СИСТЕМЫ ОБРАБОТКИ ИНФОРМАЦИИ

ЗАЩИТА КРИПТОГРАФИЧЕСКАЯ

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ИСПОЛЬЗОВАНИЮ КОМБИНИРОВАННОГО АЛГОРИТМА ШИФРОВАНИЯ ВЛОЖЕНИЙ IPSEC ESP НА ОСНОВЕ ГОСТ 28147-89

Проект первой редакции,
июль 2012,
rus-fedchenko-cpesp-ipsecme-gost-00-rt

Москва
2012

Введение

Протокол инкапсуляции зашифрованных данных (Encapsulating Security Payload, ESP) используется для обеспечения конфиденциальности, целостности и аутентичности содержимого IP пакетов и входит в группу протоколов защиты сетевого трафика на IP-уровне – IP Security (IPsec). Полное описание протокола ESP приведено в документе **RFC4303**.

Настоящая рекомендация содержит описание использования алгоритма **ГОСТ 28147-89** при шифровании вложений IPsec ESP.

Настоящая рекомендация не определяет криптографический алгоритм **ГОСТ 28147-89** и форматы представления криптографических типов данных. Алгоритм и представление данных определены национальным стандартом **ГОСТ 28147-89**, а представление параметров соответствует определенному в документах **RFC4357** и **RFC4490**.

Необходимость разработки настоящего документа вызвана потребностью в обеспечении совместимости реализаций протокола IPsec ESP российских производителей.

Содержание

1 Область применения

Настоящая рекомендация описывает особенности реализации протокола ESP при использовании алгоритма шифрования **ГОСТ 28147-89**. В настоящем документе описаны только отличия от базовой реализации протокола ESP, в то время как полное описание протокола IPsec ESP изложено в документе **RFC4303**.

Настоящая рекомендация определяет следующие преобразования вложений в рамках протокола ESP:

- комбинированное преобразование ESP_GOST-4M-IMIT;
- комбинированное преобразование ESP_GOST-1K-IMIT.

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

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 марта 2013.

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 г.

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).

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

RFC4301 — С. Кент, К. Сео, «Архитектуры секретности в протоколах сети Интернет» (Kent S. and K. Seo, Security Architecture for the Internet Protocol, IETF RFC 4301, 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 (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).

2.2 Информативные ссылки

RFC2409 — 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).

RFC4106 — Viega, J. and D. McGrew, “The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)”, IETF RFC 4106, June 2005.

RFC4134 — П. Хоффман, «Примеры сообщений формата S/MIME» (Hoffman P., Examples of S/MIME Messages, IETF RFC 4134, July 2005).

RFC4309 — Housley, R., “Using Advanced Encryption Standard (AES) CCM Mode with IPsec Encapsulating Security Payload (ESP)”, IETF RFC 4309, December 2005.

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).

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).

RFC5116 — Д. Макгрейв, «Интерфейс и алгоритмы для аутентификации при шифровании» (McGrew D., An Interface and Algorithms for Authenticated Encryption, IETF RFC 5116, January 2008).

RFC5282 — Black, D. and D. McGrew, “Using Authenticated Encryption Algorithms with the Encrypted Payload of the Internet Key Exchange version 2 (IKEv2) Protocol”, IETF RFC 5282, August 2008.

RFC5996 — С. Кауфман, П. Хофман, Й. Нир, П. Еронен, «Протокол обмена ключами в сети Интернет, версия 2 (IKEv2)» (Kaufman C., Hoffman P., Nir Y., and P. Eronen, Internet Key Exchange Protocol Version 2 (IKEv2), IETF RFC 5996, September 2010).

RFC6071 — Frankel, S. and S. Krishnan, “IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap”, IETF RFC 6071, February 2011.

RFC6311 — Singh R., Kalyani G., Nir Y., Sheffer Y. and D. Zhang, “Protocol Support for High Availability of IKEv2/IPsec”, IETF RFC 6311, July 2011.

ГОСТ Р ИСО/МЭК 7498-1-99 — Государственный стандарт Российской Федерации. 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), Госстандарт России, 2007© Национальные стандарты

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).

[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.

Примечание – При пользовании настоящим 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 настоящим 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 Определения и обозначения

3.1 Определения

В настоящем документе определены следующие термины:

3.1.1 **искажённый пакет**: ESP вложение, для которого вычисленное значение ICV не совпало с переданным значением.

3.1.2 **сопоставление безопасности (Security Association, SA)**: Совокупность атрибутов безопасности и ключевой информации, ассоциируемая с безопасным соединением, представляющим собой виртуальный однонаправленный канал для передачи данных.

3.1.3 **пакет с искажённым *Seq#***: ESP вложение, для которого не прошёл предварительный контроль соответствия SPI, *Seq#* или не совпала старшая часть ***ICV***[32..63] для ESP_GOST-1K-IMIT.

3.2 Обозначения

В настоящем документе используются следующие обозначения:

encryptCNT (IV, K, D)	Шифрование **ГОСТ 28147-89** в режиме "гаммирования" на ключе K данных D с начальным вектором IV
decryptCNT (IV, K, D)	Расшифрование **ГОСТ 28147-89** в режиме "гаммирования" на ключе K данных D с начальным вектором IV
Divers (K,D)	Алгоритм диверсификации ключа K по данным D (см. раздел 7 в **RFC4357**). В целях настоящего документа, аргументом D является 64-битное целое число, представленное в сетевом порядке байт
gost28147IMIT (IV, K, D)	Выработка имитовставки **ГОСТ 28147-89** на ключе K от данных D, с внутренним выравниванием нулями до границы блока 8 байт. Описание и пример сетевого представления результата приведёны в документе **RFC4490**, разделы 9.2, 9.3
A	Первые блоки открытых данных, участвующие в выработке имитовставки, которые содержат служебную информацию (адресную часть, отметку времени, синхропосылку и др.) и не зашифровываются, смотри в **ГОСТ 28147-89**.
Seq#	64-битный номер пакета, если использование расширенного номера пакета в последовательности (ESN) не согласовано, то значение *Seq#* всегда меньше 2^{32}
IV(Seq#)	Синхропосылка пакета *Seq#*
Kc_e (Seq#)	Ключ комбинированного алгоритма шифрования пакета *Seq#*
Kc_i (Seq#)	Ключ комбинированного алгоритма имитозащиты пакета *Seq#*
Kc_i2 (Seq#)	Ключ предварительного контроля пакета *Seq#* и SA для ESP_GOST-1K-IMIT
Kr_e	Корневой ключ шифрования SA

Kr_i	Корневой ключ имитозащиты SA
KeyMeshing	Алгоритм усложнения ключа, описанный в документе **RFC4357**
Seq#h	Старшая часть *Seq#*
Seq#l	Младшая часть *Seq#*
SPI-Auth-Code	Код аутентификации, вычисляемый в рамках ISAKMP SA или иной не-IPsec SA, предназначен для целей аудита, а также используется для предварительного контроля *Seq#* и SA
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 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 (SA)

Протокол управления ключами и группами атрибутов сетевой безопасности (ISAKMP) предоставляет механизмы согласования атрибутов безопасности. Базовое описание протокола ISAKMP содержится в документе **RFC2408**.

Особенности реализации алгоритма **ГОСТ 28147-89** в рамках ISAKMP требуют обязательного наличия в составе каждого сопоставления безопасности (SA) следующих компонент:

- 256-бит симметричный ключ *Kr_e*;
- 256-бит симметричный ключ *Kr_i*;
- 32-х битный код аутентификации SPI (неконфиденциален);
- параметры ГОСТ 28147-89;
- максимальный объём данных, переданных с использованием этого сопоставления безопасности (Lifetime SA, Kbytes);
- максимальное время жизни соединения, установленного с использованием этого сопоставления безопасности (Lifetime SA, sec);
- максимальное значение счётчика искажённых пакетов.

Размеры согласуемого ключевого материала (KEYMAT) в зависимости от преобразования следующие:

- ESP_GOST-4M-IMIT: 36 байт (*Kr_e* и *SPI-Auth-Code*);
- ESP_GOST-1K-IMIT: 68 байт (*Kr_e, Kr_i* и *SPI-Auth-Code*).

Примечание - Для приложений, в которых организационно-техническими мерами обеспечивается защита от навязывания повторных пакетов (услуга anti-replay не согласуется) и соответствие между ESP SA и получаемыми пакетами, ключевой материал для SPI-Auth-Code может не вырабатываться, а при выработке IV величины SPI-Auth-Code и SPI полагаются равными 0. Например, в случае приёма и передачи одного SA по одной линии связи без переупорядочивания пакетов.

6 Инкапсуляция зашифрованных данных (ESP)

6.1 Общие требования

Вложение ESP-пакета должно соответствовать описанному для комбинированного преобразования в документе **RFC4303** (см. раздел 2). Инкапсуляция зашифрованных данных с использованием алгоритма шифрования **ГОСТ 28147-89** должна выполняться с учетом следующих требований:

6.1.1 Синхропосылка IV передаётся в пакете и имеет размер 8 байт;

6.1.2 ESP вложение выравнивается на границу 8 байт;

6.1.3 Если согласовано использование расширенного номера в последовательности (ESN), то $Seq\#h$ в пакете не передаётся;

6.1.4 Явного выравнивания ICV не производится;

6.1.5 ICV передаётся в пакете, имеет размер 4 байта (для преобразования ESP_GOST-4M-IMIT) или 8 байт (для преобразования ESP_GOST-1K-IMIT).

6.1.6 Для сопоставления безопасности (SA) РЕКОМЕНДУЕТСЯ:

- либо включение услуги обеспечения защиты от навязывания повторных пакетов (anti-replay);
- либо в случае, если услуга защиты от навязывания повторных пакетов не используется или используется не в полном объёме, РЕКОМЕНДУЕТСЯ обеспечивать дополнительными организационно-техническими мерами ограничения на общее количество и суммарный объём ESP пакетов с одинаковым значением $Seq\#$.

6.2 Порядок применения ГОСТ 28147-89 для вложений ESP

Первые блоки открытых данных, которые участвуют в выработке имитовставки для вложения ESP пакета, должны содержать следующую служебную информацию $A = SPI \mid Seq\#l \mid IV$:

- адресная часть (SPI);
- отметка времени ($Seq\#l$);
- синхропосылка (IV).

Если согласовано использование расширенного номера в последовательности (ESN), то $Seq\#h$ в пакете не передаётся.

Рисунок 1. Служебная информация (A) для вложений ESP

Полное описание блоков служебной информации приводится в **ГОСТ 28147-89** (см. раздел 5.4).

6.3 Обработка исходящих пакетов

Порядок обработки исходящих пакетов ДОЛЖЕН соответствовать разделу 3.3 документа **RFC4303** со следующими уточнениями:

6.3.1 Дополнительно к проверкам, предусмотренным положениями раздела 3.3.1 документа **RFC4303** РЕКОМЕНДУЕТСЯ проверить длину ESP вложения на соответствие параметрам сопоставления безопасности (SA).

6.3.2 Имитовставка в преобразованиях вырабатывается по формуле:

$$substr(0..3, ICV) =$$

$$gost28147IMIT(0, Kc\_i(Seq\#), A|..|Next\ Header[|Seq\#h])$$

6.3.3 Шифрование в преобразовании ESP_GOST-4M-IMIT осуществляется без усложнения ключа, а в преобразовании ESP_GOST-1K-IMIT в режиме усложнения ключа id-Gost28147-89-CryptoPro-KeyMeshing, и осуществляется по формуле:

$$encryptCNT(IV(Seq\#), Kc\_e(Seq\#), Payload\ data|...|Next\ Header)$$

6.3.4 Для преобразования ESP_GOST-1K-IMIT:

$$substr(4..7, ICV) =$$

$$gost28147IMIT(0, Kc\_i2(Seq\#), A|Encrypted\ payload[|Seq\#h]|substr(0..3, ICV))$$

6.3.5 Отправителю РЕКОМЕНДУЕТСЯ увеличить счётчик объёма данных, переданных с использованием текущего сопоставления безопасности (Lifetime SA, Kbytes), и сравнить его с максимально разрешенным для данного SA значением. При превышении этого значения РЕКОМЕНДУЕТСЯ заблокировать дальнейшую работу в рамках данного SA.

6.4 Обработка входящих пакетов

Порядок обработки входящих пакетов ДОЛЖЕН соответствовать определенному в разделе 3.4 документа **RFC4303**, со следующими уточнениями:

6.4.1 Дополнительно к проверкам, определенным в разделе 3.4.2 документа **RFC4303**, РЕКОМЕНДУЕТСЯ проверить длину ESP вложения на соответствие параметрам SA.

6.4.2 При предварительном контроле (preliminary Sequence Number check) *Seq#l* пакета в соответствии с положениями, содержащимися в разделе 3.4.3 документа **RFC4303**, для преобразований ESP_GOST-4M-IMIT и ESP_GOST-1K-IMIT РЕКОМЕНДУЕТСЯ выполнить проверку вектора *IV* (*IV.IVCounter*, см. раздел 6.6 настоящих рекомендаций).

6.4.3 Для преобразования ESP_GOST-1K-IMIT на этапе предварительного контроля получатель ДОЛЖЕН вычислить:

$$ICVchk2 = gost28147IMIT(0, Kc\_i2(Seq\#), A|Encrypted\ payload[|Seq\#h]|substr(0..3, ICV))$$

6.4.4 Если *substr(4..7, ICV)* не равна *ICVchk2*, то получатель ДОЛЖЕН прервать обработку пакета и НЕ ДОЛЖЕН изменять состояние SA. Получатель МОЖЕТ не обеспечивать аудит этих событий (РЕКОМЕНДУЕТСЯ не обеспечивать аудит этих событий без явного на то указания).

6.4.5 Получателю РЕКОМЕНДУЕТСЯ увеличить счётчик текущего объёма данных, получаемых с использованием текущего сопоставления безопасности (Lifetime SA, Kbytes) и сравнить его с максимально разрешенным для данного сопоставления значением. При превышении максимального значения счетчика РЕКОМЕНДУЕТСЯ заблокировать дальнейшую работу SA.

6.4.6 Расшифрование в преобразовании ESP_GOST-4M-IMIT осуществляется без усложнения ключа, а в преобразовании ESP_GOST-1K-IMIT в режиме усложнения ключа id-Gost28147-89-CryptoPro-KeyMeshing, и осуществляется по формуле:

$$decryptCNT(IV(Seq\#), Kc\_e(Seq\#), Encrypted\ payload)$$

6.4.7 Имитовставка в преобразованиях проверяется по формуле:

$$ICVchk = gost28147IMIT(0, Kc\_i(Seq\#), A|..|Next\ Header[|Seq\#h])$$

6.4.8 Если *substr(0..3, ICV)* не равна *ICVchk*, то получателю РЕКОМЕНДУЕТСЯ увеличить счётчик искажённых пакетов, полученных в рамках текущего сопоставления безопасности (SA), и сравнить его с максимально разрешенным для данного SA значением. При превышении максимально допустимого значения счетчика РЕКОМЕНДУЕТСЯ заблокировать дальнейшую работу SA.

6.5 Вычисление MTU

6.5.1 Для определения MTU в случае использования преобразований ESP_GOST-SIMPLE-IMIT и ESP_GOST-4M-IMIT следует руководствоваться правилами, описанными в разделе 2 документа **RFC4303**, то есть производить выравнивание до размера, кратного 8 байтам, с учётом фиксированного добавленного размера 12 байт (8 байт IV + 4 байта ICV).

6.5.2 Для определения MTU в случае использования преобразования ESP_GOST-1K-IMIT следует руководствоваться правилами, описанными в разделе 2 документа **RFC4303**, то есть производить выравнивание до размера, кратного 8 байтам, с учётом фиксированного добавленного размера 16 байт (8 байт IV + 8 байт ICV).

6.6 Преобразование ESP_GOST-4M-IMIT

В преобразовании ESP_GOST-4M-IMIT используется вектор *IV(Seq#l)*, который имеет следующий вид:

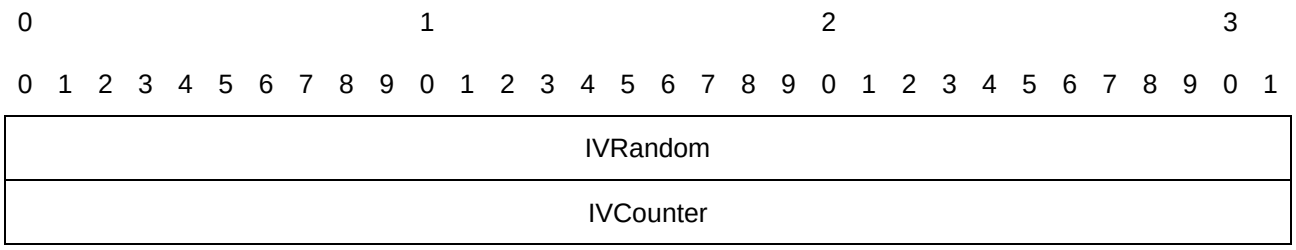


Рисунок 2. для ESP_GOST-4M-IMIT и ESP_GOST-1K-IMIT

В этом случае:

IVRandom - случайные 4 байта;

$IVCounter = SPI\text{-}Auth\text{-}Code + SPI + Seq\#l + IVRandom \pmod{2^{32}}$;

Получатель ДОЛЖЕН контролировать *IVCounter* на фазе предварительного контроля *Seq#* и НЕ ДОЛЖЕН выполнять криптографических преобразований, если на этапе предварительного контроля выявлена ошибка. Если реализация ESP поддерживает ведение журналов аудита, то это событие МОЖЕТ классифицироваться как ошибка контроля *Seq#*. В частности, пакеты с ошибочным *IVCounter* НЕ ДОЛЖНЫ вызывать увеличения счётчика искажённых пакетов и уменьшения счетчика объёма данных SA.

KeyMeshing = id-Gost28147-89-None-KeyMeshing;

Kc_e(Seq#) = Divers(Divers(Divers(Kr_e, Seq#&0xffffffff00000000),
Seq#&0xffffffffffff0000),
Seq#&0xffffffffffffffc0);

Kc_i(Seq#) = Kc_e(Seq#).

НЕ РЕКОМЕНДУЕТСЯ согласовывать размеры ESP вложений с длиной более чем 64 Кбайт.

6.7 Преобразование ESP_GOST-1K-IMIT

В преобразовании ESP_GOST-1K-IMIT используются следующие элементы:

IV(Seq#l) получается так же, как в разделе 6.6 ;

KeyMeshing = id-Gost28147-89-CryptoPro-KeyMeshing;

Kc_e(Seq#) = Divers(Divers(Divers(Kr_e, Seq#&0xffffffff00000000),
Seq#&0xffffffffffff0000),
Seq#);

Kc_i(Seq#) = Kc_e(Seq#);

Kc_i2(Seq#) = Divers(Divers(Divers(Kr_i, Seq#&0xffffffff00000000),
Seq#&0xffffffffffff0000),
Seq#);

7 Дополнительные параметры и атрибуты ESP SA

Для согласования атрибутов преобразований, описанных в разделе 6 настоящего документа, при использовании протокола IKE (см. в документе **RFC2409**) обе стороны ДОЛЖНЫ согласовать идентификатор приложения ESP_GOST_vendor_ID.

ESP_GOST_vendor_ID имеет следующий формат:

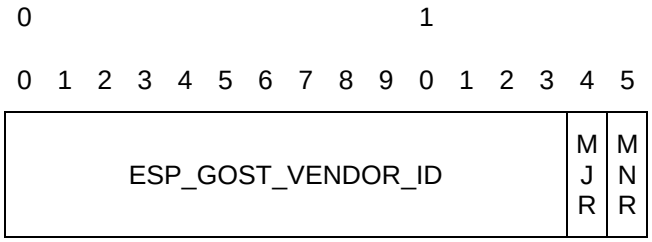


Рисунок 3. ESP_GOST_VENDOR_ID

В данном случае ESP_GOST_VENDOR_ID = { '\x03', '\x10', '\x17', '\xE0', '\x7F', '\x7A', '\x82', '\xE3', '\xAA', '\x69', '\x50', '\xC9', '\x99', '\x99' } (первые 14 байт ГОСТ Р 34.11-94 хэш от char строки "IKE/GOST"), а байты MJR и MNR соответствуют текущей major и minor версии преобразований ESP_GOST (т.е. 1 и 1).

Таблица 1. Параметры ESP_GOST SA

Параметр	Атрибут	Формат	Умолчание
Параметры ГОСТ 28147-89	32401	B	-
Максимальный размер пакета	32403	V	65536
Максимальное значение счётчика искажённых пакетов (SA Life Type)	64402	-	10^6

7.1 Параметры ГОСТ 28147-89

7.1.1 При согласовании SA РЕКОМЕНДУЕТСЯ согласовать параметры **ГОСТ 28147-89**. Класс атрибута: GOST-28147-89-SBOX (32401), формат атрибута: базовый (B).

Таблица 2. Параметры ГОСТ 28147-89

GOST-28147-89 S-Box	Значение
id-Gost28147-89-CryptoPro-A-ParamSet	65403
id-Gost28147-89-CryptoPro-B-ParamSet	65404
id-Gost28147-89-CryptoPro-C-ParamSet	65405
id-Gost28147-89-CryptoPro-D-ParamSet	65406

7.1.2 Приложения IPsec, удовлетворяющие данному документу, ДОЛЖНЫ реализовать набор параметров id-Gost28147-89-CryptoPro-B-ParamSet. В противном случае, для применения в сети Интернет РЕКОМЕНДУЕТСЯ использовать набор параметров id-Gost28147-89-CryptoPro-B-ParamSet. Остальные опциональные алгоритмы МОГУТ применяться в сетях со специальными требованиями (например, при использовании многоуровневого шифрования).

7.2 Максимальное значение счётчиков искажённых пакетов

При достижении максимального значения счётчиков искажённых пакетов, определяемых SA-Life-Duration для значения SA-Life-Type=Max-Integrity-Fails, РЕКОМЕНДУЕТСЯ уничтожить ESP SA или заблокировать обработку входящих пакетов.

7.3 Максимальный размер пакета

Класс атрибута: Max-Packet-Len (32403), формат атрибута: переменная длина (V).

В случае применения ESP для описанных в документе **RFC2675** «JUMBOGRAMS» пакетов IPv6 (размерами от 64 Кб до 4 Гб), приложению РЕКОМЕНДУЕТСЯ согласовать этот параметр.

8 Зашифрованные вложения IKEv2

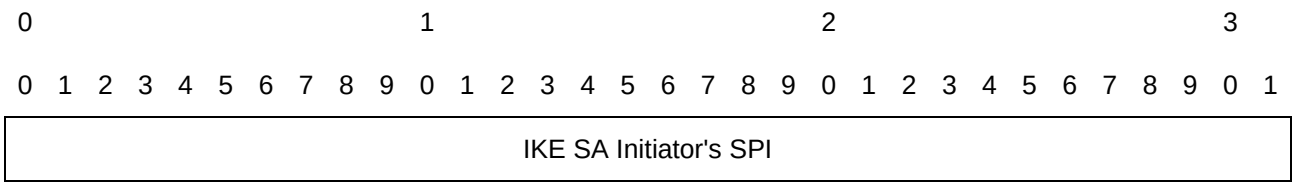
Этот раздел основывается на требованиях раздела 5.4 **ГОСТ 28147-89**, которые определяют порядок имитозащиты служебной информации (адресной части (SPIs), отметок времени (M-ID), синхропосылки (IV) и др.) передаваемой в незашифрованном виде. Порядок контроля целостности, в целом соответствует рекомендациям документов **RFC5282** (см. раздел 5) и **RFC5116**, которые расширяют базовый способ контроля целостности, описанный в документе **RFC5996**, на случай применения комбинированных алгоритмов.

Выработка ключевого материала для преобразований ESP осуществляется в соответствии с правилами, определенными в документе **RFC5996** (см. раздел 2.14), при этом ключи SK_ai и SK_ar контроля целостности IKEv2 не используются. Таким образом, размер каждого ключа ДОЛЖЕН трактоваться как 0 октетов.

Размеры ключевого материала для ключей SK_ei и SK_er определяются согласно определенным в разделе 3 документа **RFC 5996** – два раза по 36 байт или два раза по 68 байта. Ключевой материал необходимой длины вырабатывается итеративным применением функции PRF без выравнивания на размер значения хэш-функции.

8.1 Порядок применения ГОСТ 28147-89 для вложений IKEv2

Первые блоки открытых данных, которые участвуют в выработке имитовставки для зашифрованных вложений IKEv2, имеют следующий вид **ГОСТ 28147-89** (раздел 5.4):



<table>
<tr><td colspan="6">IKE SA Responder's SPI</td></tr>
<tr><td>Next Payload</td><td>MjVer</td><td>MnVer</td><td colspan="2">Exchange Type</td><td>Flags</td></tr>
<tr><td colspan="6">Message ID</td></tr>
<tr><td colspan="6">Length</td></tr>
<tr><td colspan="6">Unencrypted IKE Payloads</td></tr>
<tr><td>Next Payload</td><td>C</td><td colspan="2">RESERVED</td><td colspan="2">Payload Length</td></tr>
<tr><td colspan="6">IV (зависит от преобразования)</td></tr>
</table>

Рисунок 4. Служебная информация (A) для вложений IKEv2

Служебная информация: $A = IKEv2\ Header|Unencrypted\ IKE\ Payloads|Payload\ Header|IV$

8.2 Выработка IV для вложений IKEv2

Для ESP_GOST-4M-IMIT и ESP_GOST-1K-IMIT требования на выработку и проверку *IV* аналогичны требованиям изложенным в разделе 6.6 настоящих рекомендаций, за исключением следующего уточнения:

$$Seq\# = Message\text{-}ID*2 + R\text{-}flag;$$

$$SPI = SPIi\#h + SPIi\#l;$$

или

$$SPI = SPIr\#h + SPIr\#l;$$

в зависимости от направления и назначения передачи.

Получателю РЕКОМЕНДУЕТСЯ контролировать *IV*, согласно требованиям в разделах 6.7 и 6.8 настоящих рекомендаций, и он НЕ ДОЛЖЕН выполнять криптографические преобразования при обнаружении ошибки.

При применении положений, содержащихся в документе **RFC6311,** РЕКОМЕНДУЕТСЯ, либо отказаться от согласования IKEV2_MESSAGE_ID_SYNC_SUPPORTED, либо обеспечить ограничение количества и суммарного объёма второго и последующих пакетов с Message-ID равными 0, смотри в разделе 12 документа **RFC6311**.

9 Регистрация IANA

IANA выделяет три номера преобразований ESP для использования ГОСТ 28147-89:
<TBD-3> для ESP_GOST-4M-IMIT;
<TBD-4> для ESP_GOST-1K-IMIT

9.1 Удалить после регистрации в IANA

Пока, предварительные реализации используют следующие приватные номера преобразований:

254 для ESP_GOST-SIMPLE-IMIT;
253 для ESP_GOST-4M-IMIT;
252 для ESP_GOST-1K-IMIT.

9.2 Регистрации в IANA не подлежит

Используемые в этом документе приватные "magic numbers":

Таблица 3. ESP_GOST "magic numbers"

Класс	Значение	Тип	Ссылка
GOST-28147-89-SBOX	32401	B	Раздел 7.1
Max-Packet-Len	32403	B	Раздел 5.3

Используемые в этом документе приватные значения:

Таблица 4. ESP_GOST приватные значения

Название	Значение	Атрибут
Max-Integrity-Fails	64402	SA-Life-Type, [DOI]
id-Gost28147-89-CryptoPro-A-ParamSet	65403	GOST-28147-89-SBOX, Раздел 7.1
id-Gost28147-89-CryptoPro-B-ParamSet	65404	GOST-28147-89-SBOX, Раздел 7.1
id-Gost28147-89-CryptoPro-C-ParamSet	65405	GOST-28147-89-SBOX, Раздел 7.1
id-Gost28147-89-CryptoPro-D-ParamSet	65406	GOST-28147-89-SBOX, Раздел 7.1

10 Требования по безопасности

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

10.1.2 Параметры криптографических алгоритмов влияют на стойкость. Использование параметров, которые не перечислены в **RFC4357**, НЕ РЕКОМЕНДУЕТСЯ без соответствующих исследований, описанных в документе **RFC 4357** (см. раздел 9).

10.1.3 Поскольку **ГОСТ 28147-89** имеет размер блока 64-бит, то для обеспечения конфиденциальности и целостности данных реализациям IPsec РЕКОМЕНДУЕТСЯ соблюдать следующие ограничения:

- ESP_GOST-4M-IMIT РЕКОМЕНДУЕТСЯ обрабатывать пакеты, не превышающие размера 64 Кбайта. НЕ РЕКОМЕНДУЕТСЯ согласовывать параметр Max-Packet-Len для пакетов IPv6 больший, чем 64 Кбайта, и НЕ РЕКОМЕНДУЕТСЯ использовать JUMBO-фреймы (см. документ **RFC2675**) в IPv6. РЕКОМЕНДУЕТСЯ повторное согласование ключей для нового ESP SA по достижению максимально допустимого объёма данных SA (Lifetime SA) - 2^{80} байт;
- ESP_GOST-1K-IMIT РЕКОМЕНДУЕТСЯ повторное согласование ключей для нового ESP SA по достижению максимально допустимого объёма данных SA (Lifetime SA) - 2^{80} байт.

10.1.4 Приложениям РЕКОМЕНДУЕТСЯ согласовывать время жизни SA (Lifetime SA), как по времени, так и по объёму переданной информации, смотри раздел 4.4.2.1 в документе **RFC4301**.

10.1.5 НЕ РЕКОМЕНДУЕТСЯ согласовывать время жизни SA (Lifetime SA) в секундах более чем на 86400 сек (1 сутки).

10.1.6 НЕ РЕКОМЕНДУЕТСЯ согласовывать параметр Max-Integrity-Fails больший, чем 10^6, без соответствующего исследования.

10.1.7 Для приложений с требованиями по уровню защиты KB1 и выше НЕ РЕКОМЕНДУЕТСЯ согласовывать параметр Max-Integrity-Fails больший, чем 10^{1}, без соответствующего исследования. Так же, для таких приложений, без соответствующего исследования, НЕ РЕКОМЕНДУЕТСЯ использовать преобразование ESP_GOST-4M-IMIT.

11 Требования по совместимости

Требования по реализации преобразований:

ESP_GOST-4M-IMIT - обязательно;

ESP_GOST-1K-IMIT - опционально, требуется при повышенных требованиях к безопасности (attacks based on timing and EMI analysis), или при использовании JUMBO-фреймов [JUMBOGRAMS] при передаче пакетов IPv6 размером более 64 Кбайт.

Обязательный к реализации набор параметров ГОСТ 28147-89 - id-Gost28147-89-CryptoPro-B-ParamSet.

11.1 Совместимость со старыми реализациями IKEv1

Некоторые реализации IKEv1 не полностью совместимы с рекомендациями [ROADMAP], [ARCH], [ESP], [GCM-ESP], [CCM-ESP], и не поддерживают реализацию поля ICV и его проверки, в случае, если для ESP SA согласован Integrity algorithm "NULL", т.е. если "proposal" не содержит атрибута "Authentication Algorithm" (5).

Такие реализации протокола IKEv1 МОГУТ согласовывать в "proposal" значение атрибута "Authentication Algorithm" (5):

GOST-NULL-INTEGRITY-ALGORITHM - 65411.

Поведение ESP SA в этом случае ДОЛЖНО быть таким же, как при отсутствии атрибута "Authentication Algorithm" (5).

Примеры

Представление данных в примерах:

`0xNNNN:`

Представление целого числа в шестнадцатеричной системе счисления;

`0xFFFFFFFF FF...:`

Представление объектов 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 [CPALGS], [CPCMS] и [CPPK].

В примерах используются параметры ассоциации безопасности, принятые по умолчанию: шифрование с узлом замены id-Gost28147-89-CryptoPro-B-ParamSet.

A.1. Тестовый пакет ESP_GOST-4M-IMIT

```
 ESP   GOST 4M
 Открытые данные пакета, длина 53:
 4500001d 04050607 08090a0b 0c0d0e0f 10111213 14151617 18191a1b 1c1d1e1f
 20212223 24252627 28292a2b 2c2d2e2f 30313233 34


SPI 0x
 31323334
Seq#l 0x
 0000007d
 ECN
    не согласован

SPI-Auth-Code 0x
cb4e1a7f
Kr_e
 b63d156f 7aac0dc7 cd915c35 63f61b9d 5c730a74 e331bc8c 3fc24a36 06463893
Kr_e2 = Divers(Kr_e, Seq# & 0xffffffff00000000)
 3a742e54 a9e8a3a1 1f4af5f7 c92fdac1 55142bee 86766e8c 03fad68d 35baf3d7
Kr_e1 = Divers(Kr_e2, Seq# & 0xffffffffffff0000)
 752bdd27 99dcde7b 92c04591 40fac2cb 974f39dc cf589d45 00a67c75 99ff9fcc
Kc_e = Divers(Kr_e1, Seq# & 0xfffffffffffffc0)
 0772fe26 c770590f 22902ad2 1a919eee ccab5396 baf2f1b5 54366c30 27a38614
```

Параметры SA с комбинированным алгоритмом и промежуточные данные ESP_GOST-4M-IMIT:

```
 Промежуточные данные ESP_GOST-4M-IMIT


Seq#
```

```
 0000007d
IVRandom
 05060708
IVCounter
 01865538
 Padding, PadLen, NextProto
 000104
ICV
 0bd8ba08
```

```
ESP вложение, длина 76
31323334 0000007d 05060708 01865538 fa104495 3cd50f2b cca22b90 f4f36257
8f4c2435 f04ada62 d0abc8b3 099e0473 d1ccd142 1586d564 a5e3d1c2 34e529ff
fe652e24 caad891c 0bd8ba08
```

A.2. Тестовый пакет ESP_GOST-1K-IMIT

```
ESP   GOST 1K
Открытые данные пакета, длина 1049:
4500001d 04050607 08090a0b 0c0d0e0f 10111213 14151617 18191a1b 1c1d1e1f
20212223 24252627 28292a2b 2c2d2e2f 30313233 34353637 38393a3b 3c3d3e3f
40414243 44454647 48494a4b 4c4d4e4f 50515253 54555657 58595a5b 5c5d5e5f
60616263 64656667 68696a6b 6c6d6e6f 70717273 74757677 78797a7b 7c7d7e7f
80818283 84858687 88898a8b 8c8d8e8f 90919293 94959697 98999a9b 9c9d9e9f
a0a1a2a3 a4a5a6a7 a8a9aaab acadaeaf b0b1b2b3 b4b5b6b7 b8b9babb bcbdbebf
c0c1c2c3 c4c5c6c7 c8c9cacb cccdcecf d0d1d2d3 d4d5d6d7 d8d9dadb dcdddedf
e0e1e2e3 e4e5e6e7 e8e9eaeb ecedeeef f0f1f2f3 f4f5f6f7 f8f9fafb fcfdfeff
00010203 04050607 08090a0b 0c0d0e0f 10111213 14151617 18191a1b 1c1d1e1f
20212223 24252627 28292a2b 2c2d2e2f 30313233 34353637 38393a3b 3c3d3e3f
40414243 44454647 48494a4b 4c4d4e4f 50515253 54555657 58595a5b 5c5d5e5f
60616263 64656667 68696a6b 6c6d6e6f 70717273 74757677 78797a7b 7c7d7e7f
80818283 84858687 88898a8b 8c8d8e8f 90919293 94959697 98999a9b 9c9d9e9f
a0a1a2a3 a4a5a6a7 a8a9aaab acadaeaf b0b1b2b3 b4b5b6b7 b8b9babb bcbdbebf
c0c1c2c3 c4c5c6c7 c8c9cacb cccdcecf d0d1d2d3 d4d5d6d7 d8d9dadb dcdddedf
e0e1e2e3 e4e5e6e7 e8e9eaeb ecedeeef f0f1f2f3 f4f5f6f7 f8f9fafb fcfdfeff
00010203 04050607 08090a0b 0c0d0e0f 10111213 14151617 18191a1b 1c1d1e1f
20212223 24252627 28292a2b 2c2d2e2f 30313233 34353637 38393a3b 3c3d3e3f
40414243 44454647 48494a4b 4c4d4e4f 50515253 54555657 58595a5b 5c5d5e5f
60616263 64656667 68696a6b 6c6d6e6f 70717273 74757677 78797a7b 7c7d7e7f
80818283 84858687 88898a8b 8c8d8e8f 90919293 94959697 98999a9b 9c9d9e9f
a0a1a2a3 a4a5a6a7 a8a9aaab acadaeaf b0b1b2b3 b4b5b6b7 b8b9babb bcbdbebf
c0c1c2c3 c4c5c6c7 c8c9cacb cccdcecf d0d1d2d3 d4d5d6d7 d8d9dadb dcdddedf
e0e1e2e3 e4e5e6e7 e8e9eaeb ecedeeef f0f1f2f3 f4f5f6f7 f8f9fafb fcfdfeff
00010203 04050607 08090a0b 0c0d0e0f 10111213 14151617 18191a1b 1c1d1e1f
20212223 24252627 28292a2b 2c2d2e2f 30313233 34353637 38393a3b 3c3d3e3f
40414243 44454647 48494a4b 4c4d4e4f 50515253 54555657 58595a5b 5c5d5e5f
```

```
 60616263 64656667 68696a6b 6c6d6e6f 70717273 74757677 78797a7b 7c7d7e7f
 80818283 84858687 88898a8b 8c8d8e8f 90919293 94959697 98999a9b 9c9d9e9f
 a0a1a2a3 a4a5a6a7 a8a9aaab acadaeaf b0b1b2b3 b4b5b6b7 b8b9babb bcbdbebf
 c0c1c2c3 c4c5c6c7 c8c9cacb cccdcecf d0d1d2d3 d4d5d6d7 d8d9dadb dcdddedf
 e0e1e2e3 e4e5e6e7 e8e9eaeb ecedeeef f0f1f2f3 f4f5f6f7 f8f9fafb fcfdfeff
 00010203 04050607 08090a0b 0c0d0e0f 10111213 14151617 18
```

Параметры SA с комбинированным преобразованием ESP_GOST-1K-IMIT [RFC 2408]

```
SPI 0x
 31323334
Seq#l 0x
 0000007d
Seq# 0x
0000000b 0000007d
 ECN
    не согласован

SPI-Auth-Code 0x
c4c08a66
Kr_e
 b63d156f 7aac0dc7 cd915c35 63f61b9d 5c730a74 e331bc8c 3fc24a36 06463893
Kr_e2 = Divers(Kr_e, Seq# & 0xffffffff00000000)
 59f1548e a0b38639 c546fb94 2164d780 f075460a cb72e4cf f3068a03 a184d544
Kr_e1 = Divers(Kr_e2, Seq# & 0xffffffffffff0000)
 c210c1fc 6988bb00 6ed69111 9d63a619 6c4cee21 799786db 2af3bda9 c77f9e20
Kc_i = Kc_e = Divers(Kr_e1, Seq#)
 fdcd7812 74018a14 5aee2da7 f21a1581 148378b9 272e3d88 0585ac2e 94b4bbe2
Kr_i
 cb4e1a7f 2d61710d f264423c ad4384de ce01d676 90556865 f1cb7f7f ab4103c0
Kr_i2 = Divers(Kr_i, Seq# & 0xffffffff00000000)
 52aa9784 2ee74f7a 5c3c7436 9fe4f415 5a4bc218 05fc6263 2a1ef408 4d8de3a2
Kr_i1 = Divers(Kr_i2, Seq# & 0xffffffffffff0000)
 7ea6c8f3 209ac480 f181aa61 5c38d07b fd680717 16581ff9 c2963646 6094cc3a
Kc_i2 = Divers(Kr_i1, Seq#)
 138309a0 5813c2bf d3bfb2a9 aff9b511 555c2088 ababcac7 f21f0871 1036aff8
```

Промежуточные данные ESP_GOST-1K-IMIT

```
Seq#
 0000007d
IVRandom
 05060708

IVCounter
 faf8c51f
```

```
 Padding, PadLen, NextProto
 00000000 00050400 00000b
ICV
 bb3465d8 eb50af47


 ESP вложение, длина 1080
 31323334 0000007d 05060708 faf8c51f 85bc7a31 676f1453 c167d042 1e87a0d1
 a23cbb97 cefbd7fe e95c3d1a b9f3fa9e 144dc92a 97e6de75 5b1fda97 8436c90b
 289c222f 80de286b bdf190b3 be7f6abb f627c56d 25ecc471 9bc9a5f3 403f1852
 67b43b70 a860b606 625ab17b 839078dd a55c9e76 78388625 27f17ef8 da3c964f
 0e320c68 6e71c9bb e17381d0 321fdfb5 8092f205 2df6d199 90ec758d 31eb6eeb
 3e152d43 89d4d402 9ab77fb4 09fcf757 b4086948 cf9d8843 5a2b21f2 6c41aa5f
 6b881623 be08b64e 4aeaba95 706598f3 5d56ee18 0feafff4 32b35a54 b37a7c77
 6e408d09 65aa2aa4 41f69040 03cec18a e1529416 88afe127 1c0fd90b c9699020
 9a98527f e8d4a285 de2f1d09 3b0f6779 a2391f71 d12d1219 c98b74ce 30b35b04
 381896c5 205ca00b ed4df571 d24ecfd3 7134b910 7c8eeb2d 6e3dedf3 ffab4af1
 1e69b296 fb4a9d0d 3dc364e0 4f0c6ab9 925322e4 0a8ff71e 4281d099 87260500
 bdfbdaf2 7669db9e 5b6021c7 91e77aa9 e7e4fe4a c6cafefc 80ff180b e3ec8d33
 6fb8172f 460daaf0 1f407230 bc282c25 9f14bc46 2d8d972e d27bf894 29696abb
 03d37ff0 f4ff8c0b c1f62112 eba15368 218a94ca 16847d57 55522e27 60913848
 50e84cbb 75438c26 9d216dee 67f82392 4f90a745 1b62b561 badadf9e d9bd481f
 6c8d1152 307e5b3b ead13bea 6b3d0b8b 20c0e17e 84109d55 3c431bb3 20ce8ea1
 c69e7cfb d720e186 dd4bbdb0 00008b23 f7271bcd ab1f10f2 009d98d1 66af8d49
 bf41d101 7aec62b3 1c4ad813 f3508887 d626f23d 387e5398 0ac70ddb 2a5688b4
 97f16918 b75f52ca d70751ce 3df694ff 7a07f6ba c1de8abd 6ff88df4 c48299b5
 c3e056ec 28ab6d6b 7cd16a59 4f41617b 8cb3bdff a5819619 348cb287 6bf4dcdd
 4985141b 2dd6f25a 49fce6cb b43a3dc3 8ca7dfcc fb3b4eca 4b1750eb 0d9da228
 80bedd9a 56d1768e 5e883cb1 282c6746 792a9fe9 2a2eabfd 9e48f25c 25ee1f6e
 f75c0d05 8ea213a4 f355cac0 608625f1 d78bc810 7d382ef3 0e87240a 4a4c1b87
 0c0714a5 7ddd9d09 e12eaf2d 032a1264 cdaf6feb 52b4f3ea 3abb0304 518a11ec
 3086d016 cc81461a 34fe9c5a 112a213d ffee305a 7133184c e05df5aa eabd1d9f
 341c2951 a126eabf aad3fd0c 6f81faa4 1ccea61e 9a654dec 266147e4 cf14fed7
 17656776 781ac09c 6b1e5650 e0a37e3d 98c7a384 3f3c001f e8e5db0f d9c03490
 9775bf74 25cf5f63 5befb502 af14595a 56517525 5c3752d9 2f6c7de7 7e80fb37
 b6c7d772 d117e4aa e6b1f3a3 1215889f 02111e63 93bd59cb b263a914 275efa37
 8069f230 994564af 9f340363 293286ac 6a97d66b 8045fba9 41f41575 6f52d018
 162d445c 2f8e6d47 99d00bf7 f419207f bfc51477 7c217b7d bfe9f660 acdd2c43
 b6fcb8fc 37db0f6d 78e29e58 88f35340 18217600 cbae06d1 1f24f66c e3c876b6
 5157a1e1 356aeed2 e5f4f5c9 3e4784c2 22678beb a7113bc2 e2de9439 382395c6
 9c4d0e84 b900f9e1 88f6ec28 651d9462 bb3465d8 eb50af47
```

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;

00-rc 2009-02-15 ЛСЕ

Учёт изменений по окончании предварительного криптографического анализа;
Удалён "Алгоритм 'preliminary check', OPTIONAL";
Учёт требования [ESP] относительно методов имитозащиты Seq#h
Изменено выравнивание вложений ESP с 4 на 8 байт;

00-rd 2009-03-01 ЛСЕ

Описание PDF, XML Validated;
Подготовлено для согласования с Владимиром Олеговичем Поповым.

00-re 2009-03-16 ЛСЕ

Термин "неаутентифицированный пакет" заменён на термин "искажённый пакет";
Исправлены нестандартные по [KEYWORDS] термины;
Уточнено использование SPIcookie.

00-rf 2009-07-10 ЛСЕ

Уточнение совместного использования комбинированных алгоритмов ESP_GOST-4M-IMIT/ESP_GOST-1K-IMIT и алгоритмов контроля целостности.

00-rg 2009-09-23 ПМВ & ЛСЕ

Уточнение при передаче в ТК26 и переводе на английский.

00-rh 2009-03-16 ЛСЕ

Удалены метки конфиденциальности и Copyright;
Добавлены рыбы тестовых примеров;
Вставлен редактор английского перевода;

00-ri 2009-11-18 ПВО & ЛСЕ

Вставлены примеры пакетов;
Стиль, в первом приближении, изменён на русский, для ТК26;
Сверка русского и английского текста;

00-rj 2009-12-01 ПВО & ЛСЕ

Описание опционального алгоритма приложения В. "Использование совместно с алгоритмами обеспечения целостности IPsec ГОСТ Р 34.11-94" перенесено в [draft.CPAH], т.к. это позволило убрать "паразитную" ссылку между документами, а для основных применений IPsec [ESP] (КС1-КС3) этот алгоритм без надобности. Теперь документ не содержит нормативных ссылок на предварительные документы, только информативная ссылка на [draft.CPIKE].

00-rk 2009-12-07 ЛСЕ

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

00-rl 2009-12-08 ПВО & ЛСЕ

Исправлены примеры.

00-rm 2010-07-15 ЛСЕ

Учтены замечания Мартанова Георгия Олеговича, НТЦ "Атлас" об исключении необходимости использования HMAC для решений KB (ESP_GOST-1K-IMIT).

Учтено замечание Смыслова Валерия Анатольевича, ОАО "ЭЛВИС-ПЛЮС" об унификации использования SPIcookie.

Внесён абзац, пока под вопросом, в котором учтено пожелание Смыслова Валерия Анатольевича, ОАО "ЭЛВИС-ПЛЮС", об опциональном использования SPIcookie, для специальных применений.

00-rn 2010-10-18 ПВО & ЛСЕ

Исправлены иллюстрационные (контрольные) примеры с учётом замечаний Захарова Дмитрия Николаевича, ООО "Фактор-ТС", Мартанова Георгия Олеговича, НТЦ "Атлас", и Смыслова Валерия Анатольевича, ОАО "ЭЛВИС-ПЛЮС".

Вставлены информативные ссылки на RFC 5830, 5831 и 5832.

Вставлено разъяснение по использованию преобразований в IKEv2 и ссылки на RFC 5116 [IAEA], RFC 5282 [AEAD] и RFC 5996 (последняя версия [IKEv2]).

Вставлены информативные ссылки на RFC 4106, 4309 и draft-ietf-ipsecme-roadmap. По просьбе Igor Roytman, CheckPoint, вставлен GOST-NULL-INTEGRITY-ALGORITHM (65411).

00-ro 2011-05-21 ПВО & ЛСЕ

Учтены замечания Смыслова Валерия Анатольевича, ОАО "ЭЛВИС-ПЛЮС":

- Переименован SPIcookie в SPI-Auth-Code;
- Уточнено использование параметров ГОСТ 28147-89 с целью уменьшения различных предложений параметров SA;
- Убрано использование I-flag, как ошибочное;
- Уточнены требования по ani-replay (в частности на услугу IKEV2_MESSAGE_ID_SYNC_SUPPORTED);
- Параметр Max-Auth-Error, был атрибутом SA, стал значением SA-Life-Type - Max-Integrity-Fails;
- Уточнено описание атрибутов;
- Убраны упоминания AH, т.к. они не нужны;
- Исправлены ошибки пунктуации.

00-rp 2011-11-08 ЛСЕ

Исправлена ссылка на [IPSECHA], ссылки на [ARCH] и [JUMBOGRAMS] перенесены в информативные.

00-rq 2012-02-02 ПВО & ЛСЕ

Учли замечания представителей рецензентов от ТК26 в части исключения ESP_GOST-SIMPLE-IMIT

00-rr 2012-04-24 ПАВ & ЛСЕ

Редакторские правки.

00-rs 2012-11-08 ПВО&ЛСЕ

Исправления по результатам совместных испытаний соответствия реализации IPsec проектам методических рекомендаций ТК26 и обеспечения встречной работы ООО "Фактор-ТС" (Dionis NX) и ООО "КРИПТО ПРО" (КриптоПро CSP).

00-rt 2012-07-13 ПВО&ЛСЕ

TODO: Исправления по результатам совместных испытаний ООО "Фактор-ТС" (Dionis NX) и ООО "КРИПТО ПРО" (КриптоПро CSP) и XXX Stonesoft (YYY)