СИСТЕМЫ ОБРАБОТКИ ИНФОРМАЦИИ. ЗАЩИТА КРИПТОГРАФИЧЕСКАЯ. 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 первой редакции,
июль 2012,
rus-fedchenko-cpike-ipsecme-gost-00-rt

Москва
2012

Содержание

1 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 описывают предназначенное для обеспечения аутентификации сторон с использованием отечественной криптографии расширение протокола IKE в архитектуре ISAKMP, и именуемое здесь в дальнейшем IKE/GOST. Данное расширение применимо как для формирования параметров безопасности ISAKMP SA и IPsec SA, так и для использования его в других архитектурах безопасности.

Настоящими рекомендациями регламентируется использование **ГОСТ 28147-89**, **ГОСТ Р 34.11-94** и **ГОСТ Р 34.10-2001** в протоколах IKE и ISAKMP, но рекомендации не определяют 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).

Подробные сведения о протоколах IKE и ISAKMP содержатся в документах **RFC2408** и **RFC2409**, а в данных рекомендациях описываются особенности применения только расширения протокола IKE/GOST.

1.1 Текущий статус документа

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.

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.

Примечание – Основная часть рекомендаций дополнена приложениями:

- Приложение А : Применение.
- Приложение Б : Описание текстового представления PSK.
- Приложение В : Сведения о соответствии ссылочных международных (региональных) стандартов национальным стандартам Российской Федерации, использованным в настоящем документе в качестве нормативных ссылок.
- Приложение Г :Сведения о соответствии национальных и межгосударственных стандартов ссылочным международным стандартам.

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.

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 Р 34.10-2001 — Государственный комитет Российской Федерации по стандартам, «Информационные технологии. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи», ГОСТ Р 34.10-2001, Государственный стандарт Российской Федерации, 2001.

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 34.310-2004 — Межгосударственный совет по стандартизации, метрологии и сертификации Содружества Независимых Государств (EASC), «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма (на русском языке)», ГОСТ 34.310-2004, Минск, 2004.

2.1 Дополнительные ссылки

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).

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).

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).

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).

3 Информативные ссылки

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"

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).

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)

IETF DRAFT CPAH — Леонтьев, С. Е., Павлов М. В., А. А. Федченко «Алгоритм обеспечения целостности IPsec (ESP, AH) на основе ГОСТ Р 34.11-94», November 2011.

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

Примечание 1 - Другие международные стандарты, руководства и прочие документы по вопросам, рассматриваемым в настоящих рекомендациях, приведены в библиографии.

Примечание 2 - 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.

4 Основные понятия, термины и определения

В настоящем документе использованы следующие определения:

IPsec (сокращение от IP Security) — набор протоколов для обеспечения защиты данных, передаваемых по межсетевому протоколу IP, позволяет осуществлять подтверждение аутентичности данных. IPsec также включает в себя протоколы для защищённого обмена ключами в сети Интернет;

IKE (Internet Key Exchange) — протокол защищенного согласования ключей и аутентичности доставки идентификационного материала для формирования ассоциации безопасности (SA);

Имитозащита — защита системы шифрованной связи от навязывания ложных данных;

Имитовставка — отрезок информации фиксированной длины, полученной по определенному правилу из открытых данных и ключа и добавленный к зашифрованным данным для обеспечения имитозащиты;

Гаммирование — процесс наложения по определенному закону гаммы шифра на открытые данные;

Хэш функция (функция хэширования) — функция, отображающая строки бит в строки бит фиксированной длины. Полное определение хэш-функции приводится в **ГОСТ 34.10-2001**.

5 Обозначения и сокращения

Основные обозначения и определения используемые в данном документе соответствуют общепринятым для широкого круга специалистов, как в области криптозащиты данных, так и для специалистов в области телекоммуникаций. В целом они соответствуют примененным в технической документации к протоколу IKE терминам.

5.1 Обозначения

Для обозначения переменных, функций и их параметров в настоящих рекомендациях применяются нижеследующие обозначения:

encryptCFB(IV, K, D) — шифрование по **ГОСТ 28147-89** в режиме "гаммирования с обратной связью" на ключе K данных D с начальным вектором IV (см. **RFC4357**, раздел 1.1 и раздел 4 в **ГОСТ 28147-89**, согласование узла замены определено в нем же в разделе 7.2);

decryptCFB(IV, K, D) — расшифрование по **ГОСТ 28147-89** в режиме "гаммирования с обратной связью" на ключе K данных D с начальным вектором IV (см. **RFC4357**,раздел 1.1 и раздел 4 в **ГОСТ 28147-89**, согласование узла замены определено там же в разделе 7.2);

encryptECB(K, D)	— расшифрование данных D по **ГОСТ 28147-89** в режиме "простой замены" на ключе K (см. **RFC4357**, раздел 1.1 и раздел 2 в **ГОСТ 28147-89**);
decryptECB(K, D)	— расшифрование данных D **ГОСТ 28147-89** в режиме "простой замены" на ключе K (см. раздел 1.1 в **RFC4357** и раздел 2 в **ГОСТ 28147-89**).
gost28147IMIT(IV, K, D)	— выработка имитовставки по **ГОСТ 28147-89** на ключе K от данных D внутренним выравниванием нулями до границы блока 8 байт (см. раздел 1.1 в **RFC4357** и раздел 5 в **ГОСТ 28147-89**), описание и пример сетевого представления результата приведёны в **RFC4490** (см. разделы 9.2 и 9.3, согласование узла замены описано в разделе 7.2);
HASH(D)	— расчёт хэш функции с внутренним выравниванием по **ГОСТ Р 34.11-94**. Описан в **RFC4490**, в пункте 2.1 и в пункте 3 **IETF DRAFT CPAH**);
KE	— открытый ключ асимметричной ключевой пары, который представляется в виде последовательности октетов (см. в **RFC4490**, пункт 2.3.2), тип *GostR3410-2001-PublicKey*, длиной 64 байта;
K_i	— закрытый ключ Инициатора.
KE_i	— открытый ключ Инициатора.
K_r	— закрытый ключ Ответчика.
KE_r	— открытый ключ Ответчика.
Gx	— открытый ключ без параметров, который представляется в виде последовательности октетов (см. в **RFC4490,** пункт 2.3.2**)**, тип GostR3410-2001-PublicKey, длиной 64 байта.
Cert_i	— сертификат открытого ключа Инициатора.
Cert_	— сертификат открытого ключа Ответчика.
(x_i, gx_i)	— значение асимметричной ключевой пары Инициатора на согласованных параметрах группы.
(x_r, gx_r)	— значение асимметричной ключевой пары Ответчика на согласованных параметрах группы.
VKO(x_i, gx_r, ukm)	— алгоритм выработки сессионного ключа на основе алгоритма Диффи-Хеллмана в соответствии с "VKO GOST R 34.10-2001" (см. в **RFC4357**, раздел 5.2).
Akey	— конкатенация одного или двух результатов VKO(), является согласованным ключом фазы 1.
prf(K,D)	— ключевая функция порождения псевдослучайных величин HMAC_GOSTR3411(K,D). Описана в **RFC4357**, раздел 3.
Last_ICV	— накопленная имитовставка обмена фазы 1 (переданная в последнем пакете фазы 1).
AUTH-I, AUTH-R	— результаты аутентификации Инициатора и Ответчика соответственно, 32-байтовые величины.
substr(s..f, bytes)	— последовательность байт с байта s, по байт f, выбранная из представленной в сетевом порядке последовательности bytes.
Signature(d, h)	— вычисляет значение ЭЦП **ГОСТ Р 34.10-2001** по значению хэш-функции **ГОСТ Р 34.11-94** h на основе закрытого ключа d **ГОСТ Р 34.10-2001**.

5.2 Аббревиатуры

В тексте настоящих рекомендаций используются следующие сокращения и аббревиатуры:

ISAKMP	Internet Security Association and Key Management Protocol. Протокол управления ключами и группами параметров сетевой безопасности;
SA	Security Association. Набор параметров безопасности формируемых протоколом управления ключами и группами параметров сетевой безопасности;
ЭЦП	электронная цифровая подпись (digital signature);
IKE/GOST	расширение протокола IKE, включающее в себя механизм использования в его рамках отечественных алгоритмов криптозащиты;
SPI	Security Parameter Index. Идентификатор IPsec SA;
HMAC	Hash-based message authentication code. Хэш-код аутентификации сообщений;
PFS	Perfect Forward Security (см. **RFC2409**, раздел 3.3).

6 Использование хэш-функции по алгоритму ГОСТ Р 34.11-94

Настоящими рекомендациями определяется использование идентификатора *GOST_R_34_11_94,* описанного в **RFC2409,** для хэш-функции по **ГОСТ Р 34.11-94**. Построение кода аутентификации, расширяющего протокол IKE (см. документ **RFC2409**), определяется положениями документа **RFC4357**, разделы 3 и 4. Представление значений **ГОСТ Р 34.11-94** (а так же HMAC на её основе) определено в **RFC4490,** раздел 2.1.

Таким образом функция *prf()* при согласовании хэш-функции **ГОСТ Р 34.11-94** определяется следующим образом:

$$prf(key, msg) = HMAC\_GOSTR3411(key, msg)$$

Соответственно здесь применяется **ГОСТ Р 34.11-94** с параметрами *id-GostR3411-94-CryptoProParamSet* (см. **RFC4357,** раздел 8.2).

7 Шифрование ISAKMP вложений по алгоритму ГОСТ 28147-89

Если в заголовке ISAKMP пакета установлен бит E(ncryption Bit), то такой заголовок изображается как "HDR*" и этот пакет (все его вложения) шифруется в рамках ISAKMP SA. Шифрование пакетов ISAKMP с одинаковым Message-ID осуществляется последовательно, и в порядке обмена данными между сторонами. При этом последовательности с разными Message-ID не равными 0 могут обрабатываться независимо.

7.1 Требования к фазе 1

На фазе 1 формируется набор параметров безопасности (ISAKMP SA).

M-ID заголовков пакетов равен 0. При формировании, в рамках протокола ISAKMP, набора параметров безопасности (ISAKMP SA) должны быть соблюдены следующие требования, а именно:

- сторонами должны быть согласованы алгоритм, параметры шифрования и имитозащиты **ГОСТ 28147-89**;
- сторонами должен быть согласован алгоритм (параметры) хэширования **ГОСТ Р 34.11-94**;
- сторонами должны быть согласованы эфемерные ключи Инициатора и Ответчика gx_i и gx_r;
- должен быть вычислен ключ SKEYID-e;
- аутентификация сторон фазы 1 не должна быть закончена.

Поле Message-Nonce – должно содержать последовательность 8 нулей;

AUTH-I – должна являться пустой последовательностью;

AUTH-R – должна являться пустой последовательностью.

$$IV = substr(0..7, HASH(gx\_i|gx\_r))$$

НЕ РЕКОМЕНДУЕТСЯ до завершения аутентификации и установления ISAKMP SA шифровать информационные сообщения (см. в **RFC2409,** раздел 5.7).

7.2 Требования к фазе 2

Под фазой 2 рассматриваемого в данной рекомендации расширения протокола понимается обмен с Message-ID не равным 0 и, согласно изложенным в **RFC2409** требованиям, после завершения аутентификации фазы 1, сформированный набор данных безопасности (ISAKMP SA) должен удовлетворять следующим обязательным условиям:

- должны быть согласованы алгоритм и параметры шифрования и имитозащиты **ГОСТ 28147-89**;
- должны быть согласованы алгоритм (параметры) хэширования **ГОСТ Р 34.11-94**;
- должен быть согласован ключ SKEYID_e;
- должна быть успешно вычислена и проверена имитовставка пакетов фазы 1 Last-phase-1-ICV;
- должна быть успешно завершена аутентификация сторон, в том числе должны быть рассчитаны AUTH-I и AUTH-R.

Message-Nonce это случайная величина, выработанная одновременно с уникальным идентификатором обменов фазы 2 Message-ID. Для всех пакетов одной последовательности обменов фазы 2 используется один и тот же Message-Nonce.

$$IV = substr(0..7, HASH(Last\_ICV|Message\text{-}ID|Message\text{-}Nonce))$$

8 Шифрование и имитозащита

Поля пакета ISAKMP организуются согласно рекомендациям документа **RFC2408** с вложениями, зашифрованными по **ГОСТ 28147-89**.

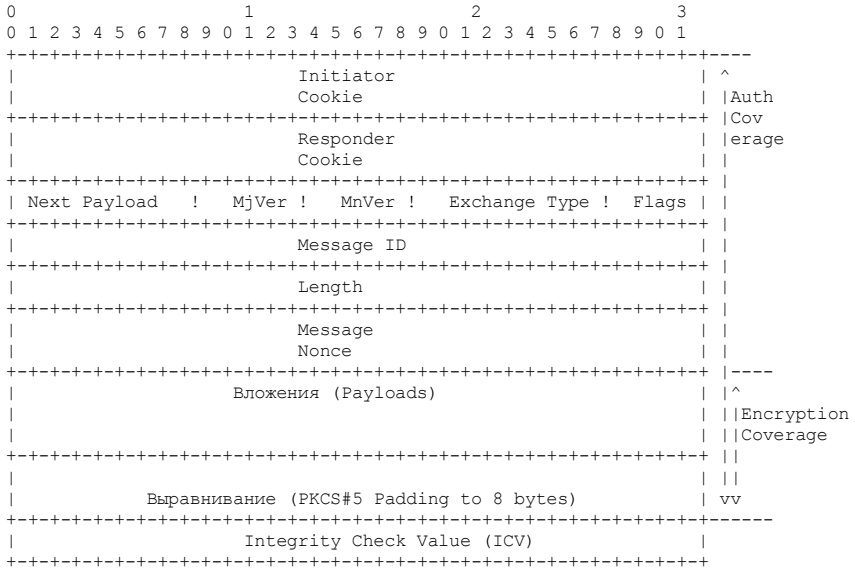

Рисунок 1: Формат зашифрованного по требованиям ГОСТ 28147-89 пакета ISAKMP

Если в заголовке ISAKMP пакета установлен бит E(ncryption Bit), то после его заголовка вставляется поле «Message Nonce», затем производится выравнивание всех его вложений до длины в 8 байт и после этого производится вычисление имитовставки (всего пакета), зашифровываются выравнивание и вложения.

Значение общей длины пакета «Length» в байтах равно сумме следующих величин: длина заголовка пакета «Header» + суммарная длина вложений пакета «Payloads» + длина поля «Message Nonce» (8 байт) + выравнивание (Padding Length) + длина контрольной суммы пакета «ICV» (4 байта). Это значение вычисляется и заполняется до имитозащиты и до шифрования пакета, оно должно содержать значение его общей длины, согласно рекомендациям, изложенным в документе **RFC2408**, раздел 3.1 (см. так же Appendix B, стр. 38, 3 и 4-ый параграф сверху в документе **RFC2409**).

Ключи шифрования – *SK_e* и имитозащиты – *SK_a* вычисляются по формуле:

$$SK\_a = SK\_e = prf(SKEYID\_e, Message\text{-}ID|Message\text{-}Nonce|AUTH\text{-}I|AUTH\text{-}R)$$

Имитовставка вычисляется до зашифрования и только после выравнивания пакета. Ключ *SK_a* используется в режиме *CryptoPro Key Meshing* (id-Gost28147-89-CryptoPro-KeyMeshing). При этом производится сквозное вычисление имитовставки по всей последовательности переданных пакетов с совпадающими значениями полей *Message-ID* и *Message-Nonce*.

$$ICV = gost28147IMIT(0, SK\_a, [пакет\ 1]|[пакет\ 2]...|[текущий\ пакет])$$

Шифрование производится в режиме *encryptCFB* согласно определенному в документе **RFC4357** (см. раздел 1.1.) режиму гаммирования с обратной связью по алгоритму **ГОСТ 28147-89** на ключе *SK_e* и синхропосылке IV (см. в **RFC4357**, раздел 3.2.3). Ключ *SK_e* используется в режиме *CryptoPro Key Meshing*, определенном и описанным там же. При этом смена ключа определяется числом байт, шифруемых ключом с учётом всех обработанных на нем пакетов.

Каждый пакет с одинаковыми значениями в полях *Message-ID*, кроме первого, шифруются с использованием синхропосылки, полученной при обработке предыдущего пакета. Все такие пакеты зашифровываются и расшифровываются последовательно и в порядке очередности их передачи и приёма из канала связи.

При несовпадении рассчитанной имитовставки принятого и расшифрованного пакета со значением поля ICV, получатель МОЖЕТ вернуть состояния ключа шифрования и объекта вычисления имитовставки в состояние, соответствующее состояниям этих объектов до начала обработки пакета.

Для приложений с повышенными требованиями к защите по побочным сигналам РЕКОМЕНДОВАНО обеспечить постоянство времени обработки пакетов ISAKMP/IKE вне зависимости от успешности или неуспешности обработки. Так же, для таких приложений НЕ РЕКОМЕНДОВАНО многократно возвращать состояние ключа шифрования и объекта имитовставки без соответствующих исследований.

9 Методы аутентификации по алгоритмам ГОСТ Р 34.11-94 и ГОСТ Р 34.10-2001

В расширении протокола IKE/GOST вырабатываются согласованные между собой ключи группы *SKEYID*, используемые для выработки ключей в фазах 1 и 2 расширения IKE/GOST:

$$SKEYID\_d = prf(SKEYID, akey \mid CKY\text{-}I \mid CKY\text{-}R \mid 0);$$

$$SKEYID\_a = prf(SKEYID, SKEYID\_d \mid akey \mid CKY\text{-}I \mid CKY\text{-}R \mid 1);$$

$$SKEYID\_e = prf(SKEYID, SKEYID\_a \mid akey \mid CKY\text{-}I \mid CKY\text{-}R \mid 2).$$

На фазе 1 расширения IKE/GOST допускается использование двух методов аутентификации:

1. аутентификация на предварительно распределяемых ключах (GOST-IKE-PSK);
2. аутентификация с использованием ЭЦП (GOST-IKE-SIGNATURE).

В качестве аутентифицирующих элементов при этом используются AUTH-I и AUTH-R и объекты типа "хэш", а именно:

$$HASH\_I = prf(SKEYID, gx\_i \mid gx\_r \mid CKY\text{-}I \mid CKY\text{-}R \mid SAi\_b \mid IDii\_b);$$

$$HASH\_R = prf(SKEYID, gx\_r \mid gx\_i \mid CKY\text{-}R \mid CKY\text{-}I \mid SAi\_b \mid IDir\_b).$$

Аутентификация фазы 1 или завершается успешно, или прерывается при невозможности проведения аутентификации, вызванной ошибкой при проверке любой из величин HASH_I, HASH_R, SIG_I или SIG_R.

При использовании быстрого (агрессивного) режима в методах GOST-IKE-PSK и GOST-IKE-SIGNATURE опциональная возможность протокола (см. **RFC2409)** по передаче последнего (3-го) пакета в открытом виде использоваться **НЕ ДОЛЖНА**. Этот пакет изображается как HDR*.

9.1 Метод аутентификации предварительно распределяемых ключах (GOST-IKE-PSK)

Аутентификация с использованием метода GOST-IKE-PSK требует, чтобы стороны имели предварительно распределённый ключ PSK.

```
Initiator                       Responder
-----------                     -----------
HDR, SA              -->
                     <--        HDR, SA
HDR, KE_i, Ni        -->
                     <--        HDR, KE_r, Nr
HDR*, IDii, HASH_I   -->
                     <--        HDR*, IDir, HASH_R
```

Рисунок 2: Основной режим GOST-IKE-PSK

```
Initiator                        Responder
-----------                      -----------
HDR, SA, KE_i, Ni, IDii    -->
                           <--   HDR, SA, KE_r, Nr, IDir, HASH_R
HDR*, HASH_I               -->
```

Рисунок 3: Быстрый (агрессивный) режим GOST-IKE-PSK

Для данного режима определяются следующие параметры:

$$akey = VKO(x\_i, gx\_r, 1) = VKO(x\_r, gx\_i, 1)$$

$$SKEYID = prf(PSK, Ni\_b \mid Nr\_b).$$

При шифровании ISAKMP вложений согласно требованиям **ГОСТ 28147-89** в фазе 2 должны использоваться следующие параметры (см. пункт 7.2 настоящих рекомендаций).

$$AUTH\text{-}I = HASH(HASH\_I)$$

$$AUTH\text{-}R = HASH(HASH\_R)$$

9.2 Метод аутентификации с использованием ЭЦП (GOST-IKE-SIGNATURE)

Аутентификация с использованием метода *GOST-IKE-SIGNATURE* требует, чтобы стороны имели предварительно распределённый ключ подписи.

При этом обе стороны должны либо найти сертификат противоположной стороны в хранилищах сертификатов на своей стороне, либо запросить сертификат у противоположной стороны запросом CERTREQ. Полученный ими от противоположной стороны сертификат должен быть проверен.

```
Initiator                              Responder
-----------                            -----------
HDR, SA                       -->
                              <--      HDR, SA
HDR, KE_i, Ni, [CERTREQ]      -->
                              <--      HDR, KE_r, Nr, [CERTREQ]
HDR*, IDii, [CERT,] SIG_I     -->
                              <--      HDR*, IDir, [CERT,] SIG_R
```

Рисунок 4: Основной режим GOST-IKE-SIGNATURE

```
Initiator                                   Responder
-----------                                 -----------
HDR, SA,KE_i,Ni,IDii,[CERTREQ]
                                  -->
                                            HDR,SA,KE_r,Nr,[CERTREQ],IDir,
                                  <--       [CERT],SIG_R
HDR*, [CERT], SIG_I               -->
```

Рисунок 5: Быстрый (агрессивный) режим GOST-IKE-SIGNATURE

Для этого режима аутентификации определяются следующие параметры:

$$akey = VKO(x\_i, gx\_r, 1) = VKO(x\_r, gx\_i, 1);$$

$$SKEYID = prf(Ni\_b \mid Nr\_b, akey);$$

$$SIG\_I = Signature(K\_i, HASH\_I);$$

$$SIG\_R = Signature(K\_r, HASH\_R);$$

Форматы представления электронно-цифровых подписей *SIG_I* и *SIG_R* определяются в документе **RFC4490** (см. раздел 3) как последовательности длиной 64 байта.

При шифровании ISAKMP вложений по **ГОСТ 28147-89** в фазе 2 должны использоваться следующие параметры (см. пункт 7.2 настоящих рекомендаций).

$$AUTH\text{-}I = HASH(SIG\_I \mid Cert\_I);$$

$$AUTH\text{-}R = HASH(SIG\_R \mid Cert\_R).$$

При расчёте HASH(SIG_I | Cert_I) и HASH(SIG_R | Cert_R) значение согласованной хэш функции рассчитывается по всему сертификату открытого ключа отправителя или получателя (включая подпись).

10 Обмены фазы 2 расширения протокола IKE/GOST

Каждый последующий обмен данными (в рамках расширенного протокола IKE/GOST), то есть следующий после завершения аутентификации фазы 1, должен обеспечивать защиту пакетов ISAKMP SA на основе *SKEYID_e*. Каждый обмен идентифицируется собственным уникальным Message-ID, обязательно отличным от 0.

Сессия характеризуется использованием следующих режимов:

- Quick Mode;
- Информационный обмен;
- Прочие обмены в рамках ISAKMP SA.

Реализация этих режимов должна удовлетворять требованиям, изложенным в документе **RFC2409**.

Счётчик числа сессий должен увеличиваться обеими сторонами в момент инициирования сессий "Quick Mode", "Информационный обмен" или прочих обменов в рамках обмена данными набора ISAKMP SA.

Сессии этих фаз завершаются либо успешно, либо ошибкой аутентификации при несовпадении значений любой из трёх величин HASH(1), HASH(2), HASH(3).

10.1 Уточнение использования ГОСТ Р 34.11-94 и ГОСТ 34.10-2001 в режиме обмена данными «Quick Mode»

Если при согласовании набора параметров безопасности (ISAKMP SA) было согласовано значение "Disable Non-PFS" (65513) атрибута "PFS Control" (32507), то на фазе 2 согласуются "Quick Mode" только в режиме PFS.

Для каждого SPI вырабатывается ключевой материал (KEYMAT) необходимого размера (см. раздел 5.5 в документе **RFC2409)**, например, для ESP SA по **ГОСТ 28147-89** (см. документ **IETF DRAFT CPESP**):

ESP_GOST-4M-IMIT:	36 байт (Kr_e == K1 и SPI-Auth-Code == substr(0..3, K2));
ESP_GOST-1K-IMIT:	68 байт (Kr_e == K1, Kr_i == K2 и SPI-Auth-Code == substr(0..3, K3)).

Где SPI-Auth-Code может использоваться как неконфиденциальный код аутентификации, применяемый для аудита и/или для предварительного контроля пакетов (соответствия SA, ключей SA и пакета между собой) до расшифрования и контроля имитозащиты.

Все идентификаторы (SPI), порождаемые одной сессией в режиме "Quick Mode", должны иметь уникальные значения, причем обе стороны должны проверить это условие, а их общее количество не должно превышать 100.

11 Дополнительные параметры и атрибуты ISAKMP SA

Для согласования атрибутов методов аутентификации (см. пункт 9 настоящих рекомендаций) при согласовании параметров набора безопасности ISAKMP SA (см. документы **RFC2408** и **RFC2409)** обе стороны ДОЛЖНЫ послать *IKE_GOST vendor ID*, который имеет следующий формат:

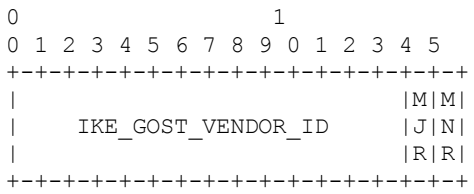

Рисунок 6: IKE_GOST-VENDOR-ID

Где IKE_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 символьной строки "IKE/GOST"), а байты *MJR* и *MNR* соответствуют текущей *major* и *minor* версии преобразований IKE_GOST (т.е. 1 и 1).

Таблица 1: Параметры ISAKMP SA для методов расширения протокола IKE/GOST

Параметр	Атрибут	Формат	Умолчание
алгоритм шифрования	1	B	-
алгоритм хэширования	2	B	-
метод аутентификации IKE	3	B	-
описание группы	4	B	-
тип группы	5	B	-
PFS Control	32507	B	Enable Non-PFS (65512)
Max Messages (SA Life Type)	64506	-	2^{14}

11.1 Алгоритм хэширования ГОСТ Р 34.11-94 и его параметры

Для атрибута "алгоритм хэширования" (2) используется идентификатор хэш-функции **ГОСТ Р 34.11-94**: *GOST_R_3411_94* (<TBD+1>)

11.2 Алгоритм ГОСТ 28147-89 и его параметры

Для атрибута "алгоритм шифрования" (1) используется идентификаторы режимов и параметров:

Таблица 2: Параметры ГОСТ 28147-89 ISAKMP SA

Алгоритм	Режим	Узел замены	Значение
GOST-A-CFB-IMIT	CFB	idGost28147-89-CryptoPro-A- ParamSet	<TBD+2>
GOST-B-CFB-IMIT	CFB	idGost28147-89-CryptoPro-B-ParamSet	<TBD+3>
GOST-C-CFB-IMIT	CFB	id-Gost28147-89-CryptoPro-C-ParamSet	<TBD+4>
GOST-D-CFB-IMIT	CFB	id-Gost28147-89-CryptoPro-D-ParamSet	<TBD+5>

Приложения IPsec удовлетворяющие данному документу ДОЛЖНЫ реализовать алгоритм GOST-B-CFB-IMIT. Для применения в сети Интернет РЕКОМЕНДОВАНО использовать алгоритм GOST-B-CFB-IMIT. Остальные опциональные алгоритмы МОГУТ применяться в сетях со специальными требованиями (например, при использовании многоуровневого шифрования).

11.3 Идентификаторы методов расширения IKE/GOST

Для атрибута "метод аутентификации IKE" (3) используется:

Таблица 3: Параметры ГОСТ 28147-89 ISAKMP SA

Метод	Значение
IKE-GOST-PSK	<TBD+6>
IKE-GOST-SIGNATURE	<TBD+8>

11.4 Описания групп типа VKO GOST R 34.10-2001

Для атрибута "описание группы" (4) используется:

Таблица 4: Группы типа VKO GOST R 34.10-2001

Группа	Параметры	Значение
VKO GOST R 34.10-2001 XchA	id-GostR3410-2001-CryptoPro-XchA-ParamSet+id-GostR34	<TBD+9>
VKO GOST R 34.10-2001 XchB	id-GostR3410-2001-CryptoPro-XchB-ParamSet+id-GostR3410-94	<TBD+10>

Приложения IPsec удовлетворяющие данному документу ДОЛЖНЫ реализовать группу VKO ГОСТ Р 34.10-2001 XchB. Для применения в сети Интернет РЕКОМЕНДУЕТСЯ использовать группу VKO ГОСТ Р 34.10-2001 XchB. Остальные опциональные алгоритмы МОГУТ применяться в сетях со специальными требованиями (например, по производительности).

11.5 Тип VKO GOST R 34.10-2001 для группы IKE

Для атрибута "тип группы" (5) используется:

Таблица 5: типы групп IKE

Тип	Значение
VKO GOST R 34.10-2001	<TBD+11>

11.6 PFS Control

Класс атрибута "PFS Control" (32507), формат: базовый (B), используются значения:

Таблица 6: Параметры ГОСТ 28147-89 ISAKMP SA

PFS Control	Значение
Enable Non-PFS	65512
Disable Non-PFS	65513

11.7 Максимальное число сообщений (Max Messages)

Максимальное значение счётчика числа сессий фазы 2 или равное ему максимальное количество различных значений Message-ID, задаётся значением SA-Life-Duration для типа значения SA-Life-Type=Max-Messages.

Если в режиме Quick Mode использование PFS является обязательным (значение атрибута "PFS Control" (32507) определено как "Disable Non-PFS" (65513)), то максимально количество сессий инициированных с Message-ID не равным 0 НЕ ДОЛЖНО быть более 2^{16}.

Если же использование PFS не является обязательным (значение атрибута "PFS Control" (32507) определено как "Enable Non-PFS" (65512)), то в этом случае количество сессий НЕ ДОЛЖНО превышать 2^{14} , причем в независимости от успешности или не успешности их завершения.

12 Регистрация IANA

IANA выделяет номер хэш функции IKE для использования ГОСТ Р 34.11-94:

<TBD+1> для *GOST_R_34_11_94*.

IANA выделяет четыре номера алгоритмов шифрования IKE для использования ГОСТ 28147-89:

<TBD+2> для GOST-A-CFB-IMIT;

<TBD+3> для GOST-B-CFB-IMIT;

<TBD+4> для GOST-C-CFB-IMIT;

<TBD+5> для GOST-D-CFB-IMIT.

IANA выделяет два номера методов аутентификации IKE для использования ГОСТ 28147-89:

<TBD+6> для IKE-GOST-PSK;

<TBD+8> для IKE-GOST-SIGNATURE.

IANA выделяет два номера описания груп:

<TBD+9> для VKO GOST R 34.10-2001 XchA;

<TBD+10> для VKO GOST R 34.10-2001 XchB.

IANA выделяет номер типа группы:

<TBD+11> для VKO GOST R 34.10-2001.

12.1 Удалить после регистрации в IANA

Пока, предварительные реализации используют следующие приватные номера преобразований:

65501 для GOST_R_34_11_94;

65502 для GOST-A-CFB-IMIT;

65503 для GOST-B-CFB-IMIT;

65504 для GOST-C-CFB-IMIT;

65505 для GOST-D-CFB-IMIT;

65506 для IKE-GOST-PSK;

65508 для IKE-GOST-SIGNATURE;

65509 для VKO GOST R 34.10-2001 XchA;
65510 для VKO GOST R 34.10-2001 XchB;
65511 для VKO GOST R 34.10-2001.

12.2 Регистрации в IANA не подлежит

Используемые в этом документе приватные номера классов и значений:

Таблица 7: IKE_GOST "magic numbers" и приватные значения, описанные в разделе 7.6 и в раздел 7.7.

Класс	Значения	Ссылка	Тип
PFS Control	32507	B	Раздел 7.7

13 Примеры

Представление данных в примерах:

0xNNNN: Представление целого числа в шестнадцатеричной системе счисления, а также представление объктов в форме big-endian;

0xFFFFFFFF FF...: Представление объектов в форме *big-endian*;
BBBBBBBB BB: Представление объектов в сетевой нотации. Числа в *big-endian*. Сетевое представление сложных объектов согласно стандартам их определяющих, в частности, ключей и хэшей согласно **RFC4357**, **RFC4490** и **RFC4490**.

13.1 Примеры значений HMAC_GOSTR3411

Тестовый пример **ГОСТ Р 34.11-94**(text)
Значение хэш-функции для сообщений с тестовыми параметрами алгоритма id-GostR3411-94-TestParamSet (1.2.643.2.2.30.0) согласно **RFC4357** и **ГОСТ Р 34.11-94**.

```
A) Сообщение (ГОСТ Р 34.11-94 п. A.3.1 и
   [ENG-GOSTR341194] п. 7.3.1):

   text (ASCII) =   "This is message, length=32 bytes"
   text (in hex) =  54686973 20697320 6D657373 6167652C
                    206C656E 6774683D 33322062 79746573

   GOSTR3411 =      b1c466d3 7519b82e 8319819f f32595e0
                    47a28cb6 f83eff1c 6916a815 a637fffa


B) Сообщение (ГОСТ Р 34.11-94 п. A.3.2 и
   [ENG-GOSTR341194] п. 7.3.2):

   text (ASCII) =   "Suppose the original message has length = 50 bytes"
   text (in hex) =  53757070 6F736520 74686520 6F726967
                    696E616C 206D6573 73616765 20686173
                    206C656E 67746820 3D203530 20627974
                    6573

   GOSTR3411 =      471aba57 a60a770d 3a761306 35c1fbea
                    4ef14de5 1f78b4ae 57dd893b 62f55208
```

Значение хэш-функции для сообщений с рабочими (применяемыми в IPsec/IKE) параметрами алгоритма хэширования (id-GostR3411-94-CryptoProParamSet или 1.2.643.2.2.30.1) согласно **RFC4357** и **RFC4490**.

```
C) Сообщение:
```

```
text (ASCII) =   "Suppose the original message has length = 50 bytes"
text (in hex) =  53757070 6F736520 74686520 6F726967
                 696E616C 206D6573 73616765 20686173
                 206C656E 67746820 3D203530 20627974
                 6573

GOSTR3411 =      c3730c5c bccacf91 5ac29267 6f21e8bd
                 4ef75331 d9405e5f 1a61dc31 30a65011
```

Пример prf(K, text) (==HMAC_GOSTR3411(K, text))

```
K =              733d2c20 65686573 74746769 79676120
                 626e7373 20657369 326c6568 33206d54  (32 bytes)
text (ASCII) =   "This is message, length=32 bytes"
text (in hex) =  54686973 20697320 6D657373 6167652C
                 206C656E 6774683D 33322062 79746573

HMAC_GOSTR3411 = 4ff66c94 bddaae61 13360514 2b582b9c
                 0f38bbdf f3d7f0ee 6a9c935d 92bfa107
```

13.2 Пример GOST-IKE-PSK

В примерах используются параметры ассоциации безопасности, принятые по умолчанию:

- шифрование обмена ISAKMP с узлом замены id-Gost28147-89-CryptoPro-B-ParamSet в режиме гаммирования с обратной связью и усложнением ключа (см. в **RFC4357,** пункт 3.2.3);
- параметры алгоритма VKO - id-GostR3410-2001-CryptoPro-XchB-ParamSet+id-GostR3411-94.

Время использования PSK: UTC Mon Oct 02 09:11:55 2009.

```
 IKE ph1   Main Mode   PSK Authentication


Initiator PSK
SiteID  11783
SiteNetID Net73
PSK_a D74RLXM4UE1FQC834G3EQBZAZ51WBXAF0VM9VG4RPCDKVEK83ZU9LZ1W
PSK
 e7bcdc1b 0b7e8e97 b76b815a cb23e786 c25bc86f 68de3073 3cbef2a5 a5da578c
 Responder PSK
SiteID  01:23:45:67:89:01:234567890123456789012345678O
SiteNetID Net73
PSK_a BXAF0VM9VG4RPCDKVEK83ZU9LZ1W
PSK
 e7bcdc1b 0b7e8e97 b76b815a cb23e786 c25bc86f 68de3073 3cbef2a5 a5da578c


 Diffi-Hellman keys
 Initiator
```

```
CKY-I
 00000003 00000004
Nonce
 496e6974 4e6f6963 65000000 00000000
x_i 0x
00000000 00000000 00000000 00000000 00000000 00000000 0079654b 74696e49
Ke_i
 20658a0c e2962747 cced0455 ea8e06d2 967469a1 8e5b830b afd120c9 aa463868
 37c30510 b0ab4f98 7ae5fa9d 479b9161 90565496 ac6d31c0 f6956886 c7765789
 Responder
CKY-R
 00000004 00000004
Nonce
 52657370 4e6f6963 65000000 00000000
x_r 0x
00000000 00000000 00000000 00000000 00000000 00000000 0079654b 70736552
Ke_r
 594de6d0 b713b0a4 bb307637 6f7e7285 41c1a2cf 2b30adff 2cd9d973 76578e0e
 3386e708 e8a6aa7c ef6c973e 8eb5ebc3 26485ab7 0027e9ba 7a5672eb 4020a724
akey
 f70c4d6f df22fbc9 5d2dd2ef c7bfdf98 10ba7cc3 6e633540 24085192 05c6cecf


 SKEYID keys
SKEYID
 59ecd564 02d3c736 b1facf69 e5604153 3ee15cbf 9d4321a5 a69e9337 d99dc1b7
SKEYID_d
 3d7f6b8c 153814e0 c35937c7 d9efa605 6273a71b 9416e603 4aafedcd 9f2a0b7a
SKEYID_a
 44343155 65b649a9 7c7a1bb4 0cd77474 0885b031 118a197a c29aaa9e 97a707c0
SKEYID_e
 85ed26bc 6ebda147 749ebb7e b2f7c75f 909de230 2ef0a5cc 2ee6bf8d a812c1e7
SK_a
 9dd0f3e7 5ea8a765 c9b20971 a17c87ea 5222d0d8 6192b1a7 adf9b583 b0bc60ee
SK_e
 9dd0f3e7 5ea8a765 c9b20971 a17c87ea 5222d0d8 6192b1a7 adf9b583 b0bc60ee
IV
 0b115cb4 0a20c9fe


 Authentication
HASH_I
 979c413b 09536510 bfee7ebb 43c15822 44b6a0c1 e52bb373 2f9f6c06 2603d38d
HASH_R
 ccd25ccb 5575865b 8f35c5d9 06a4953b 0de08f8f 53267455 9c486930 4c646e9c
AUTH_I
 97499631 5ba2703d c759cb4b c821d48e c4b25022 387e846d 8c55b9f5 0cca6c3f
AUTH_R
 dbf9a7b9 d47b4d14 833cb187 316a217a 04261a96 4635c6bd 65368614 5417b426
```

```
 Ph 1 Packet 5

Initiator Cookie
 00000003 00000004
Responder Cookie
 00000004 00000004
Flags
 05010001
Messege ID
 00000000
Lenght
 00000060
Messege-Nonce
 00000000 00000000
 PL
Identification
 08001000
 00000000
 00000001 00000001
Hash
 00002400
 979c413b 09536510 bfee7ebb 43c15822 44b6a0c1 e52bb373 2f9f6c06 2603d38d
Padding
 04040404
Cipher input packet
 00000003 00000004 00000004 00000004 05010001 00000000 00000060 00000000
 00000000 08001000 00000000 00000001 00000001 00002400 979c413b 09536510
 bfee7ebb 43c15822 44b6a0c1 e52bb373 2f9f6c06 2603d38d 04040404
Encrypted packet
 00000003 00000004 00000004 00000004 05010001 00000000 00000060 00000000
 00000000 48870189 867183aa e7540fc9 4dd3bbb4 1e08195f fd42ce48 514ca0d7
 2f3427bd 3dfd69ed 8b179611 abce17c4 58c07c71 e90dffdf f382d655 a7f7ca31


 Ph 1 Packet 6

Initiator Cookie
 00000003 00000004
Responder Cookie
 00000004 00000004
Flags
 05010001
Messege ID
 00000000
Lenght
 00000060
Messege-Nonce
 00000000 00000000
 PL
```

```
Identification
 08001000
 00000000
 00000002 00000002
Hash
 00002400
 ccd25ccb 5575865b 8f35c5d9 06a4953b 0de08f8f 53267455 9c486930 4c646e9c
Padding
 04040404
Cipher input packet
 00000003 00000004 00000004 00000004 05010001 00000000 00000060 00000000
 00000000 08001000 00000000 00000002 00000002 00002400 ccd25ccb 5575865b
 8f35c5d9 06a4953b 0de08f8f 53267455 9c486930 4c646e9c 04040404
Encrypted packet
 00000003 00000004 00000004 00000004 05010001 00000000 00000060 00000000
 00000000 d3146e1b 28ffca53 a42acd12 afcd55fb 8a00e051 18b51888 90e2b7c5
9519f417 57deb9bc 8e63ea07 2dc44169 d586c199 5cbb4c17 56ef79a0 7b7e8ee8



 IKE ph2 - Quick Mode   Non PFS


 Quick Mode keys
 Initiator
Nonce
 70325f49 6e697469 61746f72 4e6f6963
Messege Nonce
 70325f4d 5f4e5f00
 Responder
Nonce
 70325f52 6573706f 6e646572 4e6f6963
Messege Nonce
 70325f4d 5f4e5f00
SK_a
 a25d59cc c3b9d40a 8edbdd23 c3652a7e 285f4a37 0f81ce5c d1100e87 a8669908
SK_e
 a25d59cc c3b9d40a 8edbdd23 c3652a7e 285f4a37 0f81ce5c d1100e87 a8669908
IV
 609301fd 6a0a1793

spi Initiator -> Responder
 31323334
protocol
 03
K1
 b63d156f 7aac0dc7 cd915c35 63f61b9d 5c730a74 e331bc8c 3fc24a36 06463893
K2
 cb4e1a7f 2d61710d f264423c ad4384de ce01d676 90556865 f1cb7f7f ab4103c0
K3
```

```
 c4c08a66 c89ce39b e0eb7f2c d6c8af2d a096781c e982deb4 4d78dd68 43188bd7
SPI-Auth-Code K2 = sustr(0..4,K2)
 cb4e1a7f
SPI-Auth-Code K3 = sustr(0..4,K3)
 c4c08a66

spi Responder -> Initiator
 34333231
protocol
 03
K1
 24717b2d fced34ba bf004d4e 15f51253 ad74c519 4819f786 972d3aa7 cf7e5609
K2
 21348380 94c67418 e6a4ad24 e875644f 117f47e7 69c54bf1 b77047c0 eb006c24
K3
 a9491809 7302945a 28818a5a 1f23698d 58f58b26 8b065b23 69648b64 085760d1
SPI-Auth-Code K2 = sustr(0..4,K2)
 21348380
SPI-Auth-Code K3 = sustr(0..4,K3)
 a9491809

 Ph 2 Packet 1

Initiator Cookie
 00000003 00000004
Responder Cookie
 00000004 00000004
Flags
 08010001
Messege ID
 61626364
Lenght
 000000b0
Messege-Nonce
 70325f4d 5f4e5f00
 PL
Hash
 01002400
 918828f7 e54fa536 cb40d539 f6cc3821 52e25380 c597d123 bb51967e beb884d2
Security Association
 0a003000
 00000000
 00000000
 00000c00
 01030402
 00000000
 03000c00
 01fd0000
 00000000
 03000c00
```

```
 01fc0000
 00000000
Nonce
 05001400
 70325f49 6e697469 61746f72 4e6f6963
Identification
 05000c00
 00000000
 01020301
Identification
 00000c00
 00000000
 03027d02
Padding
 08080808 08080808
Cipher input packet
 00000003 00000004 00000004 00000004 08010001 61626364 000000b0 70325f4d
 5f4e5f00 01002400 918828f7 e54fa536 cb40d539 f6cc3821 52e25380 c597d123
 bb51967e beb884d2 0a003000 00000000 00000000 00000c00 01030402 00000000
 03000c00 01fd0000 00000000 03000c00 01fc0000 00000000 05001400 70325f49
 6e697469 61746f72 4e6f6963 05000c00 00000000 01020301 00000c00 00000000
 03027d02 08080808 08080808
Encrypted packet
 00000003 00000004 00000004 00000004 08010001 61626364 000000b0 70325f4d
 5f4e5f00 02238667 aab03043 5b1a4bb7 884e60c5 2941b9c5 15ff7a1d f2608d14
 c807c066 457b3b5e 9b6669d7 a7f1b5f8 32a38267 dc7ef414 d06ca59d 98a465be
 5687fc54 86eb6144 1013fe4c c47a82c5 3257d24d 37271cb6 afe3b9be 6a79310f
 e3fdacbc 1602b5a8 a130baec af8ae4f4 de3b2518 4b9db52a 3c61c482 d0dce5da
 a8edcba3 857a2cff 2a0051a8 f1d42208

 Ph 2 Packet 2

Initiator Cookie
 00000003 00000004
Responder Cookie
 00000004 00000004
Flags
 08010001
Messege ID
 61626364
Lenght
 000000a0
Messege-Nonce
 70325f4d 5f4e5f00
 PL
Hash
 01002400
 61bc0c15 d1690439 0b53bea5 3222597b daa5a75f aaf387a1 c0368ea2 beb8ce1f
Security Association
 0a002400
```

```
 00000000
 00000000
 00000c00
 01030402
 00000000
 03000c00
 01fd0000
 00000000
Nonce
 05001400
 70325f52 6573706f 6e646572 4e6f6963
Identification
 05000c00
 00000000
 01020301
Identification
 00000c00
 00000000
 03027d02
Padding
 04040404
Cipher input packet
 00000003 00000004 00000004 00000004 08010001 61626364 000000a0 70325f4d
 5f4e5f00 01002400 61bc0c15 d1690439 0b53bea5 3222597b daa5a75f aaf387a1
 c0368ea2 beb8ce1f 0a002400 00000000 00000000 00000c00 01030402 00000000
 03000c00 01fd0000 00000000 05001400 70325f52 6573706f 6e646572 4e6f6963
 05000c00 00000000 01020301 00000c00 00000000 03027d02 04040404
Encrypted packet
 00000003 00000004 00000004 00000004 08010001 61626364 000000a0 70325f4d
 5f4e5f00 fb1bab8b ac46efc7 a81c8bca b35afc19 07b4a7b0 c79a91eb 6840a860
 0c90257d 09f6ed37 07dcb089 98625051 8762671a a8be5a02 b27eed4c 90c55cf4
 534cbcff 286f2923 ee9ada8d 3e272b24 8ad8e24f 3d3c4c69 253f8beb e0da0d37
 b0907b7e 6dd978d3 10594bbe c24c3e62 6aa5d694 cec75d2e f8a66dfb 147d2969

 Ph 2 Packet 3

Initiator Cookie
 00000003 00000004
Responder Cookie
 00000004 00000004
Flags
 08010001
Messege ID
 61626364
Lenght
 00000050
Messege-Nonce
 70325f4d 5f4e5f00
 PL
Hash
```

```
 00002400
 c61dfce7 db4220ca ea65be60 02f36a0f 32d226ee faa298ed 79621161 e94acce0
Padding
 04040404
Cipher input packet
 00000003 00000004 00000004 00000004 08010001 61626364 00000050 70325f4d
 5f4e5f00 00002400 c61dfce7 db4220ca ea65be60 02f36a0f 32d226ee faa298ed
 79621161 e94acce0 04040404
Encrypted packet
 00000003 00000004 00000004 00000004 08010001 61626364 00000050 70325f4d
 5f4e5f00 db8106d1 2349fb88 407a692e 772c769e 5e0dcb9a 20ec1f2f 3590a1de
 638850e0 c640348d 3c8b5397 8cc393d8
```

13.3 Тестовые пакеты GOST-IKE-SIGNATURE

В примерах используются параметры ассоциации безопасности, принятые по умолчанию: шифрование обмена ISAKMP с узлом замены *id-Gost28147-89-CryptoPro-B-ParamSet* в режиме гаммирования с обратной связью и усложнением ключа п. 3.2.3 **RFC4357**;

- параметры алгоритма VKO - id-GostR3410-2001-CryptoPro-XchB-ParamSet+id-GostR3411-94.
- Ассиметричные ключи порождены с параметрами *CryptoPro-A-ParamSet*.

```
 IKE ph1   Aggressiv Mode   Signature Authentication


 Initiator Signature key

Signature key K_i 0x
feeed8da 176776d4 8bc20bc2 e3fd8847 a34e8339 b8d3428c f1c06fb1 d424b9e7
Public_i
 a0059433 8c67d7ca 4faa82e2 b08a145f df3cf813 e6d8b944 a62e34e9 756dade9
 c4395772 ee498e3b a52de84e fe153cf6 f1016c70 f7777508 fcd3c7be c6bfd5b4
Random Value k i 0x
00656463 62613938 37363534 33323130 3332315f 525f7965 4b676953 74696e49
 Responder Signature key

Signature key K_r 0x
8ee932fc f8a46163 0dc0a08a c691e20e 7fc40d0e 2881abfe e974ca9a b124cdbf
Public_r
 b1c30537 d435c74a c0a3ba62 e12bdfbc 5e56f8a4 6517b6d5 ea6c5976 63c98dbc
 7fc5712f ac1f201d d7071654 c4ba0fc7 d10d5e66 bec7e981 29cf0230 b3693eba
Random Value k r 0x
00313233 34353637 38396162 63646566 3332315f 525f7965 4b676953 70736552


 Diffi-Hellman keys
 Initiator
```

```
CKY-I
 00000003 00000004
Nonce
 496e6974 4e6f6963 65000000 00000000
x_i 0x
00000000 00000000 00000000 00000000 00000000 00000000 0079654b 74696e49
Ke_i
 20658a0c e2962747 cced0455 ea8e06d2 967469a1 8e5b830b afd120c9 aa463868
 37c30510 b0ab4f98 7ae5fa9d 479b9161 90565496 ac6d31c0 f6956886 c7765789
 Responder
CKY-R
 00000004 00000004
Nonce
 52657370 4e6f6963 65000000 00000000
x_r 0x
00000000 00000000 00000000 00000000 00000000 00000000 0079654b 70736552
Ke_r
 594de6d0 b713b0a4 bb307637 6f7e7285 41c1a2cf 2b30adff 2cd9d973 76578e0e
 3386e708 e8a6aa7c ef6c973e 8eb5ebc3 26485ab7 0027e9ba 7a5672eb 4020a724
akey
 f70c4d6f df22fbc9 5d2dd2ef c7bfdf98 10ba7cc3 6e633540 24085192 05c6cecf


 SKEYID keys
SKEYID
 c6689d94 8bbc4a62 2f2e8663 a96aa0c9 8a0599ee 708a8eb4 c4f51ec5 adfed2f2
SKEYID_d
 9c0af36f 5b1707ce 8b7f0ce4 b8b71170 f4ceb378 c7a1b8e6 b7a60759 fbdd035d
SKEYID_a
 5f458d4b 0d16adab 7352fa07 bf7d7d85 4837851f f9a93e9a bd4e857d f382d800
SKEYID_e
 a72a7573 f63f62fb c60db773 bac6d515 63099a5f 4660a943 d90abd68 87b0166a
SK_a
 a7722c32 c92d69ec 4ba2ec24 873454b3 4fa8106d d9e5b297 cae75893 e369f8d1
SK_e
 a7722c32 c92d69ec 4ba2ec24 873454b3 4fa8106d d9e5b297 cae75893 e369f8d1
IV
 0b115cb4 0a20c9fe


 Authentication
HASH_I
 47684e51 0e4e1dd9 b92f624f 56d3aded b460c470 84e8ff45 2f0a9551 d49349fb
HASH_R
 73904d20 69f296d0 74afb389 08c93473 9366a6f1 b54d43de 1bf1f767 d9181a6b
AUTH_I
 bbc9c7b9 5e84d340 765dc295 e351dbc6 88f2a4be 440e865d a495e982 dd614265
AUTH_R
 63444a68 a6674f23 41a80e73 3f63ccb6 99c6a345 8cdb5a6c 9a62925f 59b8fb76
```

```
 Ph 1 Packet 3

Initiator Cookie
 00000003 00000004
Responder Cookie
 00000004 00000004
Flags
 05010001
Messege ID
 00000000
Lenght
 00000258
Messege-Nonce
 00000000 00000000
 PL
Identification
 06001000
 00000000
 00000001 00000001
Certificate
 0900d701
Certificate type
 04
 308201ce 3082017d a0030201 02020102 30080606 2a850302 02033022 3120301e
 06035504 03131749 50536563 20436f6e 666f726d 69747920 526f6f74 2032301e
 170d3039 31313132 30393334 30315a17 0d343830 31303130 30303030 305a3056
 310b3009 06035504 06130252 55311730 15060355 040a0c0e 4f4f4f20 43727970
 746f2d50 726f312e 302c0603 5504030c 25495053 65632043 6f6e666f 726d6974
 7920456e 64204365 72742066 726f6d20 526f6f74 20323063 301c0606 2a850302
 02133012 06072a85 03020224 0006072a 85030202 1e010343 000440a0 0594338c
 67d7ca4f aa82e2b0 8a145fdf 3cf813e6 d8b944a6 2e34e975 6dade9c4 395772ee
 498e3ba5 2de84efe 153cf6f1 016c70f7 777508fc d3c7bec6 bfd5b4a3 68306630
 0f060355 1d0f0101 ff040503 0307ff80 30130603 551d2504 0c300a06 082b0601
 05050802 02301f06 03551d23 04183016 8014915f dd71bed3 dd9dce22 f9cf09b4
 fc862919 c06d301d 0603551d 0e041604 14c874c3 67957b6b d9720e42 e6a575c9
 e88e0a93 05300806 062a8503 02020303 4100d2e8 b243a051 b53bab3f fd15a4be
 61b9426b f34e2694 b57e9281 fddae4f2 1b087606 f0ac30f1 8054961c 7d859a02
 2cddcfa1 6ef62841 62aa218a b2965619 388d
 00
Signature
 00004400
 6c1928a9 fb891e03 5dcdc936 1fa7a2b0 41c26b94 5198f23d f0782c5a 5007e383
 ec75479a 2b49056f 2007d7d9 238d5f09 b7eed078 7a6fc400 652d33f5 d4fbaa34
Padding
 04040404
Cipher input packet
 00000003 00000004 00000004 00000004 05010001 00000000 00000258 00000000
 00000000 06001000 00000000 00000001 00000001 0900d701 04308201 ce308201
 7da00302 01020201 02300806 062a8503 02020330 22312030 1e060355 04031317
```

```
 49505365 6320436f 6e666f72 6d697479 20526f6f 74203230 1e170d30 39313131
 32303933 3430315a 170d3438 30313031 30303030 30305a30 56310b30 09060355
 04061302 52553117 30150603 55040a0c 0e4f4f4f 20437279 70746f2d 50726f31
 2e302c06 03550403 0c254950 53656320 436f6e66 6f726d69 74792045 6e642043
 65727420 66726f6d 20526f6f 74203230 63301c06 062a8503 02021330 1206072a
 85030202 24000607 2a850302 021e0103 43000440 a0059433 8c67d7ca 4faa82e2
 b08a145f df3cf813 e6d8b944 a62e34e9 756dade9 c4395772 ee498e3b a52de84e
 fe153cf6 f1016c70 f7777508 fcd3c7be c6bfd5b4 a3683066 300f0603 551d0f01
 01ff0405 030307ff 80301306 03551d25 040c300a 06082b06 01050508 0202301f
 0603551d 23041830 16801491 5fdd71be d3dd9dce 22f9cf09 b4fc8629 19c06d30
 1d060355 1d0e0416 0414c874 c367957b 6bd9720e 42e6a575 c9e88e0a 93053008
 06062a85 03020203 034100d2 e8b243a0 51b53bab 3ffd15a4 be61b942 6bf34e26
 94b57e92 81fddae4 f21b0876 06f0ac30 f1805496 1c7d859a 022cddcf a16ef628
 4162aa21 8ab29656 19388d00 00004400 6c1928a9 fb891e03 5dcdc936 1fa7a2b0
 41c26b94 5198f23d f0782c5a 5007e383 ec75479a 2b49056f 2007d7d9 238d5f09
 b7eed078 7a6fc400 652d33f5 d4fbaa34 04040404
Encrypted packet
 00000003 00000004 00000004 00000004 05010001 00000000 00000258 00000000
 00000000 f0b02f0d fa3f999a f09f833f f465f09f 02b9924a a9dac76d 6dc830c0
 f42f7054 e1006f8c e6dc52b6 31cea21b 2420c3cf 6c05a305 8ff164bf be5d5b6c
 0f2a7703 674b13b8 a937c024 09cc6956 bce0b3ac 44a16771 d3eabb90 16c69473
 3068583e 0b4bfce0 1d48fb4a 4c80a101 bd9884ac daef1849 6a2640a7 d2a6fdb9
 324dd071 880c9b19 721fea17 0c800f05 01fd66fb dfadd392 e8a195fc d210b5d6
 702236f6 6d396ba3 aec96658 1a9f234e 273e24d2 f0cf9f41 17229bd6 b8b37e4e
 9c867943 518e819c 0754c506 e873e02e 7b0491b3 814220d2 9a610882 c283d71a
 1a658ded 7746f368 f7926020 ae50e01d fedb7025 5404871f 5f0c1c73 53e728e9
 0a707677 a8cb3f37 2686b8ed 173cea11 3d4ec375 c14b6e1f 23a3b853 bd1f8213
 dc63f7f4 10b8724f 0b2e4dff a4fc4f68 d1ed4cb9 f2c5a87a cd78d37b 4addb113
 a33e4c02 a3273747 2e0ddf65 e953d19a 9279591b 474b4ba1 f9c0accb 49563bdf
 2d05d6bc 862d8a62 a8787d49 d45c2e75 abd9fc3a 48fa6229 8f225eeb b17c04d3
 04ce71aa dc165f71 28fbe31b 7099c642 fcb2ab75 fc61eb16 9029cbd1 2e0fe446
 d2d42882 ae8a3daf 1d19e607 94934fbc 6e76c69a f510a8c0 ff5aefe7 d9054127
 eb0bbcec 9c82757c 0159fd70 679cb684 afe79569 34a58e6f 385150d7 5b092785
 68852993 6b979152 edf48782 380de0da 48e19adf 83945274 a61317d6 c56b5fed
 5c785ed1 c14b20a4 770d5e08 ab777802 5db507f4 a882454e 0317a58f b432993e
     60537487 2c39ace1 b7c161ee 9fba90f5 e36efc62 16f10809


 IKE ph2 - Quick Mode   PFS


 Quick Mode keys
 Initiator
Nonce
 70325f49 6e69744e 6f696365 50465300
Messege Nonce
 70325f4d 5f4e5f50
x_i 0x
00000000 00000000 00000000 00000000 00000053 46507965 4b74696e 495f3270
KE_i
```

```
 630db614 829adc6b 1b240da6 51b52df5 87aaa464 dfe9b526 77f1dc5e 887f5696
 1fc6b090 83c9e0f3 94043040 ad3d6acd 7b85cb46 a10ef102 e31639e3 5bc58b29
 Responder
Nonce
 70325f52 6573704e 6f696365 50465300
Messege Nonce
 70325f4d 5f4e5f50
x_r 0x
00000000 00000000 00000000 00000000 00000053 46507965 4b707365 525f3270
KE_r
 806cfe17 8e1b9679 b5d7715e ef9faeb2 6fa6fd38 a0ce54cb d719b1dd c8bb7f51
 38b6728d a99c0b33 80aa8829 4966a076 cd08cbc2 5564fb65 2aba828c dec26529

 gm_ir
 21524616 69319ed8 baac8887 516ed843 44b0e973 bc9b4f8d 6463b339 f6182869
SK_a
 711a3d0c 1cf0ad46 8124c998 6266e214 a303dc8e af227c44 52f0b7cd 53710911
SK_e
 711a3d0c 1cf0ad46 8124c998 6266e214 a303dc8e af227c44 52f0b7cd 53710911
IV
 0d556677 b80e9941

spi Initiator -> Responder
 31323334
protocol
 02
K1
 9df29d9c 0c016125 43dfc664 682222e9 d9b16b1d 7cfd53b0 f9c740fe adfb4834
K2
 c613c524 505549fa f4146e81 649c2e43 baa4155f b69bbd0e b5460f9c ebbd32bd

spi Responder -> Initiator
 34333231
protocol
 02
K1
 4b2ddcdc 8012bdb5 95663079 0991c532 4a900d46 c1ae2245 97aa12c8 4ffdf992
K2
 c8e9f8d1 4f932289 fb87d169 f923cf5f f446b764 0c2ab3ad 1ad46edf d85efe66

 Ph 2 Packet 1

Initiator Cookie
 00000003 00000004
Responder Cookie
 00000004 00000004
Flags
 08010001
Messege ID
 61626364
```

```
Lenght
 000000f0
Messege-Nonce
 70325f4d 5f4e5f50
 PL
Hash
 01002400
 8e1df1c8 01709834 ed4c316c 94f27ccc 65c0eaeb ac8bd5f9 cc15ca3c 381e8c40
Security Association
 0a003000
 00000000
 00000000
 00000c00
 01030402
 00000000
 03000c00
 01fd0000
 00000000
 03000c00
 01fc0000
 00000000
Nonce
 04001400
 70325f49 6e69744e 6f696365 50465300
Key Exchange
 05004400
 630db614 829adc6b 1b240da6 51b52df5 87aaa464 dfe9b526 77f1dc5e 887f5696
 1fc6b090 83c9e0f3 94043040 ad3d6acd 7b85cb46 a10ef102 e31639e3 5bc58b29
Identification
 05000c00
 00000000
 01020301
Identification
 00000c00
 00000000
 03027d02
Padding
 04040404
Cipher input packet
 00000003 00000004 00000004 00000004 08010001 61626364 000000f0 70325f4d
 5f4e5f50 01002400 8e1df1c8 01709834 ed4c316c 94f27ccc 65c0eaeb ac8bd5f9
 cc15ca3c 381e8c40 0a003000 00000000 00000000 00000c00 01030402 00000000
 03000c00 01fd0000 00000000 03000c00 01fc0000 00000000 04001400 70325f49
 6e69744e 6f696365 50465300 05004400 630db614 829adc6b 1b240da6 51b52df5
 87aaa464 dfe9b526 77f1dc5e 887f5696 1fc6b090 83c9e0f3 94043040 ad3d6acd
 7b85cb46 a10ef102 e31639e3 5bc58b29 05000c00 00000000 01020301 00000c00
 00000000 03027d02 04040404
Encrypted packet
 00000003 00000004 00000004 00000004 08010001 61626364 000000f0 70325f4d
 5f4e5f50 bbfd4d58 3adbc856 628097bc 3a5b98a8 b893c3cd b6d643a5 f8902455
```

```
 dd361a1a a59ec2ca c5ca9a98 057148c3 47245d6d 54dedb92 acbc4efa 33cf0986
 c8da0de5 7f376cdd d6aa2b63 f5e96539 9d88f510 ad319f1a 4d16118c 2261e5fa
 9109dfa2 6af6dfc3 3b5c9b7e faf61f55 1a455cfd 268541b4 24636509 ca1879f0
 631cfebe 046ad11f c6c6380d 5d8aa385 2cb28efa 0e6dc10b 16d1d2f0 48167f1c
 08a7928c 74884d12 da82345e 75623b2a 23b9aa1b 87a0659f 43be7271 499452a0
 026cdd64 ada63fb4 f69c7e86 bcb728a6

 Ph 2 Packet 2

Initiator Cookie
 00000003 00000004
Responder Cookie
 00000004 00000004
Flags
 08010001
Messege ID
 61626364
Lenght
 000000e8
Messege-Nonce
 70325f4d 5f4e5f50
 PL
Hash
 01002400
 484cd087 f70cc1e2 40caf531 780eec2a 165da91d 8da643d9 803e2647 a8102018
Security Association
 0a002400
 00000000
 00000000
 00000c00
 01030402
 00000000
 03000c00
 01fd0000
 00000000
Nonce
 04001400
 70325f52 6573704e 6f696365 50465300
Key Exchange
 05004400
 806cfe17 8e1b9679 b5d7715e ef9faeb2 6fa6fd38 a0ce54cb d719b1dd c8bb7f51
 38b6728d a99c0b33 80aa8829 4966a076 cd08cbc2 5564fb65 2aba828c dec26529
Identification
 05000c00
 00000000
 01020301
Identification
 00000c00
 00000000
 03027d02
```

```
Padding
 08080808 08080808
Cipher input packet
 00000003 00000004 00000004 00000004 08010001 61626364 000000e8 70325f4d
 5f4e5f50 01002400 484cd087 f70cc1e2 40caf531 780eec2a 165da91d 8da643d9
 803e2647 a8102018 0a002400 00000000 00000000 00000c00 01030402 00000000
 03000c00 01fd0000 00000000 04001400 70325f52 6573704e 6f696365 50465300
 05004400 806cfe17 8e1b9679 b5d7715e ef9faeb2 6fa6fd38 a0ce54cb d719b1dd
 c8bb7f51 38b6728d a99c0b33 80aa8829 4966a076 cd08cbc2 5564fb65 2aba828c
 dec26529 05000c00 00000000 01020301 00000c00 00000000 03027d02 08080808
 08080808
Encrypted packet
 00000003 00000004 00000004 00000004 08010001 61626364 000000e8 70325f4d
 5f4e5f50 74043cef eadc368d a09419bc ed7b5cdf 477aba34 f441d562 1107bacf
 4e8fcd1a 594c83a3 019645c2 15bb1b5d f54639f0 df763861 ef4de755 5d2dda55
 71c649c0 35e4b612 c9920441 21fdc01d b217cf2f 49c7516f 4d809e06 e260662f
 891e244a d299cbd5 f26498ba 20296aa6 cf4782bc 7bfd6425 e622b552 9ff33ec6
 0eec9856 bfde9147 5d61a93b 5c852ac8 11c55963 87c25e16 526f6aaf acce6c5a
 674203c6 20b7fae9 8601f483 c860595f 0c51827a 16763fe0 1b185f5b 5ea1784c
 4c5d2487 c9bac24b

 Ph 2 Packet 3

Initiator Cookie
 00000003 00000004
Responder Cookie
 00000004 00000004
Flags
 08010001
Messege ID
 61626364
Lenght
 00000050
Messege-Nonce
 70325f4d 5f4e5f50
 PL
Hash
 00002400
 1c12e52a 0a40adb1 7780cd16 2b7130b1 46649e71 3e785af9 ef7c8188 8a9f3ac7
Padding
 04040404
Cipher input packet
 00000003 00000004 00000004 00000004 08010001 61626364 00000050 70325f4d
 5f4e5f50 00002400 1c12e52a 0a40adb1 7780cd16 2b7130b1 46649e71 3e785af9
 ef7c8188 8a9f3ac7 04040404
Encrypted packet
 00000003 00000004 00000004 00000004 08010001 61626364 00000050 70325f4d
 5f4e5f50 449623ee 476d7fef 7332b1e5 4f6495b3 5cfbb978 e2cff785 7b61f3d0
 3f3f600e 68b42f8b c9476afd 81fbe91a
```

Приложение А : Применение

Отличительные особенности алгоритмов и режимов аутентификации расширения в расширении протокола IKE/GOST

IKE-GOST-PSK:	Допускает выбор алгоритма аутентификации. Характеризуется очень высокой производительностью, но предъявляет высокие требования к управлению ключами. Применим для аутентификации в некрупных сетях равноправных шлюзов.
IKE-GOST-SIGNATURE:	Характеризуется низкой производительностью, но обладает несколько более высокой устойчивостью к DoS атакам ложных соединений в основном (*main*) режиме.
Выбор режима алгоритма аутентификации:	Основной режим (*Main*): характеризуется низкой производительностью, но одновременно обладает высокой устойчивостью к DoS атакам в Интернет. Для алгоритма IKE-GOST-PSK обеспечивается конфиденциальность идентификационной информации. Быстрый режим (Aggressive): характеризуется высокой производительностью, устойчивостью к DoS атакам при использовании радиоканалов (только при достаточной производительности процессора).

Особенности борьбы с DoS атаками при использовании расширения протокола IKE/GOST:

в Интернет:	Нарушитель не имеет возможности перехватывать трафик, не имеет достаточных вычислительных мощностей, но имеет возможность посылать большое количество пакетов (первых пакетов). Блокируется механизмом контроля CKI-I/R протокола ISAKMP.
при установлении ложных соединений:	Нарушитель не имеет возможности перехватывать трафик, но имеет возможность устанавливать большое количество соединений (первый, второй и третий пакет). Блокируется механизмом непосредственно механизмом аутентификации (распределённые DoS атаки).
при использовании радиоканалов:	Нарушитель имеет возможность как перехватывать трафик, так и посылать пакеты, но не имеет возможности искажать пакеты в канале. Блокируется механизмом имитозащиты при условии достаточной производительности процессора.

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-rc 2009-02-15 ЛСЕ

Учёт изменений по окончании предварительного криптографического анализа;

Изменил выравнивание пакета, с "NoName" по модулю 4 байта, на PKCS#5 по модулю 8 байт;

00-rd 2009-03-01 ЛСЕ

Описание PDF, XML Validated;

Подготовлено для согласования с Владимиром Олеговичем Поповым;

Вставлено забытая ссылка на UKM из VKOGOSTR34.10-2001. В алгоритме GOST-IKE-KEYEXCHANGE добавлено использование CKI-I/R в качестве UKM.

00-re 2009-03-16 ЛСЕ

Исправлены нестандартные по RFC 2119 термины;

Уточнено использование encryptECB(K, D).

00-rf 2009-03-16 ЛСЕ

Учёл требования на СКЗИ "КриптоПро CSP".

00-rg 2009-03-01 ЛСЕ

Удалён алгоритм GOST-IKE-KEYEXCHANGE.

00-rh 2009-07-10 ЛСЕ

Уточнено описание по выравниванию PKCS#5.

00-ri 2009-03-16 ЛСЕ

Удалены метки конфиденциальности и Copyright;

Добавлены рыбы тестовых примеров;

Вставлен редактор английского перевода;

00-rj 2009-12-01 ПВО&ЛСЕ

Внесено описание хэш-функции ГОСТР34.11-94, что бы убрать нормативную ссылку на [draft.СРАН];

Исправлены формулы вычисления SK_a и SK_e;

Исправлена формула вычисления SKEYID для GOST-IKE-SIGNATURE;

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 2010-10-18 ПВО&ЛСЕ

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

Вставлены информативные ссылки на RFC 5830, 5831 и 5832.

00-rn 2011-04-13 ПВО&ЛСЕ

Учтены замечания Владимира Подобаева, ООО "Фактор-ТС":

- в примерах вставлено значение "protocol";
- в примерах вставлены значения случайного числа k при расчёте ЭЦП по ГОСТР34.10-2001;
- исправлена опечатка с Cert_I/Cert_R и уточнено их использование;
- уточнёно, что до завершения аутентификации шифрование .

Учтены технические замечания Федотова Андрея Владимировича, ООО "Фактор-ТС" и Смыслова Валерия Анатольевича, ОАО "ЭЛВИС-ПЛЮС".

Информативные ссылка draft-ietf-ipsecme-roadmap заменена на RFC 6071.

00-ro 2011-05-21 ПВО&ЛСЕ

Учтено замечание Владимира Подобаева, ООО "Фактор-ТС", о Cert_I/Cert_R.

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

- Переименован SPIcookie в SPI-Auth-Code;
- Расширено определение обменов фазы 2 и уточнён порядок увеличения счётчика M-ID;
- Уточнено определение параметра Max Messages и значение его по умолчанию;
- Уточнено использование параметров ГОСТ28147-89 и групп по ГОСТР34.10-2001 с целью уменьшения различных предложений параметров SA;

00-rp 2011-11-08 ПВО&ЛСЕ

Учтены замечания Владимира Подобаева, ООО "Фактор-ТС":

- О Cert_I/Cert_R;
- Исправлена ошибка примера: Key Meshing;
- Исправлена ошибка примера: порядок байт SIG_I и SIG_R;
- В примере указаны параметры ГОСТ28147-89 и группы по ГОСТР34.10-2001.
- В примерах "0x" дано на отдельной строке, а не рядом с именем сущности ("0x" не получается дать в тоже строке, где даны значащие цифры, т.к. получается слишком длинная строка);

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

- Переименован SPIcookie в SPI-Auth-Code;
- Расширено определение обменов фазы 2 и уточнён порядок увеличения счётчика M-ID;
- Уточнено определение параметра Max Messages и значение его по умолчанию;
- Уточнено использование параметров ГОСТ28147-89 и групп по ГОСТР34.10-2001 с целью уменьшения различных предложений параметров SA;

Убрано обсуждение шифрования информационных сообщений до завершения фазы 1, как противоречащее RFC 2409.

Переупорядочены ссылки, ссылки на RFC 4301 и RFC 4303 перенесены в информативные, а так же убраны неиспользуемые ссылки [ROADMAP], [ESN], [JUMBO] и [RFC4134].

00-rq 2012-02-02 ПВО&ЛСЕ

Учли замечания представителей рецензентов от ТК26 в части определения Message-Nonce, порядка проверки имитовставки, VKO(x_i, gx_r, 1) и текстового представления PSK.

Учтено замечание ООО "Фактор-ТС" в части соответствия примеров AUTH-I/AUTH-R

00-rr 2012-04-24 ПВО

Учтено замечание Подобаева Владимира Николаевича, ООО "Фактор-ТС"

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: Будет удалён раздел текстового PSK