СИСТЕМЫ ОБРАБОТКИ ИНФОРМАЦИИ.

ЗАЩИТА КРИПТОГРАФИЧЕСКАЯ.

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ИСПОЛЬЗОВАНИЮ АЛГОРИТМОВ ОБЕСПЕЧЕНИЯ ЦЕЛОСТНОСТИ IPSEC (AH, ESP) НА ОСНОВЕ ГОСТ Р 34.11-94

Проект первой редакции,
апрель 2012,
rus-fedchenko-cpah-ipsecme-gost-00-rn

Москва
2012

Введение

Криптографическая защита информации является существенной составляющей любой информационной технологии. Стремительное развитие современных коммуникационных систем, таких как сети сотовой связи и оптоволоконных информационных магистралей, влечет за собой необходимость столь же активного развития всех компонентов систем защиты информации и подразумевает одновременное усиление роли стандартов, процедур, и методов направленных на усиление мер такой защиты.

Особую роль в этом процессе приобретают специализированные программные средства для разного рода аппаратно-программных систем обеспечения безопасности информационных магистралей, а также в сфере хранения и обработки информации.

Настоящие рекомендации предназначены для обеспечения совместимости реализаций IPsec AH (**RFC4302**).российских производителей, а также этот документ описывает соглашения по использованию ГОСТ Р 34.11-94 для обеспечения целостности (Integrity Algorithm) вложений IPsec ESP (**RFC4303**).

В данном документе описываются особенности реализации протокола AH при использовании алгоритма шифрования ГОСТ Р 34.11-94. В нем рассмотрены только отличия от базовой реализации протокола AH, в то время как полное описание протокола IPsec AH изложено в документе **RFC4302**.

Настоящими рекомендациями регламентируется использование **ГОСТ 28147-8**9, **ГОСТ Р 34.11-94** и **ГОСТ Р 34.10-2001** в протоколах AH, IKE и ISAKMP, но не определяются собственно сами алгоритмы и форматы представления криптографических типов данных. Применяемые, согласно условиям указанных выше национальных стандартов, алгоритмы описываются соответствующими национальными нормативными документами, а представление самих данных и необходимых параметров должно соответствовать положениям и требованиям, содержащихся в документах **RFC4357**, **RFC4491** и **RFC4490** организации координирующей разработки протоколов и развития архитектуры сети Интернет - IETF (Internet Engineering Task Force).

Содержание

1 Область применения

Протокол AH (**RFC4302**) используется для обеспечения целостности и аутентичности IP пакетов (вместе с заголовком). Протокол ESP используется для обеспечения конфиденциальности (опционально), целостности и аутентичности содержимого IP пакетов.

В рекомендациях определяются следующие преобразования AH и алгоритмы обеспечения целостности ESP:

— AH_GOST-HMAC-4M и GOST-HMAC-4M

— AH_GOST-HMAC-1K и GOST-HMAC-1K

Протоколы AH и ESP используется в архитектуре IPsec (**RFC4301**) для обеспечения конфиденциальности, целостности и аутентичности содержимого IP пакетов.

AH пакеты и ESP вложения обрабатываются в рамках IPsec SA, параметры которой МОГУТ быть интерпретированы согласно положениям, содержащимися в документе **RFC2407**. В этом же документе описаны и дополнительные расширяющие идентификаторы параметров.

При использовании данных рекомендаций применительно к оборонной продукции (работам, услугам), поставляемой для федеральных государственных нужд по государственному оборонному заказу, продукции (работам, услугам), используемой в целях защиты сведений, составляющих государственную тайну, или относимой к охраняемой в соответствии с законодательством Российской Федерации информации ограниченного доступа, продукции (работам, услугам), сведения о которой составляют государственную тайну, должны учитываться дополнительные требования, изложенные в специальных стандартах, устанавливающих правила использования ключей.

1.1 Текущий статус документа как проекта рекомендаций ТК26

Передача проекта настоящих рекомендаций в ТК26 означает, что каждый их автор соглашается с не эксклюзивным предоставлением IPR для ТК26, аналогично положениям стандарта Интернет IETF BCP 79.

Данный предварительный документ является открытым документом "Рабочей группы IPsec и IKE" и "Технического комитета по стандартизации "Криптографическая защита информации" (ТК26). Область распространения документа не ограничена.

Этот документ действителен в течении максимум девяти месяцев, и может быть в любое время изменён, заменён на другой или отозван его авторами в любое время.

При цитировании или ссылке на него из других документов следует ставить отметку — «документ готовится к публикации».

Список предварительных документов ТК26 доступен по <http://www.tc26.ru/>.

Настоящий предварительный документ актуален (действителен) до января 2013 года.

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 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.

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).

RFC4302 - Kent, S., "IP Authentication Header", IETF RFC 4302, December 2005.

RFC4303 - С. Кент, «Комбинированный алгоритм шифрования вложений IPSec (ESP)» (Kent S., IP Encapsulating Security Payload (ESP), IETF RFC 4303, December 2005).

RFC4304 - Kent, S., “Extended Sequence Number (RFC4304) 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).

IETF DRAFT CPESP - Леонтьев, С.Е., Павлов, М.В., А.А. Федченко, «Комбинированый алгоритм шифрования вложений IPsec на основе ГОСТ 28147-89», октябрь 2010.

CPIKE - Методические рекомендации по использованию ГОСТ 28147-89, ГОСТ Р 34.11-94 и ГОСТ Р 34.10-2001 при управлении ключами IKE и ISAKMP, проект, ноябрь 2011.

2.2 Информативные ссылки

RFC2409 - [IKE] Д. Харкинс, Д. Каррел, «Протокол защищенного согласования и аутентичности доставки идентифицированного материала для ассоциации безопасности (IKE)» (Harkins, D. and D. Carrel, The Internet Key Exchange (IKE), IETF RFC 2409, November 1998).

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

RFC4301 - [ARCH] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", IETF RFC 4301, December 2005.

RFC4491 - [CPPK] Leontiev, S. and 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", RFC 4491, May 2006.

RFC5831 - [ENG-GOSTR341194] Dolmatov, V., "GOST R 34.11-94: Hash Function Algorithm", IETF RFC 5831, March 2010.

RFC6071 - [ROADMAP] Frankel, S. and S. Krishnan, "IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap", RFC 6071, February 2011.

ПП РФ №957 - Постановление Правительства Российской Федерации от 29 декабря 2007 г. № 957 «Об утверждении положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами (в ред. Постановлений Правительства РФ от 21.04.2010 № 268, от 24.09.2010 № 749)

99-ФЗ - Федеральный закон от 04.05.2011 N 99-ФЗ (ред. от 19.10.2011, с изм. от 21.11.2011) "О лицензировании отдельных видов деятельности"

Примечание: При пользовании настоящими рекомендациями 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 настоящими рекомендациями 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 Терминология

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

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

4 Определения и обозначения

4.1 Определения

В настоящем документе определены следующие термины:

искажённый пакет:	ESP (**RFC4303**) вложение или AH пакет для которого вычисленное значение ICV не совпало с переданным значением
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 (**RFC4303**) вложение или AH пакет для которого не прошёл предварительный контроль SPI и Seq#

4.2 Обозначения

В настоящем документе используются следующие обозначения:

Divers(K,D):	алгоритм диверсификации ключа K по данным D (см. **RFC4357**, раздел 7). Узел замены определяется Раздел 6. В целях настоящего документа, аргументом D является 64-битное целое число, представленное 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 (см **RFC4357**, раздел 3, описание и пример сетевого представления результата ГОСТ Р 34.11-94 приведены в разделе 2.1 **RFC4490**)
Ki_i(Seq#):	ключ алгоритма имитозащиты пакета Seq# =3
Kr_i:	корневой ключ имитозащиты SA;
Seq#:	64-битный номер пакета, если (см. в **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 представленной в сетевом порядке последовательности **bytes**

bits[s..f]: последовательность бит с бита **s**, по бит **f**, выбранная из представленной в сетевом порядке последовательности **bits**

4.3 Сокращения

ESN Расширенный (64 бита) номер пакета в последовательности (Extended Sequence Number, см. в документе **RFC4304**)

ISAKMP Протокол управления ключами и группами атрибутов сетевой безопасности (Internet Security Association and Key Management Protocol)

MTU Наибольший размер передаваемых данных (в байтах), который может быть единовременно передан на уровне звена данных (уровень 2) базовой эталонной модели (OSI) в соответствии с **ГОСТ Р ИСО/МЭК 7498-1-99** (Maximum Transmission Unit)

SA Сопоставление параметров безопасности формируемых протоколом управления ключами и группами параметров сетевой безопасности (Security Association)

5 Состав сопоставления безопасности (AH_GOST SA)

Протокол управления ключами и группами атрибутов сетевой безопасности (ISAKMP) предоставляет механизмы согласования атрибутов безопасности. Базовое описание протокола ISAKMP содержится в документе **RFC2408**.
В рамках ISAKMP SA (**CPIKE**) или иной не-IPsec SA для данной IPsec SA, как минимум, согласуются следующие компоненты:

- 256-бит симметричный ключ Kr_i (используется K1);
- параметры ГОСТ 28147-89;
- максимальный объём данных SA в байтах (Lifetime SA, Kbytes);
- максимальный время жизни SA в секундах (Lifetime SA, sec);
- максимальное значение счётчика искажённых пакетов.

6 Преобразования

Заголовок AH пакета *ДОЛЖЕН* соответствовать требованиям документа **RFC4302** (см. раздел 2), со следующими параметрами:

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

Для SA *ДОЛЖНА* быть включена услуга 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.

7 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. услуга целостности вложения без услуги конфиденциальности.

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

Результатом алгоритмов GOST-HMAC-4M и GOST-HMAC-1K является значение ICV, которое имеет следующий вид:

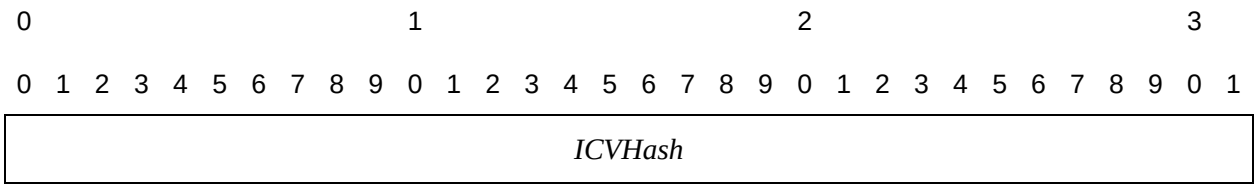

Рисунок 1. ICV для GOST-HMAC-4M и GOST-HMAC-1K

, где

h = HMAC_GOSTR3411(Ki_e(Seq#), Data);

,где *HMAC_GOSTR3411()* описан в **RFC4357** (см. раздел 3), описание и пример сетевого представления результата ГОСТ Р 34.11-94 даны в **RFC4490** (см. раздел 2.1)

ICVHash = substr(0..11, h);

7.1 Обработка исходящих пакетов

Порядок обработки исходящих пакетов ДОЛЖЕН соответствовать документам **RFC4302** (см. раздел 3.3) и **RFC4303** (см. раздел 3.3) со следующими уточнениями:

- Дополнительно к проверкам согласно требованиям содержащимся в документах **RFC4302** (см. раздел 3.3.1) и **RFC4303** (см. раздел 3.3.1) РЕКОМЕНДОВАНО проверить длину IP пакета на соответствие параметрам SA.
- ICV в преобразованиях вырабатывается для AH_GOST-HMAC-4M по формуле:

  ICV = GOST-HMAC-4M(Ki_e(Seq#), IPhdr|..[|Seq#h])

  , а для AH_GOST-HMAC-1K

  ICV = GOST-HMAC-1K(Ki_e(Seq#), IPhdr|..[|Seq#h])

- Отправителю РЕКОМЕНДОВАНО увеличить счётчик текущего объём данных SA в байтах (Lifetime SA, Kbytes) и сравнить его с максимальным. При его превышении РЕКОМЕНДОВАНО заблокировать дальнейшую работу SA.

7.2 Обработка входящих пакетов

Порядок обработки входящих пакетов ДОЛЖЕН соответствовать документам **RFC4302** (см. раздел 3.4) и **RFC4303** (см. раздел 3.4) со следующими уточнениями:

- Дополнительно к проверкам согласно требованиям содержащимся в документах **RFC4302** (см. раздел 3.4.2) и **RFC4303** (см. раздел 3.4.2) РЕКОМЕНДОВАНО проверить длину IP пакета на соответствие параметрам SA.
- Получателю РЕКОМЕНДОВАНО увеличить счётчик текущего объёма данных SA в байтах (Lifetime SA, Kbytes) и сравнить его с максимальным. При его превышении РЕКОМЕНДОВАНО заблокировать дальнейшую работу SA.
- ICV в преобразованиях проверяется для AH_GOST-HMAC-4M по формуле:

  ICVchk = GOST-HMAC-4M(Ki_i(Seq#), IPhdr|..[|Seq#h])

  , а для AH_GOST-HMAC-1K

  ICVchk = GOST-HMAC-1K(Ki_i(Seq#), IPhdr|..[|Seq#h])

- Если ICV не равно ICVchk, то получателю РЕКОМЕНДОВАНО увеличить счётчик искажённых пакетов SA и сравнить его с максимальным. При его превышении РЕКОМЕНДОВАНО заблокировать дальнейшую работу SA.

7.3 Вычисление MTU

При вычислении MTU следует руководствоваться правилами определенными в документах **RFC4302** (см. раздел 2) и **RFC4303** (см. раздел 2) с учётом фиксированного размера ICV - 12 байт, без выравнивания.

7.4 Алгоритм GOST-HMAC-4M

В алгоритме GOST-HMAC-4M используются:

Ki_i(Seq#) = Divers(Divers(Divers(Kr_i, Seq# & 0xffffffff00000000),
Seq#&0xffffffffffff0000),
Seq#&0xfffffffffffffc0);

НЕ РЕКОМЕНДОВАНО согласовывать размеры AH пакетов (ESP вложений) более 64 Кбайт.

7.5 Алгоритм GOST-HMAC-1K

В алгоритме GOST-HMAC-1K используются:

Ki_i(Seq#) = Divers(Divers(Divers(Kr_i, Seq#&0xffffffff00000000),
Seq#&0xffffffffffff0000),
Seq#);

7.6 Дополнительные параметры и атрибуты SA

Порядок согласования атрибутов описан в документе **RFC4303** (см. раздел 6). 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	10^9
Максимальный размер пакета	32507	B	65536

Таблица 1: Параметры AH_GOST SA

8 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.

8.1 Приватные номера преобразований

До регистрации 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

Примечание: После регистрации в IANA этот пункт будет необходимо изъять из данного документа.

9 Требования по безопасности

Приложения РЕКОМЕНДУЕТСЯ исследовать установленным порядком на соответствие заданным требованиям согласно Постановлению Правительства Российской Федерации (см. документ **ПП РФ №957**).

Параметры криптографических алгоритмов влияют на стойкость. НЕ РЕКОМЕНДУЕТСЯ использование параметров, которые не перечислены в **RFC4357**, без соответствующих исследований, описанных там же (см. раздел 9).

Приложениям РЕКОМЕНДОВАНО согласовывать время жизни SA (Lifetime SA), как по времени, так и по объёму переданной информации согласно требованиям, изложенным в документе **RFC4301** (см. раздел 4.4.2.1). Также НЕ РЕКОМЕНДОВАНО согласовывать время жизни SA (Lifetime SA) в секундах более, чем на 86400 сек (1 сутки).

НЕ РЕКОМЕНДОВАНО согласовывать время жизни SA в байтах (Lifetime SA, sec) более, чем на 2^{80} байт.

НЕ РЕКОМЕНДОВАНО согласовывать параметр *Max-Auth-Error* больший чем 10^{9}, без соответствующего исследования.

Для приложений с требованиями по уровню защиты КВ1 и выше НЕ РЕКОМЕНДОВАНО согласовывать параметр *Max-Auth-Error* больший чем 10^{6}, без соответствующего исследования.

10 Примеры

Представление данных в примере:

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**

10.1 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 0x
 31323334
Seq#1 0x
 0000007d
 ECN
    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# & 0xfffffffffffffffc0)
 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
```

10.2 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 0x
 31323334
Seq#l 0x
 0000007d
 ECN
    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
```

10.3 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
```

10.4 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
```

11 Совместимость

Требования по реализации 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 (attacks based on timing and EMI analysis) или для использования IPv6 «JUMBOGRAMS» пакетов(**RFC2675**).

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»:

_____ Павлов М.В.

ЗАО «Группа С-Терра»:

_____ Федченко А.А.

Лист изменений

Предназначен для подготовки документа и его поддержки. Его необходимо изъять из состава документа в момент публикации методических рекомендаций.

00-ra 2008-07-26 ЛСЕ

"Рыба", только оглавление и ссылки;

00-rb 2008-08-14 ЛСЕ

Терминология ESP (RFC4303);

00-rc 2009-02-15 ЛСЕ

Выделил Integrity Algorithm ESP (RFC4303) и AH в отдельный документ;

Упомянул внутреннее выравнивание ГОСТ Р 34.11-94, описанное в стандарте;

00-rd 2009-03-01 ЛСЕ

Описание PDF, XML Validated;

Подготовлено для согласования с Владимиром Олеговичем Поповым.

00-re 2009-03-16 ЛСЕ

удалено описание ICVCounter, оно не нужно, т.к. ключ HMAC меняется, либо каждые 4 Мбайт, либо каждый пакет;

Термин "неаутентифицированный пакет" заменён на термин "искажённый пакет";

Исправлены нестандартные по [RFC2119] термины;

Документ, который должен вводить идентификатор ГОСТ Р 34.11-94 для [IKE] пока под вопросом.

00-rf 2009-03-16 ЛСЕ

Удалены метки конфиденциальности и Copyright;

Добавлены рыбы тестовых примеров;

Вставлены окончательные значения примеров хэш-функции;

Вставлен редактор английского перевода;

00-rg 2009-12-02 ПВО & ЛСЕ

Убрано описание хэш-функции ГОСТ Р 34.11-94, перенесено в [draft.CPIKE], т.к. в основном хэш-функция используется там. Замечу, что [draft.CPIKE] - обзателен к реализации, а этот документ - нет;

Внесено описание опционального алгоритма "Использование совместно с алгоритмами обеспечения целостности IPsec ГОСТ Р 34.11-94", перенесено из [draft.CPESP (RFC4303)], т.к. это позволило убрать "паразитную" ссылку между документами, а для основных применений IPsec [ESP (RFC4303)] (КС1-КС3) этот алгоритм без надобности;

Теперь только этот документ содержит нормативные ссылки на предварительные документы [draft.CPIKE] и [draft.CPESP (RFC4303)]. И это хорошо, т.к. данный документ посвящён опциональным алгоритмам, а те посвящены обязательным алгоритмам.

00-rh 2009-12-07 ЛСЕ

Учтены остальные замечания Смыслова Валерия Анатольевича, ОАО "ЭЛВИС-ПЛЮС".

00-ri 2009-12-08 ПВО & ЛСЕ

Исправлены примеры.

00-rk 2010-07-15 ЛСЕ

Учтены замечания Мартанова Георгия Олеговича, НТЦ "Атлас" и Смыслова Валерия Анатольевича, ОАО "ЭЛВИС-ПЛЮС" об исключении специального случая использования HMAC для решений КВ и выше.

00-rl 2010-10-18 ПВО & ЛСЕ

Вставлены информативные ссылки на RFC 5830, 5831 и 5832.

00-rn 2012-04-24 ПМВ, ПВО & ЛСЕ

Изменение формата к проекту методической рекомендации.