ТК26, рабочая группа IPsec
Предварительный документ
<rus-fedchenko-cpesp-ipsecme-gost-00-rm>
Предполагаемый статус: Информационный
Действителен: Август 2010

С.Е. Леонтьев, Editor
М.В. Павлов, Editor
CRYPTO-PRO
А.А. Федченко, Editor
S-Terra
December 2009

Комбинированный алгоритм шифрования вложений IPsec (ESP) на основе ГОСТ 28147-89

rus-fedchenko-cpesp-ipsecme-gost-00-rm

Статус документа

[TODO: а надо ли в документе ТК26 авторам предоставлять права, и если надо, то как именно?]

Фактом передачи предварительного документа в ТК26, каждый автор соглашается с неэксклюзивным предоставлением IPR для ТК26, аналогично положениям стандарта Интернет IETF BCP 79.

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

Данный предварительный документ действителен в течении максимум девяти месяцев, и может быть в любое время изменён, заменён на другой или отозван в любое время. При цитировании или ссылке на него из других документов следует ставить отметку, что “документ готовится к публикации”.

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

Этот предварительный документ действителен до Август 2010.

Аннотация

Это предварительный документ на русском языке предназначен для обеспечения совместимости реализаций IPsec ESP российских производителей, а так же для создания проекта документа IETF.

Этот документ описывает соглашения по использованию алгоритма ГОСТ 28147-89 при шифровании вложений IPsec (ESP). Протокол ESP используется для обеспечения конфиденциальности, целостности и аутентичности содержимого IP пакетов.

Лист изменений

Предназначено для подготовки I-D и его поддержки. Убрать в момент публикации окончательно документа ТК26 и/или RFC.

00-ra 2008-07-26 ЛСЕ	"Рыба", только оглавление и ссылки;
00-rb 2008-08-14 ЛСЕ	Терминология ESP;

XML to PDF by RenderX XEP XSL-FO Formatter, visit us at http://www.renderx.com/

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 КВ и выше (ESP_GOST-1K-IMIT). Учтено замечание Смыслова Валерия Анатольевича, ОАО "ЭЛВИС-ПЛЮС" об об опциональности использования SPIcookie.

XML to PDF by RenderX XEP XSL-FO Formatter, visit us at http://www.renderx.com/

Авторские замечание

Предназначено для подготовки I-D и его поддержки. Убрать в момент публикации окончательно документа ТК26 и/или RFC.

Описание формата проекта RFC в XML (Internet-Draft или I-D), методы просмотра, форматирования и редактирования смотри [draft.RFC2629bis] [RFC2629] [XML2RFC] [ID-Checklist] [xml2rfc-validator]

Текущий регистр [DOI] <http://www.iana.org/assignments/isakmp-registry> [isakmp-registry]

Текущий регистр [IKE] <http://www.iana.org/assignments/ipsec-registry> [ipsec-registry]

Документ должен нормально просматриваться в любом достаточно современном browser-е при активном подключении к сети Интернет.

Извините за язык "падонков", но мы используем шаблон [XML2RFC] на английском языке, хотя и пишем по-русски.

При преобразовании в PDF следует настроить FO процессор на использование встраиваемых русских шрифтов, см. Кратчайший путь к DocBook [1].

В документе используются применяемые в IETF расширения " Draft HTML and PDF from XML source [2]", поэтому после перевода на английский надо будет применять XSLT преобразование "xml2rfc\rfc2629xslt\clean-for-DTD.xslt" перед вызовом "xml2rfc\xml2rfc.tcl" для получения текстового файла.

[1] http://docbook.ru/doc/sw/foproc.html

[2] http://greenbytes.de/tech/webdav/rfc2629xslt/rfc2629xslt.html

XML to PDF by RenderX XEP XSL-FO Formatter, visit us at http://www.renderx.com/

Содержание

XML to PDF by RenderX XEP XSL-FO Formatter, visit us at http://www.renderx.com/

1. Введение

Данный документ определяет следующие преобразования [ESP]:

- комбинированный алгоритм ESP_GOST-SIMPLE-IMIT;
- комбинированный алгоритм ESP_GOST-4M-IMIT;
- комбинированный алгоритм ESP_GOST-1K-IMIT.

Протокол [ESP] используется в архитектуре IPsec [ARCH] для обеспечения конфиденциальности, целостности и аутентичности содержимого IP пакетов. Этот документ описывает использование ГОСТ 28147-89 [GOST28147], но не определяет сам криптографический алгоритм и форматы представления криптографических типов данных. Алгоритмы описываются соответствующими национальными стандартами, а представление данных и параметров соответствует следующими документам IETF [CPALGS] [CPCMS].

ESP вложения обрабатываются в рамках IPsec SA, параметры которой МОГУТ интерпретироваться согласно [DOI]. Этот документ описывает так же дополнительные идентификаторы расширяющие [DOI].

XML to PDF by RenderX XEP XSL-FO Formatter, visit us at http://www.renderx.com/

2. Терминология

Термины "ДОЛЖНО", "ДОЛЖНА", "ДОЛЖНЫ", "ДОЛЖЕН" (MUST, REQUIRED, SHALL), "НЕ ДОЛЖЕН", "НЕ ДОЛЖНЫ" (MUST NOT, SHALL NOT), "РЕКОМЕНДОВАНО" (SHOULD, RECOMMENDED), "НЕ РЕКОМЕНДОВАНО" (SHOULD NOT, NOT RECOMMENDED), "МОГУТ", "МОЖЕТ" (MAY, OPTIONAL) в рамках этого документа ДОЛЖНЫ интерпретироваться в соответствии с RFC 2119 [KEYWORDS].

В документе используются термины и определения стандартов IPsec [ARCH] и [ESP], ниже приводятся только дополнительные определения.

encryptCNT(IV, K, D):	шифрование ГОСТ 28147-89 в режиме "гаммирования" на ключе K данных D с начальным вектором IV (Section 1.1 of [CPALGS], [GOST28147], [Schneier95]). Узел замены определяется Раздел 5.1;
decryptCNT(IV, K, D):	расшифрование ГОСТ 28147-89 в режиме "гаммирования" на ключе K данных D с начальным вектором IV (Section 1.1 of [CPALGS], [GOST28147], [Schneier95]). Узел замены определяется Раздел 5.1;
Divers(K,D):	алгоритм диверсификации ключа K по данным D (Section 7 of [CPALGS]). Узел замены определяется Раздел 5.1. 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 (Section 1.1 of [CPALGS], [GOST28147], описание и пример сетевого представления результата приведён [CPCMS], Section 9.2, 9.3). Узел замены согласуется Раздел 5.1;
Seq#:	64-битный номер пакета, если [ESN] не согласован, то значение Seq# всегда принадлежит диапазону 1..2^32-1;
IV(Seq#):	синхропосылка пакета Seq#;
Kc_e(Seq#):	ключ комбинированного алгоритма шифрования пакета Seq#;
Kc_i(Seq#):	ключ комбинированного алгоритма имитозащиты пакета Seq#;
Kr_e:	корневой ключ шифрования SA;
Kr_i:	корневой ключ имитозащиты SA;
KeyMeshing:	Используемый алгоритмы усложнения ключа, описан в Section 2.3 of [CPALGS];
Seq#h:	старшая часть Seq#;
Seq#l:	младшая часть Seq#;
SPIcookie:	величина, вычисляемая в рамках ISAKMP SA или иной не-IPsec SA, например в "Quick Mode" фазы 2 протокола [draft.CPIKE].
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;
пакет с искажённым Seq#:	ESP вложение или AH пакет, для которого не прошёл предварительный контроль SPI и Seq#;

XML to PDF by RenderX XEP XSL-FO Formatter, visit us at http://www.renderx.com/

искажённый пакет:	ESP вложение или AH пакет, для которого вычисленное значение ICV не совпало с переданным значением;

XML to PDF by RenderX XEP XSL-FO Formatter, visit us at http://www.renderx.com/

3. Состав ESP_GOST SA

В рамках ISAKMP SA [draft.CPIKE] или иной не-IPsec SA согласуются для данной IPsec SA, как минимум, следующие компоненты:

- 256-бит симметричный ключ Kr_e;
- 256-бит симметричный ключ Kr_i;
- 32-х битная случайная величина SPIcookie [rfc.comment.1];
- параметры ГОСТ 28147-89;
- максимальный объём данных SA в байтах (Lifetime SA, Kbytes);
- максимальное время жизни SA в секундах (Lifetime SA, sec);
- максимальное значение счётчика искажённых пакетов.

[rfc.comment.1] в ESP_GOST-SIMPLE-IMIT SPIcookie не используется, т.к. общее количество пакетов в SA этого типа ДОЛЖНО быть ограничено числом порядка 10^5 пакетов

XML to PDF by RenderX XEP XSL-FO Formatter, visit us at http://www.renderx.com/

4. Преобразования

Вложение ESP пакета должно соответствовать Section 2 of [ESP] для комбинированного алгоритма со следующими параметрами:

- IV передаётся в пакете и имеет размер 8 байт;
- ESP вложение выравнивается на границу 8 байт;
- Если согласовано ESN, то Seq#h в пакете не передаётся;
- Явного выравнивания ICV не производится [rfc.comment.2];
- ICV передаётся в пакете, имеет размер 4 или 8 байт .

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

4.1 Обработка исходящих пакетов

Порядок обработки исходящих пакетов ДОЛЖЕН соответствовать Section 3.3 of [ESP] со следующими уточнениями:

- Дополнительно к проверкам Section 3.3.1 of [ESP] РЕКОМЕНДОВАНО проверить длину ESP вложения на соответствие параметрам SA; [rfc.comment.3]
- Здесь и далее (xxx) означает использование величины xxx в LITTLE ENDIAN порядке байт, xxx означает использование xxx в сетевом порядке байт. Имитовставка в преобразованиях вырабатывается по формуле:

  ICV = gost28147IMIT(0, Kc_i(Seq#), SPI|Seq#l|IV|..|Next Header[|Seq#h]);
- Шифрование в преобразованиях осуществляется в режиме усложнения ключа KeyMeshing, который определяется конкретным преобразованием, по формуле:

  encryptCNT(IV(Seq#), Kc_e(Seq#), Payload data|...|Next Header);
- Отправителю РЕКОМЕНДОВАНО увеличить счётчик текущего объём данных SA в байтах (Lifetime SA, Kbytes) и сравнить его с максимальным. При его превышении РЕКОМЕНДОВАНО заблокировать дальнейшую работу SA. [rfc.comment.4]

4.2 Обработка входящих пакетов

Порядок обработки входящих пакетов ДОЛЖЕН соответствовать Section 3.4 of [ESP] со следующими уточнениями:

- Дополнительно к проверкам Section 3.4.2 of [ESP], РЕКОМЕНДОВАНО проверить длину ESP вложения на соответствие параметрам SA; [rfc.comment.5]
- Дополнительно к проверкам Section 3.4.3 of [ESP], для преобразований ESP_GOST-4M-IMIT и ESP_GOST-1K-IMIT ДОЛЖНА быть выполнена проверка IV (IV.IVCounter). Для ESP_GOST-SIMPLE-IMIT МОЖЕТ быть выполнена проверка IV на уникальность; [rfc.comment.6]
- Получателю РЕКОМЕНДОВАНО увеличить счётчик текущего объём данных SA в байтах (Lifetime SA, Kbytes) и сравнить его с максимальным. SA в байтах (Lifetime SA, Kbytes) и сравнить его с

[rfc.comment.2] оно не требуется, т.к. реально передаваемые данные уже выровнены. В результате, в случае ECN, мы при расчёте имитовставки будем всегда добавлять к Seq#h ещё 4 байта нулей, а т.к. Seq#h реально не передаётся, это нормально

[rfc.comment.3] Аудит - "No valid Security Association exists"

[rfc.comment.4] Аудит - "Attempt to transmit a packet that would result in Sequence Number overflow"

[rfc.comment.5] Аудит - "No valid Security Association exists"

[rfc.comment.6] Аудит - "The received packet fails the anti-replay checks"

XML to PDF by RenderX XEP XSL-FO Formatter, visit us at http://www.renderx.com/

максимальным. При его превышении РЕКОМЕНДОВАНО заблокировать дальнейшую работу SA; [rfc.comment.7]

- Расшифрование в преобразованиях осуществляется в режиме усложнения ключа KeyMeshing, который определяется конкретным преобразованием, по формуле:

  decryptCNT(IV(Seq#), Kc_e(Seq#), Payload data|...|Next Header);

- Имитовставка в преобразованиях проверяется по формуле:

  ICVchk = gost28147IMIT(0, Kc_i(Seq#), SPI|Seq#l|IV|..|Next Header[|Seq#h]);

- Если ICV != ICVchk, то получателю РЕКОМЕНДОВАНО увеличить счётчик искажённых пакетов SA и сравнить его с максимальным. При его превышении РЕКОМЕНДОВАНО заблокировать дальнейшую работу SA; [rfc.comment.8]

4.3 Вычисление MTU

При вычислении MTU следует руководствоваться правилами выравнивания Section 2 of [ESP] со значением модуля 8 байт, и с учётом фиксированного добавленного размера 12 байт для IV (8 байт) и ICV (4 байта).

4.4 Преобразование ESP_GOST-SIMPLE-IMIT

В преобразовании ESP_GOST-SIMPLE-IMIT используются:

IV(Seq#l) - случайные и уникальные 8 байт, получатель МОЖЕТ проверять их уникальность;

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

Kc_e(Seq#) = Kr_e;

Kc_i(Seq#) = Kr_i;

Согласованный объём данных SA НЕ ДОЛЖЕН превышать 4 Мбайт.

Согласованный размер ESP вложений НЕ ДОЛЖЕН превышать 4 Мбайт.

4.5 Преобразование ESP_GOST-4M-IMIT

В преобразовании ESP_GOST-4M-IMIT используются:

Значение IV(Seq#l) имеет следующий вид:

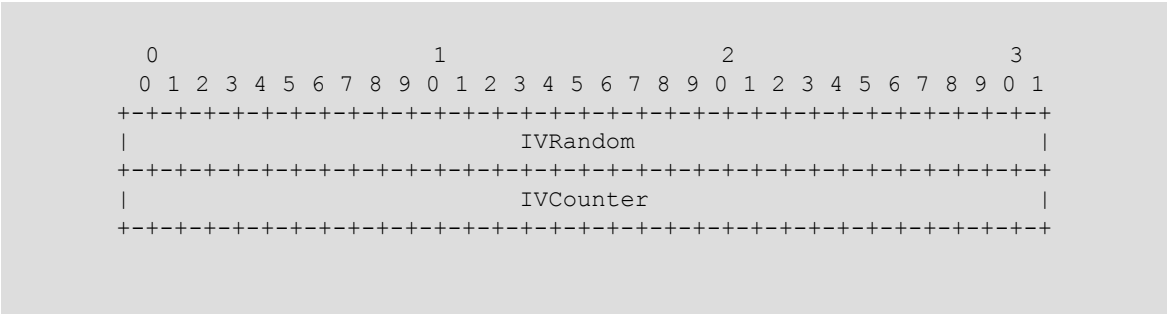

Figure 1: IV для ESP_GOST-4M-IMIT и ESP_GOST-1K-IMIT

где:

IVRandom - случайные 4 байта;

IVCounter = SPIcookie + SPI + Seq#l + IVRandom (mod 2^32);

Получатель ДОЛЖЕН контролировать IVCounter на фазе предварительного контроля Seq# и НЕ ДОЛЖЕН выполнять криптографических преобразований при ошибке. Если реализация ESP

[rfc.comment.7] Аудит - "No valid Security Association exists"

[rfc.comment.8] Аудит - "No valid Security Association exists"

XML to PDF by RenderX XEP XSL-FO Formatter, visit us at http://www.renderx.com/

ведёт протоколы аудита, то эта ошибка МОЖЕТ классифицироваться, как ошибка контроля Seq#. В частности, пакеты с ошибочным IVCounter НЕ ДОЛЖНЫ вызывать увеличения счётчика искажённых пакетов и уменьшения объёма данных SA.

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

Kc_e(Seq#) = Divers(Divers(Divers(Kr_e, Seq#&0xffffffff00000000),
Seq#&0xffffffffffff0000),
Seq#&0xfffffffffffffc0);

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

НЕ РЕКОМЕНДОВАНО согласовывать размеры ESP вложений более чем 64 Кбайт.

4.6 Преобразование ESP_GOST-1K-IMIT

В преобразовании ESP_GOST-1K-IMIT используются:

IV(Seq#l) получается так же, как в Раздел 4.5;

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#);

XML to PDF by RenderX XEP XSL-FO Formatter, visit us at http://www.renderx.com/

5. Дополнительные параметры и атрибуты ESP SA

Для согласования атрибутов преобразований Раздел 4 на фазе II протокола [IKE] обе стороны ДОЛЖНЫ послать ESP_GOST vendor ID. Формат ESP_GOST vendor ID следующий:

Figure 2: ESP_GOST-VENDOR-ID

, где 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 MJR и MNR соответствуют текущей major и minor версии преобразований ESP_GOST (т.е. 1 и 0). [rfc.comment.9]

Параметр	Атрибут	Формат	Умолчание
Параметры ГОСТ 28147-89	32401	B	-
Максимальное значение счётчика искажённых пакетов	32402	B	10^6
Максимальный размер пакета	32507	B	65536

Table 1: Параметры ESP_GOST SA

5.1 Параметры ГОСТ 28147-89

При согласовании SA РЕКОМЕНДОВАНО согласовать параметры ГОСТ 28147-89

GOST-28147-89 S-Box	Значение
id-Gost28147-89-CryptoPro-A-ParamSet	65503
id-Gost28147-89-CryptoPro-B-ParamSet	65504
id-Gost28147-89-CryptoPro-C-ParamSet	65505
id-Gost28147-89-CryptoPro-D-ParamSet	65506

Table 2: Параметры ESP_GOST SA

5.2 Максимальное значение счётчиков искажённых пакетов

Реализация ESP МОЖЕТ иметь предопределённые настройки конфигурации данного значения.

5.3 Максимальный размер пакета

В случае применения ESP для [JUMBO] пакетов IPv6, приложение РЕКОМЕНДОВАНО согласовать этот параметр.

[rfc.comment.9] Идею использования MJR и MNR в Vendor ID позаимствовали из RFC 3706

XML to PDF by RenderX XEP XSL-FO Formatter, visit us at http://www.renderx.com/

6. Благодарности

Авторы документа благодарят российское представительство CISCO, российское представительство CheckPoint и ГАЗПРОМ, которые инициировали процесс обеспечения совместимости продуктов IPsec.

Выражаем благодарность Чмора Андрею Львовичу, ОАО "Инфотекс", за дискуссию по определению понятия DoS.

Выражаем особую благодарность Смыслову Валерию Анатольевичу, ОАО "ЭЛВИС-ПЛЮС", за большое количество ценных замечаний и улучшений, как в сам протокол, так и в его описание.

Выражаем благодарность Тимакову Виктору Михайловичу, ЗАО "Сигнал-КОМ", за дискуссию по поводу криптографически стойкого режима выработки имитовставки ГОСТ 28147-89.

Благодарности рецензентам...

XML to PDF by RenderX XEP XSL-FO Formatter, visit us at http://www.renderx.com/

7. Авторский коллектив

Адреса авторов


```
Дмитрий Г. Дьяченко
ООО Крипто-Про
Сущёвский вал., д. 16, стр. 5
Москва, 127018
Россия
Phone: +7 (495) 780 48 20
Fax: +7 (495) 780 48 20
EMail: lse@cryptopro.ru
URI: http://www.CryptoPro.ru

Владимир О. Попов
ООО Крипто-Про
Сущёвский вал., д. 16, стр. 5
Москва, 127018
Россия
Phone: +7 (495) 780 48 20
Fax: +7 (495) 780 48 20
EMail: lse@cryptopro.ru
URI: http://www.CryptoPro.ru

Кирилл А. Корнилов
S-Terra
Зеленоград, МГИЭТ, корпус 10, офис 110
Москва, 124498
Россия
Phone: +7 (495) 726 98 91
Fax: +7 (495) 531 9789
EMail: hell@s-terra.com
URI: http://www.s-terra.ru
```


XML to PDF by RenderX XEP XSL-FO Formatter, visit us at http://www.renderx.com/

8. Регистрация IANA

IANA выделяет три номера преобразований ESP для использования ГОСТ 28147-89:

<TBD-2> для ESP_GOST-SIMPLE-IMIT;

<TBD-3> для ESP_GOST-4M-IMIT;

<TBD-4> для ESP_GOST-1K-IMIT.

8.1 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.

8.2 Регистрации в IANA не подлежит

Используемые в этом документе приватные "magic numbers":

Класс	Значения	Ссылка	Тип
GOST-28147-SBOX[rfc.comment.10]	32401	B	[draft.CPESP]
Max-Auth-Error[rfc.comment.11]	32402	B	[draft.CPESP]
Max-Packet-Len	32403	B	[draft.CPESP]

Table 3: ESP_GOST "magic numbers"

и приватные значения, описанные Раздел 5.1.

[rfc.comment.10] TODO: ?? GOST-28147-89-SBOX

[rfc.comment.11] TODO: ?? Max-Integrity-fails

XML to PDF by RenderX XEP XSL-FO Formatter, visit us at http://www.renderx.com/

9. Обсуждение требований по безопасности

Приложения РЕКОМЕНДОВАНО исследовать установленным порядком на соответствие заданным требованиям согласно [RFLLIC], и [CRYPTOLIC].

Параметры криптографических алгоритмов влияют на стойкость. Использование параметров, которые не перечислены в [CPALGS], НЕ РЕКОМЕНДОВАНО без соответствующих исследований Section 9 of [CPALGS].

Поскольку ГОСТ 28147-89 имеет размер блока 64-бит, то для обеспечения конфиденциальности и целостности данных реализациям IPsec РЕКОМЕНДОВАНО соблюдать следующие ограничения [Schneier95]:

- ESP_GOST-SIMPLE-IMIT РЕКОМЕНДОВАНО повторное согласование ключей для новой ESP SA при достижении объём данных SA (Lifetime SA) в байтах - 4 Мбайта;
- ESP_GOST-4M-IMIT РЕКОМЕНДОВАНО обрабатывать пакеты размером не превышающим 64 Кбайта. НЕ РЕКОМЕНДОВАНО согласовывать параметр Max-Packet-Len для пакетов IPv6 больший 64 Кбайт и НЕ РЕКОМЕНДОВАНО использовать IPv6 [JUMBO]. РЕКОМЕНДОВАНО повторное согласование ключей для новой ESP SA при достижении объём данных SA (Lifetime SA) в байтах - 2^80 байт;
- ESP_GOST-1K-IMIT РЕКОМЕНДОВАНО повторное согласование ключей для новой ESP SA при достижении объём данных SA (Lifetime SA) в байтах - 2^80 байт.

Приложениям РЕКОМЕНДОВАНО согласовывать время жизни SA (Lifetime SA), как по времени, так и по объёму переданной информации Section 4.4.2.1 of [ARCH]. НЕ РЕКОМЕНДОВАНО согласовывать время жизни SA (Lifetime SA) в секундах более, чем на 86400 сек (1 сутки).

НЕ РЕКОМЕНДОВАНО согласовывать параметр Max-Auth-Error больший чем 10^6, без соответствующего исследования.

Для приложений с требованиями по уровню защиты КВ1 и выше НЕ РЕКОМЕНДОВАНО согласовывать параметр Max-Auth-Error больший чем 10^1, без соответствующего исследования. Так же, для таких приложений, без соответствующего исследования, НЕ РЕКОМЕНДОВАНО использовать ESP_GOST-SIMPLE-IMIT или ESP_GOST-4M-IMIT.

XML to PDF by RenderX XEP XSL-FO Formatter, visit us at http://www.renderx.com/

10. 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] [rfc.comment.12].

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

10.1 Тестовый пакет ESP_GOST-SIMPLE-IMIT

Открытые данные пакета, длина 53:

```
 4500001d 04050607 08090a0b 0c0d0e0f 10111213 14151617 18191a1b 1c1d1e1f
 20212223 24252627 28292a2b 2c2d2e2f 30313233 34
```

Параметры SA с комбинированным алгоритмом ESP_GOST-SIMPLE-IMIT

```
   SPI
      31323334
   ECN
      несогласован
   SPIcookie
      не используется этим алгоритмом
  Kr_e 0x
93384606 364ac23f 8cbc31e3 740a735c 9d1bf663 355c91cd c70dac7a 6f153db6
  Kr_i 0x
c00341ab 7f7fcbf1 65685590 76d601ce de8443ad 3c4264f2 0d71612d 7f1a4ecb
```

[rfc.comment.12] Рабочее название "little-endian", хотя это и не совсем так.

XML to PDF by RenderX XEP XSL-FO Formatter, visit us at http://www.renderx.com/

Промежуточные данные ESP_GOST-SIMPLE-IMIT

```
  Seq#l
     0x3d
  IV
     05060708 090a0b0c
  Pad
     000104
  Seq#h
     0, т.к. ECN несогласован
  ICVpad
     не используется этим алгоритмом
  ICV
     75c1bff1
```

ESP вложение длина 76 (8+8+53+3+4):

```
31323334 0000003d 05060708 090a0b0c c4b75cf1 09a36e66 fc08edf9 1fe08898
74625fac 6b50fbda b6b2fa47 a2ce2305 9c1ed1a5 5868aaf4 985ef0f9 518b2a7c
54de1a71 f82570fe 75c1bff1
```

10.2 Тестовый пакет ESP_GOST-4M-IMIT

Открытый пакет длина 53:

```
4500001d 04050607 08090a0b 0c0d0e0f 10111213 14151617 18191a1b 1c1d1e1f
20212223 24252627 28292a2b 2c2d2e2f 30313233 34
```

Параметры SA с комбинированным алгоритмом ESP_GOST-4M-IMIT

```
  SPI
     31323334
  ECN
     несогласован
  SPIcookie
     0x00000007
 Kr_e 0x
93384606 364ac23f 8cbc31e3 740a735c 9d1bf663 355c91cd c70dac7a 6f153db6
  Kr_i
     не используется данным алгоритмом
```


XML to PDF by RenderX XEP XSL-FO Formatter, visit us at http://www.renderx.com/

Промежуточные данные ESP_GOST-4M-IMIT

```
   Seq#l
      0x3d
   IVRandom
      05060708
   IVCounter
      36383a80  (0x36383a80=0x05060708+0x0000003d+0x00000007+0x31323334)
  Kr_e2 = Divers(Kr_e, Seq# & 0xffffffff00000000) 0x
d7f3ba35 8dd6fa03 8c6e7686 ee2b1455 c1da2fc9 f7f54a1f a1a3e8a9 542e743a
  Kr_e1 = Divers(Kr_e2, Seq# & 0xffffffffffff0000) 0x
cc9fff99 757ca600 459d58cf dc394f97 cbc2fa40 9145c092 7bdedc99 27dd2b75
  Kc_e = Divers(Kr_e1, Seq# & 0xfffffffffffffc0) 0x
3fbd3df2 eae2bc04 db0e980f c6833cd7 ac1a2ce1 f3127535 e5a207b4 ec58986b
   Pad
      000104
   Seq#h
      0, т.к. ECN несогласован
   ICVpad
      не используется этим алгоритмом
   ICV
      b455ad95
```

ESP вложение длина 76 (== 8+8+53+3+4):

```
31323334 0000003d 05060708 36383a80 6468784e 17a0a4cc 6cb4f529 0a9d28ca
1628fac0 f4a0adff 92507aa5 24de2635 f43b9ce7 5ba5dc6a ad7ee852 29b9fe41
7e12d70b dd12eb13 b455ad95
```


XML to PDF by RenderX XEP XSL-FO Formatter, visit us at http://www.renderx.com/

10.3 Тестовый пакет ESP_GOST-1K-IMIT

Открытые данные пакета, длина 1049 [rfc.comment.13] :

```
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 алгоритмом ESP_GOST-1K-IMIT

```
   SPI
      31323334
   ECN
      согласован
   SPIcookie
      00000007
  Kr_e 0x
93384606 364ac23f 8cbc31e3 740a735c 9d1bf663 355c91cd c70dac7a 6f153db6
   Kr_i
      не используется данным алгоритмом
```

[rfc.comment.13] Что-бы проверить усложнение ключа, длина должна быть больше 1024.

XML to PDF by RenderX XEP XSL-FO Formatter, visit us at http://www.renderx.com/

Промежуточные данные ESP_GOST-1K-IMIT

```
   Seq#l
      0x3d
   IVRandom
      05060708
   IVCounter
      36383a80  (0x36383a80=0x05060708+0x0000003d+0x00000007+0x31323334)
  Kr_e2 = Divers(Kr_e, Seq# & 0xffffffff00000000) 0x
44d584a1 038a06f3 cfe472cb 0a4675f0 80d76421 94fb46c5 3986b3a0 8e54f159
  Kr_e1 = Divers(Kr_e2, Seq# & 0xffffffffffff0000) 0x
209e7fc7 a9bdf32a db869779 21ee4c6c 19a6639d 1191d66e 00bb8869 fcc110c2
  Kc_e = Divers(Kr_e2, Seq#) 0x
7c841f78 1fa98545 c31605f1 dff08c2d bca454c7 7d9252f4 de58b5bd c71ccce4
    Pad
      00000000 000504
   Seq#h
      0x0b
   ICVpad
      не используется этим алгоритмом
   ICV
      5a253387
```


XML to PDF by RenderX XEP XSL-FO Formatter, visit us at http://www.renderx.com/

ESP вложение длина 1076 (== 8+8+1049+7+4):

```
31323334 0000003d 05060708 36383a80 9a388999 0a819a95 83bee3c6 2e06601b
224d7a5f 5b4ce278 d89c2551 7065d035 043ed552 f513a694 bc452034 ba9a189f
08da2512 c5ce8ebe 30bc6da8 ec23f4cd 83f0151f 5bb54922 a1a00b98 d59b5368
72581a2c 4ad77d9a 0b3eb7bd 6d6d4ce7 3c3e768b 1518cc86 a748d60e fe6053d9
dcd37a8b 7da39b18 3fc8cba0 af3f25eb 47c2bcd8 efa78d61 78a9f2d9 e4993a64
1c1755b2 693dcfdd 8de34137 23f72ac8 1605e590 fe3569a0 8f5296da e3c1df32
75c6d770 1b768796 8d1a35ee 2263cdae 27075165 e3974748 1101ba40 f12471ed
91e6a866 a0340e1d a2343ee2 bd730ebf d662ce3b 4237f73d 34b43dc0 88f378c1
47afae8e 9e67f65f 4a51c93a 19549dde 3dffaedf d89c3c4d 2fdb5ea5 cdc554de
ee1e7a06 7480328a dac9c66d 01ce5618 16a9934f 6372b1b5 e165a92b fc1e8ab4
ad6fcc93 542b30ff cb7b4b94 733fe633 5e7c0064 bb7a7ae7 9bf62c00 eba462cb
94fb05fb de98b428 60834a2d 6e24bee0 195600df 8a574842 2e53ecf6 2d9a5216
10dcaf12 97db8940 a24887a8 b9d3e2ee 09cfe0fc c80f49df 90b795e6 8c95416d
94140a70 07e484fc 68f09a32 cc60461b 88629cb6 ff728e19 9f862c53 c9005760
e68e12b2 9ecc0cd5 41ae60b2 138839e8 a0cfc0b3 a6a4482b 9bea0d01 5e2ed3e7
85679cd7 be169f0a 0624c583 1ea765d0 fc614ae0 86df8c54 735ab3cd 261586fe
b1b67c61 eef609e1 190b4b73 9738303c 00f632a2 486c9ed4 9ac9ae8b d5b8eaa2
4efbbf7f f6db424b 7c7f0a1e 916b2d91 94030ad1 bb4bb25e e0f5d4ad 6dff2469
d915eccf 5ce4e132 ffda0e30 dd2daa93 797dc362 f853fa41 f68dfcee e43f079b
0e014a27 0454faa7 f3578e0d 5ecad2cd 585d1d91 bca56bb6 7c0f46ad 0a442c97
b46dd109 ae70853a 7d823d34 f193293b 60280076 13bbf7aa 5fcbb513 c288e1c4
a3f564b8 4eab6014 364702e1 23cef078 b3cc072c 7638f8a1 dd8181fe e6457d71
a156a7c5 2883e4e3 8d538519 795cf1e0 09fd729c b34792fb 3a3652ca 9043b067
c0a74dfc 61c4a3f6 0f59c9ad e4ca1dab 4427c7f4 461cf0bd 193963e6 c6b64c96
61a19aed 9d8a2ea9 8487dc7f 1a9f0a27 fff41ef1 1d8beac4 40adc933 139d4f14
d05efab4 31916a7d f77ec4fb 0f48b5f1 95d91ab1 39747199 2da49fbd e2986d46
fabb0f29 75cee7d4 5aa1f71a 706f45bb b00aa884 ad012601 d38d95c1 f03bc971
f3384cee d44366d1 20fe4f79 5ed7e336 8c525627 5f2b3a3a 1893c887 6c91fb93
0433c990 cded2cb5 0b2dd6f0 b2cf86ee 993ec588 c5595005 6faad873 de204a6a
1a695832 e0964ea3 aeb4f6b2 548d966d 58503dbf a38f5002 a32c2c88 d3dedff4
da5f096f 543a695e 1b25d733 7e7bb999 d31113e1 12d45299 6f87581a 6173f215
74e2f802 948eada1 8a509318 fc9aba78 2b63d51a c64d11e7 f81d4aad 8c01cdf0
5c7ea615 4852ee6d 3d42289a 63f12ebc 00003a55 989338a1 026e4482 da659a1d
30a04f7c 358173b6 7bdfe1ed 25cf1f05 5a253387
```


XML to PDF by RenderX XEP XSL-FO Formatter, visit us at http://www.renderx.com/

11. Библиография

11.1 Нормативные ссылки

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

[CPALGS] 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", RFC 4357, January 2006.

[DOI] Piper, D., "The Internet IP Security Domain of Interpretation for ISAKMP", RFC 2407, November 1998.

[ESN] Kent, S., "Extended Sequence Number (ESN) Addendum to IPsec Domain of Interpretation (DOI) for Internet Security Association and Key Management Protocol (ISAKMP)", RFC 4304, December 2005.

[ESP] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, December 2005.

[GOST28147] Government Committee of the USSR for Standards , "Cryptographic Protection for Data Processing System, Gosudarstvennyi Standard of USSR (In Russian)", GOST 28147-89, 1989.

[JUMBO] Borman, D., Deering, S., and R. Hinden, "IPv6 Jumbograms", RFC 2675, August 1999.

[KEYWORDS] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

11.2 Информативные ссылки

[CPCMS] Leontiev, S. and 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)", RFC 4490, May 2006.

[CPPK] Leontiev, S. and D. Shefanovski, "Using the GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms with the Internet X.509 Public Key Infrastructure Certificate and CRL Profile", RFC 4491, May 2006.

[CRYPTOLIC] "Russian Federal Government Regulation on Licensing of Selected Activity Categories in Cryptography Area, 23 Sep 2002 N 691", September 2002.

[draft.CPIKE] Леонтьев, С.Е., Ed., Павлов, М.В., Ed., and А.А. Федченко, Ed., "Использование ГОСТ 28147-89, ГОСТ Р 34.11-94 и ГОСТ Р 34.10-2001 при управлении ключами IKE и ISAKMP", December 2009.

[IKE] Harkins, D. and D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, November 1998.

[RFC4134] Hoffman, P., "Examples of S/MIME Messages", RFC 4134, July 2005.

[RFLLIC] "Russian Federal Law on Licensing of Selected Activity Categories, 08 Aug 2001 N 128-FZ", August 2001.

[Schneier95] Schnier, B., "Applied cryptography, second edition", John Wiley, 1995.

11.3 Библиотека ссылок

[AH] Kent, S., "IP Authentication Header", RFC 4302, December 2005.

XML to PDF by RenderX XEP XSL-FO Formatter, visit us at http://www.renderx.com/

[draft.CPAH] Леонтьев, С.Е., Ed., Павлов, М.В., Ed., and А.А. Федченко, Ed., "Алгоритм обеспечения целостности IPsec (ESP, AH) на основе ГОСТ Р 34.11-94", December 2009.

[GOST3431195] Council for Standardization, Metrology and Certification of the Commonwealth of Independence States (EASC), Minsk , "Information technology. Cryptographic Data Security. Cashing function (In Russian)", GOST 34.311-95, 1995.

[GOSTR341194] Government Committee of the Russia for Standards , "Information technology. Cryptographic Data Security. Hashing function, Gosudarstvennyi Standard of Russian Federation (In Russian)", GOST R 34.11-94, 1994.

[RFEDSL] "Russian Federal Electronic Digital Signature Law, 10 Jan 2002 N 1-FZ", January 2002.

11.4 Ссылки на примеры и методы редактирования

[draft.rfc2434bis] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", Internet-Draft draft-narten-iana-considerations-rfc2434bis-09 (work in progress), March 2008.

[draft.RFC2629bis] Rose, M.T., "Writing I-Ds and RFCs using XML (revised)", February 2009, <http://xml.resource.org/authoring/draft-mrose-writing-rfcs.html>.

[ID-Checklist] Wijnen, B., "Checklist for Internet-Drafts (IDs) submitted for RFC publication", October 2006, <http://www.ietf.org/ID-Checklist.html>.

[ipsec-registry] IANA, "Internet Key Exchange (IKE) Attributes - per RFC 2409 (IKE)", January 2009, <http://www.iana.org/assignments/ipsec-registry>.

[isakmp-registry] IANA, "FROM RFC 2407 and RFC 2408 "Magic Numbers" for ISAKMP Protocol", October 2006, <http://www.iana.org/assignments/isakmp-registry>.

[RFC2629] Rose, M.T., "Writing I-Ds and RFCs using XML", RFC 2629, June 1999.

[RFC3552] Rescorla, E. and B. Korver, "Guidelines for Writing RFC Text on Security Considerations", BCP 72, RFC 3552, July 2003.

[XML2RFC] Rose, M.T., Fenner, B., and C. Levert, "xml2rfc v1.33", February 2009, <http://xml.resource.org/authoring/README.html>.

[xml2rfc-validator] Fenner, , "xml2rfc validator", January 2007, <http://www.fenron.com/~fenner/ietf/xml2rfc-valid/>.

XML to PDF by RenderX XEP XSL-FO Formatter, visit us at http://www.renderx.com/

Адреса авторов

Сергей Е. Леонтьев (editor)
ООО Крипто-Про
Сущёвский вал., д. 16, стр. 5
Москва, 127018
Россия
Phone: +7 (916) 686 10 81
Fax: +7 (495) 780 48 20
EMail: lse@cryptopro.ru
URI: http://www.CryptoPro.ru

Михаил В. Павлов (editor)
ООО Крипто-Про
Сущёвский вал., д. 16, стр. 5
Москва, 127018
Россия
Phone: +7 (495) 780 48 20
Fax: +7 (495) 780 48 20
EMail: pav@cryptopro.ru
URI: http://www.CryptoPro.ru

Андрей А. Федченко (editor)
S-Terra
Зеленоград, МГИЭТ, корпус 10, офис 110
Москва, 124498
Россия
Phone: +7 (495) 726 98 91
Fax: +7 (495) 531 9789
EMail: hell@s-terra.com
URI: http://www.s-terra.ru

XML to PDF by RenderX XEP XSL-FO Formatter, visit us at http://www.renderx.com/

A. Совместимость

Требования по реализации алгоритмов:

- 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] пакетов IPv6;
- ESP_GOST-SIMPLE-IMIT - опционально, РЕКОМЕНДОВАНО только для совместимости.

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

Copyright

[TODO: пока секции прав полностью неопределены стоят все возможные Copyright]

Copyright © Технический комитет по стандартизации №26 "Криптографическая защита информации", ФАТРМ (2009)

Copyright © ЗАО "С-Терра СиЭсПи" (2009)

Copyright © ООО "Крипто-Про" (2009)

Этот документ и информация в нём содержащаяся поставляется "КАК ЕСТЬ", ТК26, S-Terra, Крипто-Про не несут, ни прямой, ни косвенной ответственности, а так же не предоставляют никаких гарантий на последствия использования данного документа. [TODO: дать чёткую формулировку того, что вся ответственность, в конечном счёте, ляжет на читателя документа, а не на тех кто его написал или опубликовал]

XML to PDF by RenderX XEP XSL-FO Formatter, visit us at http://www.renderx.com/

Права на интеллектуальную собственность

[TODO: Описать позицию ТК26 относительно прав на интеллектуальную собственность, возможность для российских потребителей использовать результаты ТК26, а так же на потенциальные конфликты интересов]

Всё согласно IETF BCP 78 and BCP 79.

XML to PDF by RenderX XEP XSL-FO Formatter, visit us at http://www.renderx.com/