ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ
(РОССТАНДАРТ)

Технический комитет 026

«Криптографическая защита информации»

СИСТЕМЫ ОБРАБОТКИ ИНФОРМАЦИИ

ЗАЩИТА КРИПТОГРАФИЧЕСКАЯ

ТЕХНИЧЕСКАЯ СПЕЦИФИКАЦИЯ

ПО ИСПОЛЬЗОВАНИЮ ГОСТ Р 34.11-94 ПРИ ОБЕСПЕЧЕНИИ ЦЕЛОСТНОСТИ В ПРОТОКЛАХ IPSEC AH И ESP

(проект)

Москва
2013

Содержание

1 Введение

В архитектуре IPsec (**RFC4301**) для защиты конечных IP-пакетов используются протоколы AH (**RFC4302**) и ESP (**RFC4303**). Протокол AH используется для обеспечения целостности и аутентичности IP-пакетов (включая заголовок IP-пакета). Протокол ESP используется для обеспечения конфиденциальности (опционально), целостности и аутентичности содержимого IP пакетов. В данном документе определяются следующие преобразования с алгоритмами обеспечения целостности для AH и ESP:

— преобразование AH_GOST-HMAC-4M с алгоритмом GOST-HMAC-4M;

— преобразование AH_GOST-HMAC-1K с алгоритмом GOST-HMAC-1K;

AH-заголовки и ESP-вложения обрабатываются в рамках IPsec SA, параметры которой МОГУТ быть интерпретированы согласно положениям, содержащимися в документе **RFC2407**. В данном документе описываются дополнительные расширяющие идентификаторы этих параметров. Этот документ описывает использование ГОСТ Р 34.11-94 в AH и ESP, но не определяет сами алгоритмы и форматы представления криптографических типов данных. Алгоритмы описываются соответствующими национальными стандартами, а представление данных и параметров соответствует документам **RFC4357**, **RFC4490**, **RFC4491** и **CPIKE (проект)**.

Необходимость разработки данного документа была вызвана потребностью в обеспечении совместимости реализаций протоколов IPsec российских производителей.

2 Нормативные ссылки

Указанные в этом разделе рекомендаций ссылочные документы являются обязательными для их применения. Для датированных ссылок используют только указанное здесь издание. Для недатированных ссылок последнее и актуальное издание со всеми изменениями и дополнениями:

ГОСТ 28147-89 — Государственный комитет СССР по стандартам, «Защита криптографическая. Алгоритм криптографического преобразования», Государственный стандарт СССР, ГОСТ 28147-89, 1989.

ГОСТ Р 34.11-94 — Государственный комитет Российской Федерации по стандартам, «Информационные технологии. Криптографическая защита информации. Функция хэширования», ГОСТ Р 34.11-94, Государственный стандарт Российской Федерации, 1994.

ГОСТ 34.311-95 — Межгосударственный совет по стандартизации, метрологии и сертификации Содружества Независимых Государств (EASC), «Информационная технология. Криптографическая защита информации. Функция хэширования (на русском языке)», ГОСТ 34.311-95, Минск, 1995.

ГОСТ Р ИСО/МЭК 7498-1-99 — Государственный комитет Российской Федерации по стандартам, «Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель», (Information technology. Open systems interconnection. Basic reference model. Part 1. The basic model), ИПК Издательство стандартов, 1999.

CPIKE (проект) — Федеральное агентство по техническому регулированию и метрологии (РОССТАНДАРТ), «Системы обработки информации. Защита криптографическая. Техническая спецификация по использованию ГОСТ 28147-89, ГОСТ Р 34.11-94 и ГОСТ Р 34.10-2001 в протоколах обмена ключами IKE и ISAKMP», 2013.

CPESP (проект) — Федеральное агентство по техническому регулированию и метрологии (РОССТАНДАРТ), «Системы обработки информации. Защита криптографическая. Техническая спецификация по использованию комбинированного алгоритма шифрования вложений IPsec ESP на основе ГОСТ 28147-89», 2013.

2.1 Дополнительные ссылки

RFC2119 — С. Браднер, «Ключевые слова для использования в документах RFC, указывающие уровень требований», стандарт BCP 14, март 1997 г. (Bradner S., Key words for use in RFCs to Indicate Requirement Levels, BCP 14, IETF RFC 2119, March 1997).

RFC2407 — Д. Пайпер, «Область интерпретации IPsec для ISAKMP» (Piper D., The Internet IP Security Domain of Interpretation for ISAKMP, IETF RFC 2407, November 1998).

RFC2408 — Д. Шнейдер, М. Шертлер, «Протокол управления ключами и группами параметров сетевой безопасности (ISAKMP)» (Maughan D., Schneider M. and M. Schertler, Internet Security Association and Key Management Protocol (ISAKMP), IETF RFC 2408, November 1998).

RFC4301 — С. Кент, К. Сео, «Архитектура безопасности для протокола IP» (Kent S. and K. Seo, Security Architecture for the Internet Protocol, IETF RFC 4301, December 2005).

RFC4302 — С. Кент, «Аутентификационный заголовок IP» (Kent, S., IP Authentication Header, IETF RFC 4302, December 2005).

RFC4303 — С. Кент, «Инкапсуляция защищенных данных IP (ESP)» (Kent S., IP Encapsulating Security Payload (ESP), IETF RFC 4303, December 2005).

RFC4304 — С. Кент, «Добавление расширенных порядковых номеров (ESN) в области интерпретации IPsec (DOI) для протокола управления защитными связями и ключами (ISAKMP)» (Kent, S., Extended Sequence Number (ESN) Addendum to IPsec Domain of Interpretation (DOI) for Internet Security Association and Key Management Protocol (ISAKMP), IETF RFC 4304, December 2005).

RFC4357 — В. Попов, И. Курепкин, С. Леонтьев, «Дополнительные алгоритмы шифрования для использования с алгоритмами по ГОСТ 28147-89, ГОСТ Р 34.10-94, ГОСТ Р 34.10-2001 и ГОСТ Р 34.11-94» (Popov V., Kurepkin I. and S. Leontiev, 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, IETF RFC 4357, January 2006).

RFC4490 — С. Леонтьев, Г. Чудов, «Методические рекомендации по использованию алгоритмов ГОСТ 28147-89, ГОСТ Р 34.11-94, ГОСТ Р 34.10-94 и ГОСТ Р 34.10-2001 с синтаксисом криптографических сообщений (CMS)» (S. Leontiev, G. Chudov, 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), IETF RFC 4490, May 2006).

2.2 Информативные ссылки

ПП РФ №313 — Постановление Правительства Российской Федерации от 16 преля 2012 г. № 313 «Положение о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)».

99-ФЗ — Федеральный закон от 04.05.2011 N 99-ФЗ (ред. от 28.07.2012) «О лицензировании отдельных видов деятельности».

RFC2409 — Д. Харкинс, Д. Каррел, «Протокол согласования ключей (IKE)» (Harkins, D. and D. Carrel, The Internet Key Exchange (IKE), IETF RFC 2409, November 1998).

RFC2675 — Д. Борман, С. Диринг, Р. Хинден, «Слонограммы IPv6» (Borman, D., Deering, S., and R. Hinden, IPv6 Jumbograms, IETF RFC 2675, August 1999).

RFC4491 — С. Леонтьев, Д. Шефановский, «Методические рекомендации по использованию алгоритмов ГОСТ Р 34.10-2001 и ГОСТ Р 34.11-94 в профиле сертификата и списка отзыва сертификатов инфраструктуры открытых ключей X.509 Интернет» (S. Leontiev, D. Shefanovski, Using the GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms with the Internet X.509 Public Key Infrastructure Certificate and CRL Profile, IETF RFC 4491, May 2006).

RFC5831 — В. Долматов, «ГОСТ Р 34.11-94: алгоритм хэш-функции» (Dolmatov, V., GOST R 34.11-94: Hash Function Algorithm, IETF RFC 5831, March 2010).

RFC6071 — С. Френкель, С. Кришнан, «Дорожная карта для протоколов IP Security (IPsec) и Internet Key Exchange (IKE) в документах» Frankel, S. and S. Krishnan, IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap, IETF RFC 6071, February 2011.

Примечание: При пользовании данным документом целесообразно проверить действие ссылочных стандартов и классификаторов в информационной системе общего пользования - на официальном сайте национального органа Российской Федерации по стандартизации в сети Интернет или по ежегодно издаваемому информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по соответствующим ежемесячно издаваемым информационным указателям, опубликованным в текущем году. Если ссылочный документ заменен (изменен), то при пользовании данным документом следует руководствоваться замененным (измененным) документом. Если ссылочный документ отменен без замены, то положение, в котором дана ссылка на него, применяется в части, не затрагивающей эту ссылку.

3 Термины и определения

В документе используются термины и определения стандартов IPsec (**RFC4301**), ESP (**RFC4303**) и AH (**RFC4302**), ниже приводятся только дополнительные определения.

3.1 Терминология требований

Термины "ДОЛЖНО", "ДОЛЖНА", "ДОЛЖНЫ", "ДОЛЖЕН" (MUST, REQUIRED, SHALL), "НЕ ДОЛЖЕН", "НЕ ДОЛЖНЫ" (MUST NOT, SHALL NOT), "РЕКОМЕНДУЕТСЯ" (SHOULD, RECOMMENDED), "НЕ РЕКОМЕНДУЕТСЯ" (SHOULD NOT, NOT RECOMMENDED), "МОГУТ", "МОЖЕТ" (MAY, OPTIONAL) в рамках этого документа ДОЛЖНЫ интерпретироваться в соответствии с положениями документа **RFC2119**

3.2 Определения

В данном документе определены следующие термины:

искажённый пакет:	ESP-вложение или AH-пакет для которого вычисленное значение ICVchk не совпало со значением ICV в пакете;
сопоставление безопасности (Security Association, SA):	совокупность атрибутов безопасности и ключевой информации, ассоциируемая с безопасным соединением, представляющим собой виртуальный однонаправленный канал для передачи данных;
пакет с искажённым Seq#:	ESP-вложение или AH-пакет, для которого не прошёл предварительный контроль SPI и *Seq#*.

3.3 Условные обозначения

В данном документе используются следующие обозначения:

Divers (K, D):	алгоритм диверсификации ключа *K* по данным диверсификации *D* (раздел 7 **RFC4357**, узел замены определяется в разделе 6 **RFC4357**, в рамках данного документа в качестве данных диверсификации передаётся последовательность 8 байт, содержащая 64-битное целое число в сетевом порядке байт);
HMAC_GOSTR3411 (K, text):	выработка HMAC ГОСТ Р 34.11-94 на ключе *K* от данных *text* с внутренним выравниванием по ГОСТ Р 34.11-94 (раздел 3 **RFC4357**);
Ki_i (Seq#):	ключ имитозащиты пакета Seq#;
Kr_i:	корневой ключ имитозащиты SA;
Seq#:	64-битный номер пакета (если ESN из **RFC4304** не согласован, то значение *Seq#* всегда принадлежит диапазону 1..2^32-1;

Seq#h:	старшая часть *Seq#*;
Seq#l:	младшая часть *Seq#*;
substr (s..f, bytes):	последовательность байт с байта *s*, по байт *f*, выбранная из последовательности *bytes* представленной в сетевом порядке байт.

3.4 Аббревиатуры и сокращения

В тексте данного документа используются следующие сокращения и аббревиатуры:

ESN	расширенный номер пакета (Extended Sequence Number, **RFC4304**)
ISAKMP	протокол управления ключами и группами атрибутов сетевой безопасности (Internet Security Association and Key Management Protocol);
MTU	максимальный размер данных, который может быть единовременно передан на канальном уровне сетевой модели OSI, в соответствии с ГОСТ Р ИСО/МЭК 7498-1-99 (Maximum Transmission Unit);

4 Состав сопоставления безопасности AH и ESP SA

Протокол ISAKMP предоставляет механизмы согласования атрибутов безопасности. Базовое описание протокола ISAKMP содержится в документе **RFC2408**.

В рамках ISAKMP SA (протокола CPIKE), или другого протокола согласования ключей, для данной IPsec SA, как минимум, согласуются следующие компоненты:

- 32-битный код аутентификации SPI (неконфиденциален);
- 256-битный ключ *Kr_i*;
- параметры ГОСТ Р 34.11-94;
- максимальный объём данных SA (Lifetime SA, Kbytes);
- максимальное время жизни SA (Lifetime SA, sec);
- максимальное значение счётчика искажённых пакетов.

5 Преобразования

Заголовок AH-пакета ДОЛЖЕН соответствовать требованиям определенным в разделе 2 **RFC4302**, со следующими параметрами:

- явного выравнивания ICV не производится;
- ICV имеет размер 12 байт.

Для SA ДОЛЖЕН быть включен сервис обеспечения защиты от навязывания повторных пакетов (anti-replay).

Для преобразования AH_GOST-HMAC-4M используется алгоритм GOST-HMAC-4M, для преобразования AH_GOST-HMAC-1K используется алгоритм GOST-HMAC-1K.

6 Алгоритмы обеспечения целостности ГОСТ Р 34.11-94

Алгоритмы GOST-HMAC-4M и GOST-HMAC-1K предназначены для обеспечения целостности вложений ESP при применении с различными алгоритмами шифрования вложений. Основным применением данных алгоритмов является совместная работа с преобразованием ESP_NULL, т.е. обеспечение целостности и аутентичности ESP вложений без конфиденциальности.

Для SA ДОЛЖНА быть включена услуга обеспечения защиты от навязывания повторных пакетов (anti-replay).

Результатом применения алгоритмов GOST-HMAC-4M и GOST-HMAC-1K является значение ICV, рассчитываемое по формулам:

$$h = HMAC\_GOSTR3411(Ki\_i(Seq\#), Data)$$

$$ICV = substr(0..11, h)$$

6.1 Обработка исходящих пакетов

Порядок обработки исходящих пакетов ДОЛЖЕН соответствовать требованиям, определенным в разделах 3.3 **RFC4302** и **RFC4303**, со следующими уточнениями:

— ICV в преобразованиях с алгоритмом AH_GOST-HMAC-4M вырабатывается по формуле:

$$ICV = GOST\text{-}HMAC\text{-}4M(Ki\_i(Seq\#), IPhdr|..[|Seq\#h])$$

— ICV в преобразованиях с алгоритмом AH_GOST-HMAC-1K вырабатывается по формуле:

$$ICV = GOST\text{-}HMAC\text{-}1K(Ki\_i(Seq\#), IPhdr|..[|Seq\#h])$$

— отправителю РЕКОМЕНДУЕТСЯ увеличить счётчик объёма данных исходящих пакетов для соответствующей SA и сравнить его значение с максимальным объемом данных этой SA (Lifetime SA, Kbytes). При его превышении РЕКОМЕНДУЕТСЯ заблокировать дальнейшую работу данной SA.

6.2 Обработка входящих пакетов

Порядок обработки входящих пакетов ДОЛЖЕН соответствовать требования, определенным в разделах 3.4 **RFC4302** и **RFC4303**, со следующими уточнениями:

— получателю РЕКОМЕНДУЕТСЯ увеличить счётчик объёма данных входящих пакетов для соответствующей SA и сравнить его значение с максимальным объемом данных этой SA (Lifetime SA, Kbytes). При его превышении РЕКОМЕНДУЕТСЯ заблокировать дальнейшую работу данной SA;

— *ICV* в преобразованиях проверяется значением *ICVchk;*

— *ICVchk* для AH_GOST-HMAC-4M вырабатывается по формуле:

$$ICVchk = GOST\text{-}HMAC\text{-}4M(Ki\_i(Seq\#), IPhdr|..[|Seq\#h])$$

— *ICVchk* для AH_GOST-HMAC-1K вырабатывается по формуле:

$$ICVchk = GOST\text{-}HMAC\text{-}1K(Ki\_i(Seq\#), IPhdr|..[|Seq\#h])$$

— если *ICV* != *ICVchk*, то получателю РЕКОМЕНДУЕТСЯ увеличить счётчик искажённых пакетов соответствующей SA и сравнить его с максимальным значением счётчика искажённых пакетов этой SA. При его превышении РЕКОМЕНДУЕТСЯ заблокировать дальнейшую работу данной SA.

6.3 Вычисление MTU

При вычислении MTU следует руководствоваться правилами определенными в разделах 2 **RFC4302** и **RFC4303** с учётом фиксированного размера ICV — 12 байт, без выравнивания.

6.4 Алгоритм GOST-HMAC-4M

В алгоритме GOST-HMAC-4M используется:

$$Ki\_i(Seq\#) = Divers(Divers(Divers(Kr\_i, Seq\# \,\&\, 0xffffffff00000000)\ Seq\#\&0xffffffffffff0000)\ Seq\#\&0xffffffffffffffc0)$$

6.5 Алгоритм GOST-HMAC-1K

В алгоритме GOST-HMAC-1K используется:

$$Ki\_i(Seq\#) = Divers(Divers(Divers(Kr\_i, Seq\#\&0xffffffff00000000) Seq\#\&0xffffffffffff0000) Seq\#)$$

6.6 Дополнительные параметры и атрибуты AH и ESP SA

Порядок согласования атрибутов описан в разделе 6 **RFC4303**. Значения параметров по умолчанию для *AH_GOST-HMAC-4M*, *AH_GOST-HMAC-1K*, *GOST-HMAC-4M* и *GOST-HMAC-1K:*

Параметр	Атрибут	Формат	Умолчание
Максимальное значение счётчика искажённых пакетов	32402	B	10^5

Таблица 1: Параметры AH и ESP SA

7 Регистрация IANA

IANA выделяет два номера преобразований AH (ESP Authentication Algorithm) для использования **ГОСТ Р 34.11-94**:

<TBD-5> для AH_GOST-HMAC-4M и GOST-HMAC-4M;
<TBD-6> для AH_GOST-HMAC-1K и GOST-HMAC-1K.

7.1 Приватные номера преобразований

До регистрации в IANA предварительные реализации используют следующие приватные номера преобразований:

— 251 для AH_GOST-HMAC-4M и GOST-HMAC-4M;
— 250 для AH_GOST-HMAC-1K и GOST-HMAC-1K.

8 Примеры

Форматы представление данных в примерах:

0xNNNN: Представление целого числа в шестнадцатеричной системе счисления

0xFFFFFFFF FF...: Представление объктов в форме big-endian

BBBBBBBB BB: Представление в сетевой нотации. Числа в big-endian. Сетевое представление сложных объектов согласно стандартам их определяющих, в частности, ключей и хэшей согласно требованиям документов **RFC4357**, **RFC4490** и **RFC4491**

8.1 Тестовый пакет ESP_NULL+GOST-HMAC-4M

Открытые данные пакета, длина 53:

```
ESP   MAC 4M
Открытые данные пакета, длина 53:
4500001d 04050607 08090a0b 0c0d0e0f 10111213 14151617 18191a1b 1c1d1e1f
```

```
 20212223 24252627 28292a2b 2c2d2e2f 30313233 34
```

Параметры SA с алгоритмом шифрования ESP_NULL и алгоритмом обеспечения целостности GOST-HMAC-4M

```
SPI
 31323334
Seq#l
 0000007d
 ESN
 не согласован

Kr_i
 cb4e1a7f 2d61710d f264423c ad4384de ce01d676 90556865 f1cb7f7f ab4103c0
Kr_i2 = Divers(Kr_i, Seq# & 0xffffffff00000000)
 e88f38aa 23db821c 79f1cb4f 4ff050d0 e9165070 d16c9914 c4ed09c9 c2eddcbd
Kr_i1 = Divers(Kr_i2, Seq# & 0xffffffffffff0000)
 bfa97cea 9622d426 3e8612c0 8f022182 14ff681d 806fe1ec b2ffb569 6a9e51f6
Kc_i = Divers(Kr_i1, Seq# & 0xfffffffffffffc0)
 2a39d585 2466272f 4cc9518a db7a0798 5ec58bc7 968a2884 701f5932 419ca31b


 Промежуточные данные GOST-HMAC-4M


Seq#
 0000007d
MAC
 f5f23c4e d9c7be6a b39176ea


 ESP вложение, длина 76
 31323334 0000007d 4500001d 04050607 08090a0b 0c0d0e0f 10111213 14151617
 18191a1b 1c1d1e1f 20212223 24252627 28292a2b 2c2d2e2f 30313233 34000104
 f5f23c4e d9c7be6a b39176ea
```

8.2 Тестовый пакет ESP_NULL+GOST-HMAC-1K

Открытые данные пакета, длина 53:

```
 ESP   MAC 1K
 Открытые данные пакета, длина 53:
 4500001d 04050607 08090a0b 0c0d0e0f 10111213 14151617 18191a1b 1c1d1e1f
 20212223 24252627 28292a2b 2c2d2e2f 30313233 34
```

Параметры SA с алгоритмом шифрования ESP_NULL и алгоритмом обеспечения целостности GOST-HMAC-1K

```
SPI
 31323334
```

```
Seq#l
 0000007d
 ESN
 не согласован

Kr_i
 cb4e1a7f 2d61710d f264423c ad4384de ce01d676 90556865 f1cb7f7f ab4103c0
Kr_i2 = Divers(Kr_i, Seq# & 0xffffffff00000000)
 e88f38aa 23db821c 79f1cb4f 4ff050d0 e9165070 d16c9914 c4ed09c9 c2eddcbd
Kr_i1 = Divers(Kr_i2, Seq# & 0xffffffffffff0000)
 bfa97cea 9622d426 3e8612c0 8f022182 14ff681d 806fe1ec b2ffb569 6a9e51f6
Kc_i = Divers(Kr_i1, Seq#)
 5e7a4394 e45bc889 00c33a48 ffe870dd 7b1dc771 ab1da6dc 68251682 46c1430a


 Промежуточные данные GOST-HMAC-1K


Seq#
 0000007d
MAC
 329cff79 67085148 2bb205ea


 ESP вложение, длина 76
 31323334 0000007d 4500001d 04050607 08090a0b 0c0d0e0f 10111213 14151617
 18191a1b 1c1d1e1f 20212223 24252627 28292a2b 2c2d2e2f 30313233 34000104
 329cff79 67085148 2bb205ea
```

8.3 Тестовый пакет AH GOST-HMAC-4M

Входной пакет с обнулёнными изменяемыми полями AH и вставленным заголовком AH, длина 84:

```
 Vvvv      Len      vv Protocol=51=AH           vv Next Header=01=ICMP

 AH   AH 4M
 Данные пакета, длина 40:
 00005547 00010014 08090a0b 0c0d0e0f 10111213 14151617 18191a1b 1c1d1e1f
 20212223 24252627
```

Параметры AH SA GOST-HMAC-1K

```
SPI
 31323334
Seq#
 0000007d
ICV
 c2152293 42d2f0af c6a4f78d
```

Промежуточные данные GOST-HMAC-4M

```
 AH пакет, длина  84:
 45000054 0a2c0000 00330000 c0a855a8 c0a85570 01040000 31323334 0000007d
 c2152293 42d2f0af c6a4f78d 00005547 00010014 08090a0b 0c0d0e0f 10111213
 14151617 18191a1b 1c1d1e1f 20212223 24252627
```

8.4 Тестовый пакет AH GOST-HMAC-1K

Входной пакет с обнулёнными изменяемыми полями AH и вставленным заголовком AH, длина 84:

```
  Vvvv     Len      vv Protocol=51=AH           vv Next Header=01=ICMP

 AH   AH 4M
 Данные пакета, длина 40:
 00005547 00010014 08090a0b 0c0d0e0f 10111213 14151617 18191a1b 1c1d1e1f
 20212223 24252627
```

Параметры AH SA GOST-HMAC-1K

```
SPI
 31323334
Seq#
 0000007d
ICV
 07e92722 56bbf28d 34d63c9f
```

Промежуточные данные GOST-HMAC-1K

```
 AH пакет, длина  84:
 45000054 0a2c0000 00330000 c0a855a8 c0a85570 01040000 31323334 0000007d
 07e92722 56bbf28d 34d63c9f 00005547 00010014 08090a0b 0c0d0e0f 10111213
 14151617 18191a1b 1c1d1e1f 20212223 24252627
```

9 Совместимость

Требования по реализации преобразований и алгоритмов:

— AH_GOST-HMAC-4M и GOST-HMAC-4M — обязательно;
— AH_GOST-HMAC-1K и GOST-HMAC-1K — опционально, требуется при повышенных требованиях к безопасности (КВ1 или выше), или при передаче IPv6-слонограмм размером более 64 Кбайт.

УДК 351.864.1:004:083.131 **ОКС 35.040** **П85**

Ключевые слова: *электронная коммерция, электронная цифровая подпись, безопасность*

Руководитель организации-разработчика:

Генеральный директор
ООО «КРИПТО-ПРО»

_____ Чернова Н.Г.

Генеральный директор
ЗАО «Группа С-Терра»

_____ Рябко С.Д.

Руководитель разработки:

Директор по науке
ООО «КРИПТО-ПРО»

_____ Попов В.О.

Авторы документа:

Технический Директор
ООО «КРИПТО-ПРО»

_____ Леонтьев С.Е.

ООО «Крипто-Про»

_____ Пичулин Д.Н.

ЗАО «Группа С-Терра»

_____ Федченко А.А.