $z = 32$, m_1 является первым октетом хэш-значения, m_2 – вторым и т.д.

В.2 Открытые ключи

Открытым ключам СТБ 1176.2 назначаются следующие идентификаторы:

stb11762-pubkey	открытый ключ алгоритмов stb1176-sign;
stb11762pre-pubkey	открытый ключ алгоритмов stb1176pre-sign.

Ключи ЭЦП могут использоваться совместно с ключами протоколов формирования общего ключа, определенными в проекте руководящего документа Республики Беларусь «Банковские технологии. Протоколы формирования общего ключа» (далее – ПФОК, см. [1]). В связи с этим вводятся два дополнительных типа открытых ключей СТБ 1176.2:

stb11762-bdh-pubkey	составной открытый ключ алгоритмов stb1176-sign и ПФОК;
stb11762pre-bdh-pubkey	составной открытый ключ алгоритмов stb1176pre-sign и ПФОК.

Для составных ключей долговременные параметры СТБ 1176.2 и ПФОК должны выбираться так, чтобы был обеспечен заданный в таблице В.1 паритет между уровнем стойкости СТБ 1176.2 и порядком стойкости ПФОК.

Таблица В.1 – Паритет между уровнем стойкости СТБ 1176.2 и порядком стойкости ПФОК

Уровень СТБ 1176.2	Порядок ПФОК	Уровень СТБ 1176.2	Порядок ПФОК
1	10^{20}	6	10^{30}
2	10^{22}	7	10^{32}
3	10^{25}	8	10^{34}
4	10^{26}	9	10^{36}
5	10^{28}	10	10^{37}

При задании открытых ключей stb11762-pubkey, stb11762pre-pubkey с помощью АСН.1 должен использоваться тип

```
BDSPublicKeyValue ::= INTEGER
```

При задании открытых ключей stb11762-bdh-pubkey, stb11762pre-bdh-pubkey с помощью АСН.1 должен использоваться тип

```
BDSBDHPublicKeyValue ::= SEQUENCE {
    bdsPublicKey    INTEGER,
    bdhPublicKey    INTEGER
}
```

Компонент bdsPublicKey этого типа определяет значение открытого ключа СТБ 1176.2, а компонент bdhPublicKey – значение открытого ключа ПФОК.

При использовании открытых ключей в сертификатах или списках отозванных сертификатов СТБ 34.101.19 они должны представляться значениями следующего типа АСН.1:

```
SubjectPublicKeyInfo ::= SEQUENCE {
    algorithm        PublicKeyAlgorithmIdentifier,
    subjectPublicKey BIT STRING
}
```

Компонент `algorithm` этого типа описывает свойства открытого ключа. Компонент `subjectPublicKey` описывает значение открытого ключа. Открытый ключ задается значением типа `BDSPublicKeyValue` или `BDSBDHPublicKeyValue`, которое кодируется с помощью отличительных правил, определенных в приложении Б СТБ 34.101.19. Полученное кодовое представление сохраняется в `subjectPublicKey` как значение типа `BIT STRING`.

Для описания свойств открытого ключа используется тип

```
PublicKeyAlgorithmIdentifier ::= SEQUENCE {
  algorithmId      OBJECT IDENTIFIER,
  params           PublicKeyParameters
}
```

Компонент `algorithmId` этого типа описывает идентификатор открытого ключа. Компонент `params` описывает долговременные параметры алгоритмов, с которыми используется открытый ключ.

Тип `PublicKeyParameters` определяется следующим образом:

```
PublicKeyParameters ::= CHOICE {
  bdsParams      [0] EXPLICIT BDSParams,
  bdsbdhParams   [2] EXPLICIT BDSBDHParams
}
```

Компонент `bdsParams` этого типа описывает долговременные параметры СТБ 1176.2. Компонент `bdsbdhParams` описывает долговременные параметры СТБ 1176.2 и ПФОК. Компонент `bdsbdhParams` должен присутствовать только для открытых ключей `stb11762-bdh-pubkey`, `stb11762pre-bdh-pubkey`.

Типы `BDSParams`, `BDSBDHParams` определены ниже.

В.3 Долговременные параметры

В таблице В.2 определены стандартные долговременные параметры СТБ 1176.2, полученные с помощью алгоритма `stb11762-genparam`. Данным наборам назначаются идентификаторы

<code>bds-params3</code>	стандартные параметры СТБ 1176.2, соответствующие 3-му уровню стойкости;
<code>bds-params6</code>	стандартные параметры СТБ 1176.2, соответствующие 6-му уровню стойкости;
<code>bds-params10</code>	стандартные параметры СТБ 1176.2, соответствующие 10-му уровню стойкости.

В таблице В.3 определены стандартные параметры ПФОК, полученные с помощью алгоритма, определенного в п. 5 документа [1]. Данным наборам назначаются идентификаторы

<code>bdh-params3</code>	стандартные параметры ПФОК, соответствующие порядку стойкости 10^{25} ;
<code>bdh-params6</code>	стандартные параметры ПФОК, соответствующие порядку стойкости 10^{30} ;
<code>bdh-params10</code>	стандартные параметры ПФОК, соответствующие порядку стойкости 10^{37} .

Для описания свойств составных открытых ключей могут использоваться стандартные составные параметры СТБ 1176.2 и ПФОК, которым назначаются следующие идентификаторы

<code>stb1176-params3</code>	составные параметры <code>bds-param3</code> и <code>bdh-param3</code> ;
<code>stb1176-params6</code>	составные параметры <code>bds-param6</code> и <code>bdh-param6</code> ;
<code>stb1176-params10</code>	составные параметры <code>bds-param10</code> и <code>bdh-param10</code> .

Числа p , q , a , g в таблицах В.2, В.3 записаны в шестнадцатеричной системе счисления. Это значит, что число представляется строкой шестнадцатеричной цифр. Цифры читаются слева направо и сверху вниз. Первая цифра – старшая, последняя – младшая.

При генерации стандартных параметров использовались следующие инициализирующие значения датчика случайных чисел (см. п. 7.2.1 СТБ 1176.2 и п. 5.2.1 документа [1]):

$$z_1 = 1, z_2 = 2, \dots, z_{31} = 31.$$

На шаге 7.2.4.1 алгоритма генерации параметров СТБ 1176.1 числа d_i , r_i выбирались следующим образом:

$$d_0 = \left\lfloor \frac{l}{2} \right\rfloor + 1, \quad r_0 = \left\lfloor \frac{r}{2} \right\rfloor + 1, \quad d_i = \left\lfloor \frac{d_{i-1}}{2} \right\rfloor + 1, \quad r_i = \left\lfloor \frac{r_{i-1}}{2} \right\rfloor + 1, \quad i = 1, 2, \dots$$

На шаге 7.3.3.1 алгоритма генерации параметров СТБ 1176.1 число d выбиралось равным 5.

На шаге 5.2.4.1 алгоритма генерации параметров ПФОК числа l_i выбирались следующим образом:

$$l_0 = l - 1, \quad l_i = \left\lfloor \frac{l_{i-1}}{2} \right\rfloor + 1, \quad i = 1, 2, \dots$$

При задании долговременных параметров СТБ 1176.2 с помощью АСН.1 должен использоваться тип:

```

BDSParams ::= CHOICE {
    bdsParamsReference    OBJECT IDENTIFIER,
    bdsParamsList        BDSParamsList
}

```

Выбор компонента `bdsParamsList` означает явное задание параметров. Компонент `bdsParamsReference` используется для ссылки на зарегистрированные параметры, например, на параметры из таблицы В.2.

Явно задаваемые параметры должны представляться значениями типа:

```

BDSParamsList ::= SEQUENCE {
    bdsParameterL        [0] IMPLICIT INTEGER,
    bdsParameterR        [1] IMPLICIT INTEGER,
    bdsParameterP        [2] IMPLICIT INTEGER,
    bdsParameterQ        [3] IMPLICIT INTEGER,
    bdsParameterA        [4] IMPLICIT INTEGER,
    bdsParameterH        [5] IMPLICIT OCTET STRING,
    bdsParamsInitData    BDSParamsInitData OPTIONAL
}

```

Компонент `bdsParameterL` этого типа описывает параметр l , компонент `bdsParameterR` – параметр r , компонент `bdsParameterP` – параметр p , компонент `bdsParameterQ` – параметр q , компонент `bdsParameterA` – параметр a , компонент `bdsParameterH` – параметр H . Первый октет компонента `bdsParameterH` представляет собой младший октет большого числа, содержащего значение H , последний октет компонента `bdsParameterH` представляет собой старший октет двоичного представления большого числа, содержащего значение H .

Тип `BDSParamsInitData` описывает инициализирующие значения, использованные для генерации долговременных параметров СТБ 1176.2:

```

BDSParamsInitData ::= SEQUENCE {
    bdsPrmsInitZSequence OCTET STRING,
    bdsPrmsInitDSequence OCTET STRING,
    bdsPrmsInitRSequence OCTET STRING,
    bdsPrmsInitDValue    INTEGER
}

```

Компонент `bdsPrmsInitZSequence` этого типа описывает последовательность чисел z_1, \dots, z_{31} , компонент `bdsPrmsInitDSequence` – последовательность d_0, \dots, d_t , компонент `bdsPrmsInitRSequence` – последовательность r_0, \dots, r_s , компонент `bdsPrmsInitDValue` – параметр d .

Таблица В.1 – Стандартные долговременные параметры СТБ 1176.2

Уровень стойкости 3	
l	1022
r	175
p	2846B979 F51D4156 B881C96F 3C61A5F3 B5A8F4B4 7B604657 8B92205C A7ADCB9A 77CF7780 023B7217 1BB3BED1 569ECA57 2C5E423B 885C70F5 D2CD3C17 0E31CE50 7DE12C9E 535D71DA 16530C9B E6D078C4 67CE4D24 E7C63181 7FB4BE8F 16EB1B4D E7152DB1 8B23E9B8 99CDAAAB CF7BEC42 CBA90DE4 747EA228 BC267048 0EB191E5
q	7A3D 48C80B17 84985341 4EE450CC 636C93F5 1D63F3C5
a	0CA7F481 B9D2ABE2 E1CBC58F AB8B1FC9 D05234B0 B72AA69B 9A522E1C 18EB73FC CF86CBED 32BD11D0 41AE0434 0D9F732E 7D6A88D0 52BC2CEE 1F8F64CB 0893D92F 365D162E 67B04EEA D6F8FE7F 51B74CF6 1C90C9F4 53F35E56 8E2225F4 5C62BDF0 1E96E131 67CE3338 33B93F65 96332013 2112AADB E4D93404 7AFFB35 7D931983
H	0
Уровень стойкости 6	
l	1534
r	143
p	2E4BC383 5A5B41E3 5D9DC735 157891FC 868064AD 80086810 CB68F580 3DD79608 20A2BAAF 7588969A B9BF5187 3B1E393D 6DABA057 C219EDC6 8183B7EF 07C4C3CE D5466C41 A598A28B D0812BB7 F8AB721D CA6D6D09 AFB97604 4CE6D36C 5F4C1C58 6179EB2F B8F77415 70E8B492 44FD8E02 4398EBED 9B3DD66C 591FD864 83B9FA62 D66F3AFF 7F98ED22 61B15F45 5DEAB8D4 DDC3855D 6EBA0C8A 706F48AC A209ACE2 87AF3A81 CD0AF711 F82A1C65 3C5E5AAA 6BC05AA9 2591AC22 5BEBC6E5 5E953453
q	B7B5 417D8085 27DED8EA EC7CFCB9 742C871B DF45DA71 5F6A453D
a	017CA54B C1BD338D 2F760ACF 08D1124A 57FF866C 24F3DC85 19E03C44 210F4E08 D9950280 C0CC9FBD BA3916D4 18CF1999 B91E413C 402BC00D B8B6BA76 8C45257F 25E9F4D7 1CC78ED3 EF1201D0 12E6B9CE 24913F2F 57E38606 C84D8E18 1A420D54

СТБ П 34.101.XX-2011

	F1B1E2A1 987BED42 2079E48E 88A03E73 0C36055B 9C9A15D4 2BA8DCCB F810E193 A7653A9C 175A8185 FD73BB1C 17139B31 160B42CA EDF01F01 F799A0B6 1AF8FF8B DE3E2AC1 7145A727 FD7AE027 1BF97092 BF730F08 16C8F376 450A350E B7C78044
<i>H</i>	0
Уровень стойкости 10	
<i>l</i>	2462
<i>r</i>	257
<i>p</i>	2F01EACA 0363BB43 DA7CF0A2 14D2FC03 3A592B2F 2E3FB58D 61D7E42B AA17455B 38167684 BF8F418E 2DF4EFD3 E1D105E0 34A497CF C0FA4C02 39E755C1 3965D096 452B055A 5314C80F C7F63C81 014EEE3F A9C6FDFE 9A88A2E8 D1137ABE 01E6DD80 6D0A64A4 05B3F30D 909C84B6 008F9D06 D1102024 A7D2CF7F 5C041887 3BD222EF 2BE1BFAF 66CB3BBD 7E34AEDF 10C5A70E 1CAC0566 DBC96E05 8B5D0B9D 6875951B 0ADF8D09 BCE5CE60 FC1CBEC0 C49DE8A4 94568263 9E9CF549 93A62251 372DD0EE B3007644 5EFD9B15 5194FA32 54CF3DA6 D0EE8B0C 0F515DF1 949E8F8B 67E7DC1A 14433033 9BA0AEA1 E93C551A 3117CE98 AFD69473 2667E4CE 226779E3 4726E78E 13E916D8 916D2918 BDF5DD77 8C9938E2 F52E3425 714CA7C9 122330D9 2A2DF086 1516CCE3 51E6D76D 7537432A F1F2285F 6F9B1D95
<i>q</i>	01 C3CED546 6C41A582 9D099FA4 4491B119 3D1AB138 A1781046 73D152C1 4F804EEB
<i>a</i>	1E921804 B4E9624E 38CE41C7 79846D4D BB98D53D F634ED69 85FA42BF 079A7BD0 5AAC508F BFC47892 8F9EE2B2 2C2F1B97 D98F6147 7EDC2AAB 4AA32499 552FF72F F1B3AEF2 7F5231DA 1880A153 F1B283E2 2A386554 3B642C35 EFE211C5 046AAE39 6C2811B8 1DBED9C4 AFB1F39E D2F36799 1CC77980 51B99F0B 7FEE1AB4 E85CDBBD 853BCB1B A1902175 9E588CC7 0AF9888A 5C4EC7FF F330749C EA1890BC F722BAE9 37D2B366 3805DC67 F55A591B 6E288962 9D11CD03 C1555AC8 63827B88 A0451A47 26597359 E5902CAD 1EEAF794 EB600530 9988F333 95F42041 4BB0B218 75305E12 CCF177BE 765DF18E DDB7E9AA 37631867 94D3C446 38E1B11A B87C6957 F5C14787 D540959D 3ACB53D3 1BBB2482 3F5AC505 FAF5D86E 0EBA65AE CB14B4B0 0601CC24 26CC476D 8837CC6C 4FCE7B07 0E19ABEB 6DC34FEE
<i>H</i>	0

Таблица В.3 – Стандартные долговременные параметры ПФОК

Порядок стойкости 10 ²⁵	
<i>l</i>	1022
<i>r</i>	161
<i>p</i>	339617C5 38F666A4 80AF8C8C 8B509E78 4EE3E693 42B83E64 74669834 6E87E566 77FE1E5D 5E7E6A48 A69DCB27 51EBE9AB 7868C2E7 2B0510EE 4BC19B98 050C240E 94AB14A2 E8B7809C B62710D8 80AB0B4F 721683AB EC19D248 2CE567A6 BF04B627 650717C4 ECCBEA3F 7BBE822C EADE426E E067C74E ABC53F84 177655D7 31BE5E6F
<i>g</i>	322A3AD3 50DCFE8 690DBCA0 A2EED3D8 698711A3 0F10B53B 675880C4 18065E6C FF17541F 58824CD8 CD8CE48B C272E6F3 548349A4 34CEE725 AC9856B5 80465F39 C7E6FFC2 85EB7813 D47DE1C3 C3F02BE7 9A600C02 6A8141EA 7A7D0A64 2F80ECA6 D7CAB616 991445FA 03C63CEE A5FB882E E4CB61CD 9553FB5C 1B1A371D FB084D69
Порядок стойкости 10 ³⁰	
<i>l</i>	1534
<i>r</i>	194
<i>p</i>	397C1F50 6BA9F5A5 2D054BD4 8CDF3A50 D54ECA88 B56C5E1C 7878AA61 58E75594 BBBF6530 B14DE91F E1EB51AD CC02D266 CBE0AD2B 6B06929E E0005CF4 77E639AD A01D8224 46D28598 E07CF4A1 44970874 4557090D C377A574 BB388896 9FA8061A 8C3EFA6F 2E9A253A 79043CB4 CFEC74C DCC1BE1B 580F703B D985C822 0540952E FA197328 F894400F C7E08FFA 61461B49 F0B169A7 AAB8BF1B ACF27E35 7A3F2E42 2DF51764 F62E14B5 36BFCB42 35BFE134 A5AF660A 45B15F32 2DF469ED 7B1451C7
<i>g</i>	24E7A8B6 5E3E90EF 6BE3F4BD F98421B4 41DA4D0B B3CBA7CC 9AD0F766 EE7D6FFD 3C3A138F 7BC825AF C3A957B7 EE47C5C7 8B587DD8 1EBF5047 C17662D9 73D7A0CD D288AD56 1322E5D1 0825F9E1 AFB4D397 3AC51532 C798D70D 972B0906 33B100A3 4554C6B7 B76D201A 3A313E59 B0F9C6C8 F64B85A6 A04D53E2 18CEF699 EC01CC1B 6074E54E 64FD716A 8C78DF22 13A4FCCE E421C525 5E71D8A1 D834F994 7B5E9BE2 B4402CEE 3F543176 1D35DFD7 C2740F78 C5922EB7 48CE23BD 5AE7EB48 F34885B2
Порядок стойкости 10 ³⁷	
<i>l</i>	2462
<i>r</i>	240
<i>p</i>	20A8F485 EA81C26F AF8F13A0 AA206B38 D0C365EE 26C0AD12 A0DD8C08 230FED3A

	D80AB6A9 9B9292EC 694A599B 931F8F7F 4631ED9C 94EAF4B1 16105496 1C6942CF 2DE4F1DA 22F33DA1 EB7D2387 218D34E5 3D38052D F6D7A48E B772023B E5B1ADF0 B68BB6DF 5139267F 66ABD05B A358AE40 AF7433EE 1FF470C1 4E2711F2 DCF99F26 53F6B9B4 516FA3C1 3936A1D1 A8462E5F E163DD11 0C019B75 D9B2A3A6 FF5647E6 41504569 42648597 F429BF52 F8E95B08 379A3CD5 C4001356 A8E452EF 9ACDECC3 36204BDE 3A2FB563 8ED3B005 21FDA08F 0914BAFC F1417B39 F5E0C40D 2DAD92AE 73AE16E0 1CBF075E A9E6680B 68938436 37DE1FED 4DFEA458 27C8C633 3AFA29B8 23081AA6 8EDF3338 C64A7F92 A6086539 945E8C90 6AA603D8 1733E220 75BB823E 120CE8E1 FC74AE65 4799F956 9C152D29 654A80DB
g	038364E5 FAC23957 62450601 442E4B94 ED79F195 26E2B675 9A42AD96 848F8E82 6D413D73 613E8D10 0CE60AA5 D90241B9 7E342BC9 873D8823 110F547C 97575276 8D29A886 A9469E03 9135F249 C2B2180C 284C4E58 E526398D 67BBBA9F 1396F584 4F5552D4 AB822271 486C6A04 1ECD4169 E33FD26C 5AC8DBB5 DDB3E62B 1FAEB900 873B92C0 C29A7C9A 95276FCC 8C8F11F1 4C173894 0AEF9667 7BD9C709 3A1BB08A 58C4DDB6 FC6AB465 1620BA32 96707E7C AA6DCF0A B5F7049F 54EB2E67 016A03F4 74F87AA9 48D6087A 94D55557 3853B7FB C4679C19 945E30E2 8464DDD9 3B32967C 6D446EF4 446387BF AE13CE80 9BA68838 335C96A6 4EF466D9 0F19D5DA 51B8AF3B 10C66A5F D7A0406D 7451A950 D7BF9697 FDFDF4F9 9798E0D7 904ABC39 2A25B52E 30E6F804 DE2C1274 7B32F32E 04CD277C 4996E114

Первая пара октетов `bdsPrmsInitZSequence` должна представлять z_1 , вторая пара – z_2 и т.д. При этом первый октет пары должен представлять младший октет двоичной записи z_i , второй октет пары – старший октет двоичной записи z_i . Данные соглашения об описании последовательностей распространяются также на компоненты `bdsPrmsInitDSequence` и `bdsPrmsInitRSequence`.

При задании долговременных параметров ПФОК с помощью АСН.1 должен использоваться тип:

```
BDHParamsList ::= SEQUENCE {
    bdhParameterL          [0] IMPLICIT INTEGER,
    bdhParameterR          [1] IMPLICIT INTEGER,
    bdhParameterP          [2] IMPLICIT INTEGER,
    bdhParameterG          [3] IMPLICIT INTEGER,
    bdhParameterN          [4] IMPLICIT INTEGER,
    bdhParamsInitData      BDHParamsInitData OPTIONAL
}
```

Компонент `bdhParameterL` этого типа описывает параметр l , компонент `bdhParameterR` – параметр r , компонент `bdhParameterP` – параметр p , компонент `bdhParameterQ` – параметр g , компонент `bdhParameterN` – параметр n .

Тип `BDHParamsInitData` описывает инициализирующие значения, использованные для генерации долговременных параметров ПФОК:

```
BDHParamsInitData ::= SEQUENCE {
    bdhPrmsInitZSequence  OCTET STRING,
    bdhPrmsInitLSequence  OCTET STRING
}
```

Компонент `bdhPrmsInitZSequence` этого типа описывает последовательность чисел z_1, \dots, z_{31} , компонент `bdhPrmsInitDSequence` – последовательность l_0, \dots, l_t . Соглашения об описании последовательностей, заданные при описании типа `BDHParamsInitData`, распространяются на компоненты `bdhPrmsInitZSequence` и `bdhPrmsInitLSequence`.

Тип `BDSBDHParams` описывает значения долговременных параметров СТБ 1176.2 и ПФОК:

```
BDSBDHParams ::= CHOICE {
    bdsbdhParamsReference OBJECT IDENTIFIER,
    bdsbdhParamsList      BDSBDHParamsList
}
```

Выбор компонента `bdsbdhParamsList` означает явное задание параметров. Компонент `bdsbdhParamsReference` используется для ссылки на зарегистрированные параметры, например, на параметры из таблиц В.2, В.3.

Тип `BDSBDHParamsList` определяется следующим образом

```
BDSBDHParamsList ::= SEQUENCE {
    bdsParamsList BDSParamsList,
    bdhParamsList BDHParamsList
}
```

В.4 Протоколы

Составные ключи СТБ 1176.2 и ПФОК могут использоваться в следующих протоколах:

СТБ П 34.101.ХХ-2011

bdh-noauth	протокол без аутентификации сторон, определенный в п. 4.1 документа [1];
bdh-auth	протокол с аутентификацией сторон, определенный в п. 4.2 документа [1];
bdh-oneside	протокол одностороннего формирования ключа, определенный в п. 4.3 документа [1];
bdh-keytransport	протокол транспорта ключа, основанный на протоколе bdh-oneside.

В протоколе bdh-keytransport сторона *A* передает стороне *B* секретный ключ *X*, представляющий собой строку октетов, длина которой кратна 8. Сторона *A* действует следующим образом:

- вырабатывает по протоколу bdh-oneside общий со стороной *B* ключ K_{AB} из 32 октетов;
- выполняет зашифрование *X* на K_{AB} в режиме простой замены ГОСТ 28147 (см. приложение Г, алгоритм gost28147-ecb);
- вычисляет имитовставку *X* на K_{AB} в соответствии с ГОСТ 28147 (см. приложение Г, алгоритм gost28147-mac). Должна вычисляться имитовставка из 4 октетов (32 битов);
- пересылает стороне *B* сообщение (v_A, Y, T) , где v_A – посылка протокола bdh-oneside, *Y* – результат зашифрования *X*, *T* – имитовставка.

Сторона *B* обрабатывает полученное сообщение следующим образом:

- вырабатывает по протоколу bdh-oneside общий со стороной *A* ключ K_{AB} ;
- выполняет расшифрование *Y* на K_{AB} и определяет *X*;
- вычисляет имитовставку *X* на K_{AB} ;
- если полученная имитовставка совпадает с *T*, то принимает *X*.

Для описания параметров протокола bdh-keytransport с помощью АСН.1 должен использоваться

тип

```
BDHKeytransParams ::= SEQUENCE {
    va          INTEGER,
    mac         OCTET STRING (SIZE(4))
    sblock     OBJECT IDENTIFIER OPTIONAL
}
```

Компонент *va* этого типа описывает посылку v_A , Компонент *mac* описывает имитовставку *T*. Компонент *sblock* определяет идентификатор блока подстановки ГОСТ 28147, который используется для шифрования и имитозащиты. Если компонент *sblock* отсутствует, то должен использоваться стандартный блок gost28147-sblock-1, определенный в приложении Г.

Зашифрованный ключ *Y* должен описываться типом

```
BDHKeytransEncryptedKey ::= OCTET STRING
```

В.5 Модуль АСН.1

```
Stb11762-module-v1 {1 2 112 0 2 0 1176 2 module(1) ver1(1)}
```

```
DEFINITIONS ::=
```

```
BEGIN
```

```
stb11762 OBJECT IDENTIFIER ::= {1 2 112 0 2 0 1176 2}
```

```
stb11762-sign OBJECT IDENTIFIER ::= {stb11762 11}
```

```
stb11762pre-sign OBJECT IDENTIFIER ::= {stb11762 12}
```

```
stb11762-genparam OBJECT IDENTIFIER ::= {stb11762 21}
```

```
bdh-noauth OBJECT IDENTIFIER ::= {stb11762 31}
```

```
bdh-auth OBJECT IDENTIFIER ::= {stb11762 32}
```

```
bdh-oneside OBJECT IDENTIFIER ::= {stb11762 33}
```

```
bdh-keytrans OBJECT IDENTIFIER ::= {stb11762 34}
```

```
stb11762-keys OBJECT IDENTIFIER ::= {stb11762 keys(2)}
```

```
stb11762-pubkey OBJECT IDENTIFIER ::= {stb11762-keys 1}
```

```
stb11762pre-pubkey OBJECT IDENTIFIER ::= {stb11762-keys 2}
```

```
stb11762-bdh-pubkey OBJECT IDENTIFIER ::= {stb11762-keys 3}
```

```
stb11762pre-bdh-pubkey OBJECT IDENTIFIER ::= {stb11762-keys 4}
```

```
stb11762-params OBJECT IDENTIFIER ::= {stb11762 params(3)}
```

```
stb11762-params3 OBJECT IDENTIFIER ::= {stb11762-params 3}
```

```
stb11762-params6 OBJECT IDENTIFIER ::= {stb11762-params 6}
```

```
stb11762-params10 OBJECT IDENTIFIER ::= {stb11762-params 10}
```

```

bds-params3 OBJECT IDENTIFIER ::= {stb11762-params3 1}
bds-params6 OBJECT IDENTIFIER ::= {stb11762-params6 1}
bds-params10 OBJECT IDENTIFIER ::= {stb11762-params10 1}

```

```

bdh-params3 OBJECT IDENTIFIER ::= { stb11762-params3 2}
bdh-params6 OBJECT IDENTIFIER ::= { stb11762-params6 2}
bdh-params10 OBJECT IDENTIFIER ::= { stb11762-params10 2}

```

```

BDSParamsList ::= SEQUENCE {
    bdsParameterL [0] IMPLICIT INTEGER,
    bdsParameterR [1] IMPLICIT INTEGER,
    bdsParameterP [2] IMPLICIT INTEGER,
    bdsParameterQ [3] IMPLICIT INTEGER,
    bdsParameterA [4] IMPLICIT INTEGER,
    bdsParameterH [5] IMPLICIT OCTET STRING,
    bdsParamInitData BDSParamsInitData OPTIONAL
}

```

```

BDSParamsInitData ::= SEQUENCE {
    bdsPrmsInitZSequence OCTET STRING,
    bdsPrmsInitDSequence OCTET STRING,
    bdsPrmsInitRSequence OCTET STRING,
    bdsPrmsInitDValue INTEGER
}

```

```

BDHParamsList ::= SEQUENCE {
    bdhParameterL [0] IMPLICIT INTEGER,
    bdhParameterR [1] IMPLICIT INTEGER,
    bdhParameterP [2] IMPLICIT INTEGER,
    bdhParameterG [3] IMPLICIT INTEGER,
    bdhParameterN [4] IMPLICIT INTEGER,
    bdhParamsInitData BDHParamsInitData OPTIONAL
}

```

```

BDHParamsInitData ::= SEQUENCE {
    bdhPrmsInitZSequence OCTET STRING,
    bdhPrmsInitLSequence OCTET STRING
}

```

```

BDSBDHParamsList ::= SEQUENCE {
    bdsParamsList BDSParamsList,
    bdhParamsList BDHParamsList
}

```

```

BDSParams ::= CHOICE {
    bdsParamsReference OBJECT IDENTIFIER,
    bdsParamsList BDSParamsList
}

```

```

BDSBDHParams ::= CHOICE {
    bdsbdhParamsReference OBJECT IDENTIFIER,
    bdsbdhParamsList BDSBDHParamsList
}

```

```

PublicKeyParameters ::= CHOICE {
    bdsParams [0] EXPLICIT BDSParams,
    bdhParams [2] EXPLICIT BDSBDHParams
}

```

```

BDSPublicKeyValue ::= INTEGER

```

```

BDSBDHPublicKeyValue ::= SEQUENCE {
    bdsPublicKey INTEGER,

```

СТБ П 34.101.XX-2011

```
    bdhPublicKey  INTEGER
  }

BDHKeytransParams ::= SEQUENCE {
    va            INTEGER,
    mac          OCTET STRING (SIZE(4)),
    sblock       OBJECT IDENTIFIER OPTIONAL
}

BDHKeytransEncryptedKey ::= OCTET STRING
END
```

Приложение Г
(рекомендуемое)
Идентификаторы объектов ГОСТ 28147

Г.1 Объекты

Алгоритмам ГОСТ 28147 назначаются следующие идентификаторы:

<code>gost28147-ecb</code>	алгоритмы шифрования в режиме простой замены, определенные в п. 2 ГОСТ 28147;
<code>gost28147-cfb</code>	алгоритмы шифрования в режиме гаммирования с обратной связью, определенные в п. 3 ГОСТ 28147;
<code>gost28147-ctr</code>	алгоритмы шифрования в режиме гаммирования, определенные в п. 4 ГОСТ 28147;
<code>gost28147-mac</code>	алгоритм выработки имитовставки, определенный в п. 5 ГОСТ 28147.

Долговременным параметром алгоритмов является блок подстановки (см. п. 1.2 ГОСТ 28147). В таблице Г.1 определен стандартный блок подстановки. Этому блоку назначается идентификатор `gost28147-sblock-1`.

Блок подстановки состоит из 8 узлов замены K_1, K_2, \dots, K_8 . Каждый узел представляет собой массив из 16 тетрад (4-битовых векторов). Элементы массива индексируются в таблице Г.1 тетрадами. Тетрады представляются целыми числами от 0 до 15 так, что число 0 соответствует тетраде 0000, число 1 – тетраде 0001, ..., число 15 – тетраде 1111.

Таблица Г.1 – Стандартный блок подстановки ГОСТ 28147

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$K_1[i]$	2	6	3	14	12	15	7	5	11	13	8	9	10	0	4	1
$K_2[i]$	8	12	9	6	10	7	13	1	3	11	14	15	2	4	0	5
$K_3[i]$	1	5	4	13	3	8	0	14	12	6	7	2	9	15	11	10
$K_4[i]$	4	0	5	10	2	11	1	9	15	3	6	7	14	12	8	13
$K_5[i]$	7	9	6	11	15	10	8	12	4	14	1	0	5	3	13	2
$K_6[i]$	14	8	15	2	6	3	9	13	5	7	0	1	4	10	12	11
$K_7[i]$	9	13	8	5	11	4	12	2	0	10	15	14	1	7	3	6
$K_8[i]$	11	15	10	8	1	14	3	6	9	0	4	5	13	2	7	12

Если блок подстановки описывается с помощью АСН.1, то для описания должен использоваться тип `SBlockTable ::= OCTET STRING (SIZE(64))`

Первый октет значения этого типа должен содержать тетрады $K_1[0]$ (старшая) и $K_1[1]$ (младшая), второй октет – тетрады $K_1[2]$ (старшая) и $K_1[3]$ (младшая), ..., восьмой октет – тетрады $K_1[14]$ и $K_1[15]$, девятый октет – тетрады $K_2[0]$ и $K_2[1]$ и т. д.

Если синхропосылка в алгоритмах `gost28147-cfb`, `gost28147-ctr` описывается с помощью АСН.1, то для описания должен использоваться тип

`IV ::= OCTET STRING (SIZE(8))`

Если параметры алгоритмов ГОСТ 28147 описываются с помощью АСН.1, то для описания должен использоваться тип

```
GOSTParams ::= SEQUENCE {
  iv IV OPTIONAL,
  sblock SBlock OPTIONAL
}
```

Компонент `iv` этого типа определяет используемую синхропосылку. Компонент `iv` должен указываться только при описании параметров алгоритмов `gost28147-cfb` и `gost28147-ctr`. Компонент `sblock` определяет используемый блок подстановки. Если компонент `sblock` отсутствует, то используется стандартный блок подстановки `gost28147-sblock-1`.

Тип `SBlock` определяется следующим образом:

```
SBlock ::= CHOICE {
  table SBlockTable,
  oid OBJECT IDENTIFIER
}
```

Компонент `table` этого типа задает таблицу блока, а компонент `oid` – идентификатор блока.

Г.2 Модуль АСН.1

```
Gost28147-module-v1 {1 2 112 0 2 1 28147 module(1) ver1(1)}
DEFINITIONS ::=
BEGIN
```

СТБ П 34.101.XX-2011

```
gost28147 OBJECT IDENTIFIER ::= {1 2 112 0 2 1 28147}

gost28147-ecb OBJECT IDENTIFIER ::= {gost28147 11}
gost28147-cfb OBJECT IDENTIFIER ::= {gost28147 12}
gost28147-ctr OBJECT IDENTIFIER ::= {gost28147 13}
gost28147-mac OBJECT IDENTIFIER ::= {gost28147 14}

gost28147-sblock-1 OBJECT IDENTIFIER ::= {gost28147 params(3) 1}

SBlockTable ::= OCTET STRING (SIZE(64))

SBlock ::= CHOICE {
    table SBlockTable,
    oid OBJECT IDENTIFIER
}

IV ::= OCTET STRING (SIZE(8))

GOSTParams ::= SEQUENCE {
    iv IV OPTIONAL,
    sblock SBlock OPTIONAL
}
END
```

Приложение Д (рекомендуемое)

Идентификаторы объектов Государственной системы управления открытыми ключами

Регистрация объектов информационных технологий Государственной системы управления открытыми ключами Республики Беларусь (далее – ГосСУОК) осуществляется Национальным банком Республики Беларусь.

Объектам ГосСУОК назначаются идентификаторы, подчиненные идентификатору:

```
pki-gov OBJECT IDENTIFIER ::= {by registration-authority nbrb(3) 1}
```

Объекты ГосСУОК, подлежащие регистрации, – это дополнения сертификатов СТБ 34.101.19 и другие атрибуты, применяемых в ГосСУОК (ext). Им назначаются следующие идентификаторы:

```
ext OBJECT IDENTIFIER ::= {pki-gov 1}
name OBJECT IDENTIFIER ::= {pki-gov 1 1}
app OBJECT IDENTIFIER ::= {pki-gov 1 2}
```

Идентификатор `name` определяет дополнения и атрибуты сертификатов открытых ключей, связанные с идентификацией (именованием) субъектов инфраструктуры открытых ключей ГосСУОК.

Идентификатор `app` определяет прикладные дополнения сертификатов открытых ключей инфраструктуры открытых ключей ГосСУОК.

Объектам, относящимся к вершине `name` назначаются идентификаторы:

```
priv-num OBJECT IDENTIFIER ::= {pki-gov 1 1 1}
tax-id OBJECT IDENTIFIER ::= {pki-gov 1 1 2}
```

Идентификатор `priv-num` определяет личный номер (данные из документа, удостоверяющего личность: паспорта, вида на жительство и т.д.) субъекта инфраструктуры открытых ключей ГосСУОК, являющегося физическим лицом.

Идентификатор `tax-id` определяет уникальный номер налогоплательщика (УНП) субъекта инфраструктуры открытых ключей ГосСУОК, являющегося юридическим лицом (организацией).

Объектам, относящимся к вершине `app` назначается идентификатор

```
pk-card OBJECT IDENTIFIER ::= {pki-gov 1 2 1},
```

определяющий формат бланка карточки открытого ключа субъекта инфраструктуры открытых ключей ГосСУОК.

Объектам, относящимся к типам применяемых в ГосСУОК бланкам карточек открытого ключа назначаются идентификаторы:

```
root-ca OBJECT IDENTIFIER ::= {pki-gov 1 2 1 1}
sub-ca OBJECT IDENTIFIER ::= {pki-gov 1 2 1 2}
ra OBJECT IDENTIFIER ::= {pki-gov 1 2 1 3}
org OBJECT IDENTIFIER ::= {pki-gov 1 2 1 4}
person OBJECT IDENTIFIER ::= {pki-gov 1 2 1 5}
```

Идентификатор `root-ca` определяет бланк карточки открытого ключа корневого удостоверяющего центра инфраструктуры открытых ключей ГосСУОК.

Идентификатор `sub-ca` определяет бланк карточки открытого ключа подчиненного удостоверяющего центра инфраструктуры открытых ключей ГосСУОК.

Идентификатор `ra` определяет бланк карточки открытого ключа регистрационного центра инфраструктуры открытых ключей ГосСУОК.

Идентификатор `org` определяет бланк карточки открытого ключа юридического лица (организации) – пользователя инфраструктуры открытых ключей ГосСУОК.

Идентификатор `person` определяет бланк карточки открытого ключа физического лица – пользователя инфраструктуры открытых ключей ГосСУОК.

Библиография

- [1] Проект руководящего документа Республики Беларусь «Банковские технологии. Протоколы формирования общего ключа»
Мн.: Национальный банк Республики Беларусь, 1997.
- [2] Руководящий документ Республики Беларусь 07040/1206-2004 «Банковские технологии. Формат сертификатов открытых ключей и списков отзыванных сертификатов»
Мн.: Национальный банк Республики Беларусь, 2004.

Директор ЗАО «АВЕСТ»руководитель (заместитель руководителя) организации-разработчика,
наименование организации

личная подпись

А.Н. Скобов

расшифровка подписи

**Начальник отдела разработки программных
средств защиты информации ЗАО «АВЕСТ»**

руководитель подразделения организации-разработчика

личная подпись

Д.В. Шпилевский

расшифровка подписи

**Начальник группы контроля качества
ЗАО «АВЕСТ»**

руководитель разработки (темы), должность

личная подпись

С.В. Степченко

расшифровка подписи

СОГЛАСОВАНО:**От Национального банка Республики
Беларусь**

должность

личная подпись

расшифровка подписи

должность

личная подпись

расшифровка подписи

должность

личная подпись

расшифровка подписи

должность

личная подпись

расшифровка подписи

**От Оперативно-аналитического центра при
Президенте Республики Беларусь**

должность

личная подпись

расшифровка подписи

должность

личная подпись

расшифровка подписи

должность

личная подпись

расшифровка подписи

должность

личная подпись

расшифровка подписи