ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО/МЭК 24767-2— 2018

Информационные технологии

БЕЗОПАСНОСТЬ ДОМАШНЕЙ СЕТИ

Часть 2

Внутренние службы безопасности. Безопасный протокол связи для связующего программного обеспечения (SCPM)

(ISO/IEC 24767-2:2009, IDT)

Издание официальное

Москва
Стандартинформ
2018

gost.e-ecolog.ru

Предисловие

1 ПОДГОТОВЛЕН Федеральным государственным бюджетным образовательным учреждением высшего образования «Российский экономический университет им. Г.В. Плеханова» (ФГБОУ ВО «РЭУ им. Г.В. Плеханова») на основе собственного перевода на русский язык англоязычной версии международного стандарта, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 22 «Информационные технологии»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 4 сентября 2018 г. № 558-ст

4 Настоящий стандарт идентичен международному стандарту ИСО/МЭК 24767-2:2009 «Информационные технологии. Безопасность домашней сети. Часть 2. Внутренние службы безопасности. Безопасный протокол связи для связующего программного обеспечения (SCPM)» (ISO/IEC 24767-2:2009, «Information technology — Home network security — Part 2: Internal security services — Secure communication protocol for middleware (SCPM)», IDT).

При применении настоящего стандарта рекомендуется использовать вместо ссылочных международных стандартов соответствующие им национальные стандарты Российской Федерации, сведения о которых приведены в дополнительном приложении ДА

5 ВВЕДЕН ВПЕРВЫЕ

*Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. №162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (*gost.e-ecolog.ru

© Стандартинформ, оформление, 2018

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

Содержание

1 Область применения 1
2 Нормативные ссылки 1
3 Термины, определения и сокращения 2
3.1 Термины и определения 2
3.2 Сокращения 2
4 Соответствие 3
5 Проектные решения внутренних служб безопасности для домашних сетей 3
5.1 Общие положения 3
5.2 Вопросы, связанные с безопасностью 4
5.2.1 Общие положения 4
5.2.2 Небезопасная передача 5
5.2.3 Намеренно неправильное использование 5
5.3 Принципы разработки мер безопасности 5
5.3.1 Общие положения 5
5.3.2 Минимизация ресурсов для экономии расходов 5
5.3.3 Независимость коммуникационной среды 5
5.3.4 Независимость криптографических алгоритмов 6
5.3.5 Расширяемость вариантов использования широкополосных подключений 6
6 Безопасный протокол связи для связующего программного обеспечения (SCPM) 6
6.1 Общие положения 6
6.2 Суть протокола SCPM 6
6.3 Принципы работы протокола SCPM 6
6.4 Где реализуется протокол SCPM 7
6.5 Уровни применения протокола SCPM 7
6.6 Ключи применения протокола SCPM 9
7 Формат кадра защищенного сообщения 9
7.1 Общий кадр передачи данных 9
7.1.1 Общие положения 9
7.1.2 Заголовок кадра (HD) 10
7.1.3 Адрес источника (SA) и адрес назначения (DA) 10
7.1.4 Счетчик байтов (BC) 10
7.1.5 Данные приложения (ADATA) 10
7.2 Структура защищенного кадра 10
7.2.1 Общие положения 10
7.2.2 Защищенный заголовок (SHD) 11
7.2.3 Поле порядкового номера (SNF) 11
7.2.4 Счетчик байтов незашифрованной текстовой части данных (PBC) 12
7.2.5 Незашифрованные текстовые данные приложения (PADATA) 12
7.2.6 Код проверки блоков (BCC) 12
7.2.7 Холостое заполнение (PDG) 12
7.2.8 Подпись проверки подлинности данных сообщения (MDAS) 12
8 Реализация протокола SCPM 12
8.1 Алгоритмы и обработка данных 12
8.1.1 Общие положения 12
8.1.2 Криптографические алгоритмы и криптовычисления 12
8.1.3 Алгоритмы аутентификации и вычисление данных аутентификации 13
8.1.4 Режим сцепления блоков шифртекста (CBC) 14
8.1.5 Инициализация и проверка значения поля SNF 14
8.1.6 Вычисление значения вектора инициализации (IV) 14
8.2 Обработка кадра защищенного сообщения 14
8.2.1 Общие положения 14
8.2.2 Обработка кадра сообщения только при проверке подлинности данных 15
8.2.3 Обработка кадра сообщения только в режиме конфиденциальности 16
8.2.4 Обработка кадра сообщения при проверке подлинности данных и конфиденциальности 17

9 Управление ключами 19
9.1 Общие положения 19
9.2 Инициализация ключей 20
9.2.1 Инициализация ключа пользователя 20
9.2.2 Инициализация ключа провайдера услуг 22
9.2.3 Инициализация ключа изготовителя 23
9.3 Обновление мастер-ключа 23
9.3.1 Обновление мастер-ключа между узлом KSN и устройством 23
9.3.2 Синхронизация ключа 27
9.3.3 Запрос на обновление мастер-ключа от устройства 30
Приложение А (справочное) Авторизация узла установки ключа 32
Приложение ДА (справочное) Сведения о соответствии ссылочного международного стандарта национальному стандарту Российской Федерации 33
Библиография 34

Введение

ИСО (Международная организация по стандартизации) и МЭК (Международная электротехническая комиссия) образуют специализированную систему всемирной стандартизации. Государственные органы, являющиеся членами ИСО или МЭК, участвуют в разработке международных стандартов посредством технических комитетов. Участие в разработке стандарта в конкретной области может принять любой заинтересованный орган, являющийся членом ИСО или МЭК. Другие международные организации, правительственные и неправительственные, контактирующие с ИСО и МЭК, также принимают участие в работе.

В области информационных технологий ИСО и МЭК учредили Объединенный технический комитет, ИСО/МЭК СТК 1. Проекты международных стандартов, подготовленные Объединенным техническим комитетом, рассылаются национальным комитетам на голосование. Публикация в качестве международного стандарта требует утверждения не менее чем 75 % национальных комитетов, участвующих в голосовании.

Официальные решения или соглашения МЭК и ИСО по техническим вопросам выражают, насколько это возможно, международное согласованное мнение по относящимся к делу вопросам, так как каждый технический комитет имеет представителей от всех заинтересованных национальных комитетов — членов МЭК и ИСО.

Публикации МЭК, ИСО и ИСО/МЭК имеют форму рекомендаций для международного использования и принимаются национальными комитетами — членами МЭК и ИСО именно в таком понимании. Несмотря на все приложенные усилия для обеспечения точности технического содержания публикаций МЭК, ИСО и ИСО/МЭК, МЭК или ИСО не несут ответственность за то, каким образом они используются или за их неправильную трактовку конечным пользователем.

В целях обеспечения международной унификации (единой системы), национальные комитеты МЭК и ИСО обязуются обеспечить максимальную прозрачность применения международных стандартов МЭК, ИСО и ИСО/ МЭК, насколько это позволяют государственные и региональные условия данной страны. Любое расхождение между публикациями ИСО/МЭК и соответствующими национальными или региональными стандартами должно быть четко обозначено в последних.

ИСО и МЭК не предусматривают процедуры маркировки и не несут ответственность за любое оборудование, заявленное на соответствие одному из стандартов ИСО/МЭК.

Все пользователи должны удостовериться в использовании последнего издания настоящей публикации.

МЭК или ИСО, их руководство, сотрудники, служащие или представители, включая отдельных экспертов и членов их технических комитетов, а также члены национальных комитетов МЭК или ИСО не несут ответственности за несчастные случаи, материальный ущерб или иной нанесенный ущерб, прямой или косвенный, или за затраты (включая судебные издержки), понесенные в связи с публикацией или вследствие использования настоящей публикации ИСО/МЭК или другой публикации МЭК, ИСО или ИСО/МЭК.

Особого внимания требует нормативная документация, цитируемая в настоящей публикации. Использование ссылочных документов необходимо для правильного применения настоящей публикации.

Обращается внимание на то, что некоторые элементы настоящего международного стандарта могут быть объектом патентных прав. ИСО и МЭК не несут ответственности за определение какого-либо или всех таких патентных прав.

Международный стандарт ИСО/МЭК 24767-2 был разработан подкомитетом 25: «Взаимосвязь оборудования для информационных технологий» Объединенного технического комитета ИСО/МЭК 1 «Информационные технологии».

Перечень всех имеющихся в настоящее время частей серии ИСО/МЭК 24767 под общим названием «Информационные технологии. Безопасность домашней сети» представлен на сайте МЭК.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационные технологии

БЕЗОПАСНОСТЬ ДОМАШНЕЙ СЕТИ

Часть 2

Внутренние службы безопасности. Безопасный протокол связи для связующего программного обеспечения (SCPM)

Information technology. Home network security. Part 2. Internal security services. Secure communication protocol for middleware (SCPM)

Дата введения — 2019—02—01

1 Область применения

Настоящий стандарт описывает безопасность оборудования с ограниченными возможностями с точки зрения применения информационных технологий в домашних сетях. Безопасный протокол связи для связующего программного обеспечения (SCPM) прежде всего разработан для поддержки сетевой безопасности (см. 5.2) оборудования, не поддерживающего протоколы интернет-безопасности, такие как IPSec или SSL/TLS. Несмотря на то, что данный протокол разработан для незащищенной передачи, он также может использоваться для других типов передачи данных. Разумеется качественный уровень служб безопасности протокола SCPM не соответствует уровню протоколов интернет-безопасности, но обеспечивает безопасное подключение такого промежуточного программного обеспечения в рамках домашней сети.

Протокол SCPM не заменяет существующие механизмы обеспечения безопасности протоколов, которые уже были опубликованы.

Протокол SCPM обеспечивает безопасность на сетевом уровне и не основан на каком-либо особом способе передачи данных. Настоящий стандарт содержит подробные технические спецификации поддерживаемых служб безопасности, необходимые форматы сообщений, информационные потоки и обработку данных фрагментов информации, необходимые для реализации данного протокола.

Таким образом, в настоящем стандарте не рассматриваются проблемы среды данных или общей архитектуры системы безопасности и не охвачены все технологии домашних сетей. Описанный в настоящем стандарте протокол не зависит от информационной среды. В стандарте регламентируются службы безопасности на сетевом уровне для протоколов, которые не имеют конфликтующей схемы адресации на сетевом уровне. Службы безопасности сетевого уровня представлены сочетанием использования криптографических и защитных механизмов.

Каждый протокол должен содержать подробную информацию по реализации данной защиты. Для системы HES, поддерживающей более одного протокола, требуется шлюз протоколов.

Таким образом, настоящий стандарт не определяет какой-либо конкретный тип приложения, за исключением управления ключами, которое жизненно необходимо для любой службы безопасности. Тем не менее, ограничения по типам приложений, используемых с протоколом SCPM, отсутствуют.

2 Нормативные ссылки

Для пользования настоящим стандартом необходимы следующие стандарты. Для датированных ссылок применяют указанную версию ссылочного стандарта. Для недатированных — последнее издание стандарта (включая любые поправки к нему).

Издание официальное

ISO/IEC 10116, Information technology — Security techniques — Modes of operation for an n-bit block cipher (ISO/IEC 10116, Информационные технологии. Методы обеспечения безопасности. Режимы работы для n-битовых блочных шифров)

3 Термины, определения и сокращения

3.1 Термины и определения

В настоящем стандарте применены следующие термины и определения.

3.1.1 **конфиденциальность:** Свойство, обеспечивающее недоступность и неразглашение информации неуполномоченным лицам, организациям или процессам.

3.1.2 **аутентификация данных:** Служба, используемая для обеспечения корректной верификации источника данных, заявленного стороной для установления канала связи.

3.1.3 **целостность данных:** Свойство, подтверждающее, что данные не были изменены или уничтожены неразрешенным образом.

3.1.4 **узел установки ключа:** Орган, ответственный за генерирование, распространение ключей и управление ими.

3.1.5 **MAC-адрес:** Подслой уровня управления доступом к среде передачи канального уровня используемого протокола передачи данных.

3.1.6 **кадр сообщения:** Минимальный блок данных, передаваемый между узлом домашних устройств и системой управления домашними устройствами.

3.1.7 **внеполосная передача данных:** Использование средств передачи данных, отличающихся от тех, которые требуются для передачи данных по каналу связи.

3.1.8 **запрашиваемая служба:** Сетевой узел, отвечающий на служебные запросы.

3.1.9 **инициатор службы:** Сетевой узел, который инициирует служебные запросы.

3.1.10 **аутентификация пользователя:** Служба для обеспечения корректной проверки идентификационной информации, представленной участником коммуникации. При этом служба авторизации обеспечивает доступ идентифицированного и авторизованного пользователя к конкретному устройству или приложению домашней сети.

3.1.11 **бытовая техника:** Устройства, применяемые в повседневной жизни, например кондиционер, холодильник, и т.д.

3.2 Сокращения

В настоящем стандарте применены следующие сокращения:

ADATA	—	(Application DATA (7.1.5)) данные приложения (7.1.5);
BC	—	(Byte Counter [data length in bytes of the following data payload (size of ADATA)]) счетчик байтов [длина данных в байтах последующей полезной информации (размер ADATA)];
BCC	—	(Block Check Code (7.2.6)) код проверки блоков (7.2.6);
CBC	—	(Cipher Block Chaining) сцепление блоков шифртекста;
CPU	—	(Central Processing Unit) центральное процессорное устройство (ЦПУ);
DA	—	(Destination Address (of a message frame)) адрес назначения (кадра сообщения);
DCL	—	(Data-Link Layer) канальный уровень;
DES	—	(Data Encryption Standard) стандарт шифрования данных;
DH	—	(Diffie-Hellman (was the first published public-key algorithm and it can be used for key distribution)) алгоритм Диффи-Хеллмана (был первым опубликованным алгоритмом шифрования с открытым ключом и может использоваться для распространения ключей);
DoS	—	(Denial of Services) отказ в обслуживании;
HD	—	(HeaDer (of the message frame)) заголовок (кадра сообщения);
HES	—	(Home Electronic System) домашняя электронная система;
IP	—	(Internet Protocol) интернет-протокол;
IPSec	—	(IP Security protocol) протокол безопасности Интернет-протокола;

IPv4 — (Internet Protocol version 4) Интернет-протокол, версия 4;

IPv6 — (Internet Protocol version 6) Интернет-протокол, версия 6;

IV — (Initialisation Vector) вектор инициализации (синхропосылка);

KSN — (Key Setting Node) узел установки ключа;

MAC — (Message Authentication Code) код проверки подлинности сообщения;

MDAS — (Message Data Authentication Signature) подпись проверки подлинности данных сообщения;

PBC — (Plain text data part Byte Counter (data length in bytes of the following data) счетчик байтов незашифрованной текстовой части данных (длина данных в байтах последующей полезной информации (размер ADATA));

PDG — (PaDdinG) холостое заполнение (дополнение);

PADATA — (Plain text Application DATA) незашифрованные текстовые данные приложения;

PIN — (Personal Identification Number) персональный идентификационный код;

SA — (Source Address (of a message frame)) адрес источника (кадра сообщения);

SCPM — (Secure Communication Protocol for Middleware) безопасный протокол связи для промежуточного программного обеспечения;

SHD — (Secure Header) защищенный заголовок;

SNF — (Sequence Number Field) поле порядкового номера;

SSL — (Secure Sockets Layer) уровень защищенных сокетов;

TLS — (Transport Layer Security) протокол безопасности транспортного уровня;

XOR — (eXclusive OR) исключающее ИЛИ.

4 Соответствие

В соответствии с настоящим стандартом применимо нижеследующее:

a) структура должна соответствовать требованиям, изложенным в разделе 6;

b) формат кадра сообщения должен соответствовать техническим требованиям, изложенным в разделе 7;

c) алгоритмы и процедуры обработки должны соответствовать техническим требованиям, изложенным в разделе 8;

d) управление ключами должно соответствовать техническим требованиям, изложенным в разделе 9. Это достигается путем обеспечения соответствия инициализации ключа техническим требованиям 9.2.1.

5 Проектные решения внутренних служб безопасности для домашних сетей

5.1 Общие положения

По мере того, как все большее количество бытовых приборов подключается к домашним сетям, жители домов все больше беспокоятся о безопасности своего имущества. Таким образом, одна из наиболее актуальных исследовательских проблем, которые нужно решить для удовлетворения потребностей пользователей — это обеспечение безопасности. И, если проблема защиты от внешних угроз сегодня довольно успешно решается с использованием таких решений, как протоколы IPSec или SSL/TLS (см. Библиографию спецификаций SSL/TLS), то проблема защиты от внутренних угроз по-прежнему остается нерешенной из-за нескольких изменяющихся критериев. Настоящий стандарт определяет требования к службам внутренней безопасности для домашних электронных систем и домашних сетей.

Внутренняя домашняя сеть требует защиты. Однако не все оборудование, находящееся в доме под контролем, нуждается в одинаковой защите. Можно предусмотреть как минимум три уровня защиты. Некоторое оборудование поддерживает полный стек IP-протоколов с различными протоколами защиты, при том что другие устройства являются независимыми, и поэтому для них защита может не требоваться вообще. Помимо двух данных категорий существует оборудование, которое нуждается в

защите, но не поддерживает полный комплект протоколов IP. Цель настоящего стандарта — обеспечить защиту такого промежуточного оборудования, которое не поддерживает протоколы IP. Протокол SCPM обеспечивает различные службы безопасности на сетевом уровне и не зависит от среды данных, защищая таким образом коммуникации от вторжений во внутреннюю домашнюю сеть.

Для применения мер защиты через Интернет для бытовой техники можно адаптировать существующие решения, такие как протоколы IPSec или SSL/TLS. Комбинация протокола SCPM и существующих решений, настроенных надлежащим образом, в сочетании с технологией межсетевой защиты удовлетворит критериям низкой стоимости и сложности, и будет причинять минимальные неудобства, обеспечивая при этом качественную защиту дома от угроз.

На рисунке 1 показан пример комбинированных технологий защиты. Центр технического обслуживания пытается обновить программное обеспечение бытовой техники, например стиральной машины. Однако стиральная машина без поддержки протоколов IPSec или SSL не сможет обеспечить защиту данных в линии передачи при связи с сервером в центре техобслуживания. Линию разграничения можно провести между двумя сегментами, от сервера центра техобслуживания до контроллера (с поддержкой IP протокола) в доме и от контроллера до стиральной машины. Протоколы IPSec или SSL/TLS используются для защиты сегмента (от сервера центра техобслуживания до контроллера), а протокол SCPM используется для защиты второго сегмента (от контроллера до стиральной машины). Контроллер отвечает за дешифрование кодов, переданных с сервера с защитой протоколом IPSec или SSL/TLS, и повторное шифрование сообщений с использованием протокола SCPM. Стиральная машина, поддерживающая протокол SCPM, может дешифровать данные и в конечном итоге получить код, переданный с сервера. Поскольку домашняя сеть защищена межсетевым экраном, взломщик не может проникнуть в сеть и получить переданный код, пока контроллер занят его дешифрованием и повторным шифрованием.

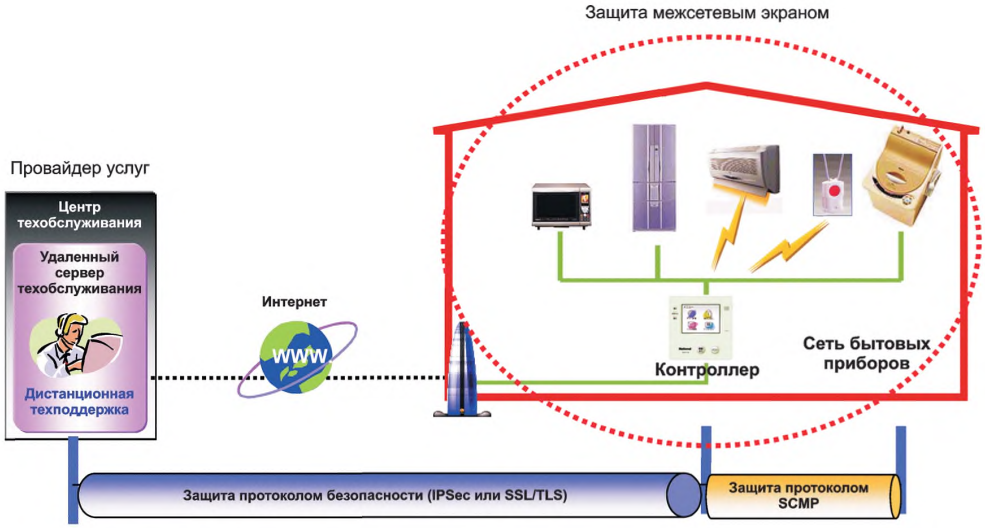

Рисунок 1 — Использование комбинированных технологий для защиты от угроз безопасности

Настоящий стандарт предлагает решение для субкомпонентов, которые содержат устройства без IP в составе домашней электронной сети. Протоколы IPsec и TLS обеспечивают решение для устройств с поддержкой IP в составе домашней электронной сети.

5.2 Вопросы, связанные с безопасностью

5.2.1 Общие положения

В домашних сетях существует множество угроз безопасности. Цель служб безопасности — защита от злонамеренных/угрожающих факторов, которые стремятся нарушить информационную безопасность дома. Будучи направленными на сетевую передачу данных в доме, следующие факторы определяют требования к внутренней безопасности дома.

5.2.2 Небезопасная передача

Линия электропитания

- В большинстве домов имеются подключенные к электросети устройства, а дома по соседству обычно подключены к той же «подсети электропитания», которая подключена к тому же распределительному трансформатору. Таким образом, команды по линии электропитания из одного дома потенциально могут достичь устройства в другом доме по соседству и мешать управлению этими устройствами. Данный фактор также делает возможным перехват информации.

Беспроводная связь

Беспроводная сеть — это, пожалуй, самый привлекательный подход к созданию домашней сети, поскольку она позволяет избежать затрат и сложностей, связанных с проводкой. Тем не менее, она обладает и изъяном в безопасности. Взломщикам больше не требуется физический доступ к сетевой среде, вместо этого они могут просто перехватить передачу данных от другого пользователя в радиусе действия/вещания транслирующего узла.

Суть небезопасной среды передачи данных делает домашние сети уязвимыми для различных атак, таких как пассивный перехват информации, активное вмешательство, утечка «секретной» информации, искажение данных, имитация и отказ от обслуживания.

5.2.3 Намеренно неправильное использование

Несмотря на то, что службы безопасности по настоящему стандарту сосредоточены в доме, при использовании небезопасной среды передачи рассматриваемая область более не ограничивается границами дома. Службы безопасности должны защищать от получения доступа посторонними лицами к информации, передаваемой в пределах дома, и от возможности влиять на такие фрагменты информации или манипулировать ими.

Для выполнения требований к обеспечению безопасности связи в домашней сети главный акцент необходимо сделать на следующих четырех наиболее сложных требованиях:

- конфиденциальность — информация должна быть доступна только авторизованным лицам. Данная функция защищает данные от несанкционированного разглашения;
- аутентификация источника данных и подлинность данных — аутентификация источника данных обеспечивает проверку источников поступления данных на соответствие запросу. Тем не менее, данная функция не может обеспечить защиту от дублирования или изменения данных. В этом случае подлинность данных должна проверяться совместно с аутентификацией источника данных;
- антиповтор — обеспечивает безопасность кадра сообщения, делая невозможным перехват кадра сообщения хакером и внесение измененных кадров в поток данных между узлом источника и узлом назначения;
- управление доступом — обеспечивает защиту ресурсов системы от несанкционированного доступа.

5.3 Принципы разработки мер безопасности

5.3.1 Общие положения

Принимая во внимание тот факт, что механизм SCPM планируется реализовывать в бытовых приборах с ограниченными ресурсами, таких как бытовые приборы с 8-битным ЦПУ, а также то, что безопасность жилого здания должна быть гибкой, особое внимание было уделено следующим вопросам, направленным на предоставление владельцу возможности выбирать между удобством, риском и затратами.

5.3.2 Минимизация ресурсов для экономии расходов

Предполагается, что механизм SCPM будет реализован настолько легко, насколько это возможно при имеющихся ограниченных аппаратных ресурсов (производительность ЦПУ и объем памяти). Указанные выше ограничения затрудняют реализацию в полном объеме и на длительный срок общепринятых мер безопасности, существующих в сфере информационных технологий, которые обычно требуют большого объема вычислений.

5.3.3 Независимость коммуникационной среды

Существует много типов сред передачи данных, используемых в домах для подключения различных устройств к сети. Механизмы, указанные в разделе 6, являются независимыми от среды передачи данных. Данные механизмы дают возможность гибкого использования служб и одновременно обеспечивают их безопасность.

5.3.4 Независимость криптографических алгоритмов

Предполагается, что механизм SCPM позволит выбирать между различными криптографическими алгоритмами без оказания влияния на другие части его реализации, а также внедрять недавно разработанные криптографические методы для совершенствования безопасности в дальнейшем.

5.3.5 Расширяемость вариантов использования широкополосных подключений

В то время как широкополосные подключения в основном используются для доступа в Интернет сегодня, в будущем они также создают новые возможности для обслуживания, такие как обслуживание бытовой техники, контроль за домашней безопасностью или услуги, связанные с измерением. Для обеспечения будущего использования в сочетании с различными службами, которые будут применяться в домашних сетях, предполагается, что механизм SCPM будет оснащен возможностью устанавливать два или более общих ключа для бытового прибора, специфических для службы, позволяющих создание двух или более безопасных доменов в домашних сетях.

6 Безопасный протокол связи для связующего программного обеспечения (SCPM)

6.1 Общие положения

В данном пункте представлено высокоуровневое описание принципа действия протокола SCPM, чтобы показать общую картину процессов данного протокола и его поведения с точки зрения системы, а также чтобы понять, как он встраивается в коммуникацию между сетевыми узлами. В данном пункте также приводится базовое описание следующих далее пунктов, каждый из которых содержит более подробное описание каждого вопроса.

Реализация протокола SCPM, действующего в домашних приборах и контроллере приборов, обеспечивает защиту сетевого трафика. Предложенная защита основывается на требованиях, выбранных исходя из различных предположений, разъясненных в 5.3.

6.2 Суть протокола SCPM

Протокол SCPM разработан для обеспечения сочетания служб безопасности, включая конфиденциальность, аутентификацию источника данных, подлинность данных и службу антиповтора (форма частичной проверки целостности последовательности данных). Набор служб зависит от того, включен ли механизм аутентификации/шифрования или нет.

Службу конфиденциальности можно выбрать отдельно от других служб. Тем не менее, использование службы конфиденциальности без проверки подлинности/аутентификации может подвергнуть системы передачи данных некоторым формам активных атак, способных отрицательно сказаться на работе службы конфиденциальности.

Аутентификация источника данных и целостность данных являются совмещенными службами (далее по тексту — аутентификация) и предлагаются как вариант дополнения совместно (опционно) с конфиденциальностью. Службу антиповтора можно выбрать только если выбрана аутентификация источника данных, и выбор осуществляется исключительно на усмотрение принимающего устройства. (Хотя по умолчанию требуется, чтобы отправитель увеличивал порядковый номер, используемый для антиповтора. Функция работает только если приемное устройство проверяет порядковый номер.)

6.3 Принцип работы протокола SCPM

В целях минимизации размера сообщения протокол SCPM не будет применять механизм формирования пакетов данных, используемый в модели сети ИСО. Модель сети ИСО показана на рисунке 4. Вместо этого используется тот же формат сообщений с добавлением полей, таких как заголовок безопасности, порядковый номер и длина данных между адресом назначения (DA) и счетчиком байтов незашифрованной текстовой части данных (PBC) и шифрованием/аутентификацией некоторых из полей. На рисунке 2 в сравнении показаны кадр обычного сообщения и кадр безопасного сообщения. Точное определение полей будет описано в разделе 7.

На рисунке 2 также показано, что сообщения, переносимые в виде кадров, в линиях связи домашней сети можно условно разделить на два типа: незашифрованный текст и шифрованный текст, в зависимости от соответствующего флага в заголовке. Незашифрованные текстовые сообщения переносятся непосредственно в информационное наполнение в виде открытого текста, а защищенные сообщения хранятся в информационном наполнении в аутентифицированной или зашифрованной форме.

Если флаг в заголовке показывает, что кадр является безопасным, будет активирован протоколом SCPM для интерпретации зашифрованных / аутентифицированных данных информационного наполнения. В противном случае выполняются стандартные процедуры связи в обычном порядке.

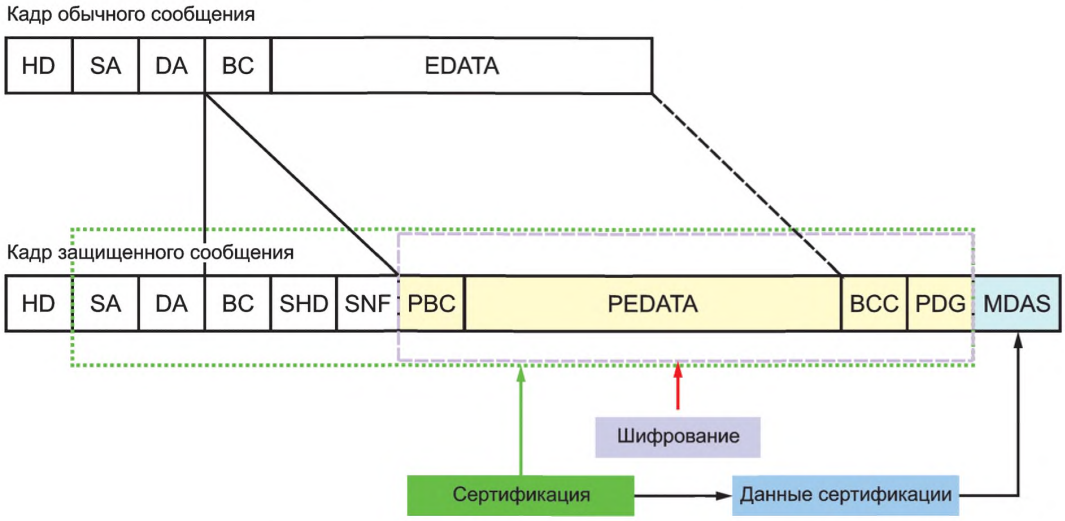

Рисунок 2 — Сравнение кадров обычного и защищенного сообщений

Помимо приведенной структуры сообщений протокол SCPM также использует механизм одного законченного цикла связи для снижения объема передачи данных для сред с низкой или ограниченной пропускной способностью. Законченный цикл связи представляет собой протокол «запрос-ответ», в котором при связи между двумя узлами инициатор службы отсылает сообщение-запрос, а запрашиваемая служба возвращает сообщение-ответ. Последовательность обработки сообщений показана на рисунке 3.

6.4 Где реализуется протокол SCPM

Главная цель протокола SCPM — обеспечение механизмов достаточной защиты для широкого перечня приложений с ограниченными возможностями в плане информационных технологий, а также обеспечение безопасной связи на сетевом уровне, как показано на рисунке 4. Протокол SCPM реализуется связующим ПО защищенной связи на сетевом, транспортном и сеансовом уровнях (рисунок 4).

У кадров сетевого уровня отсутствуют механизмы обеспечения безопасности. Подделать адрес, изменить содержимое, повторить старые кадры и проверить содержимое кадров при передаче довольно легко. Поэтому нет гарантии, что:

a) полученные пакеты отправлены заявленным отправителем;

b) пакеты содержат исходные данные, отправленные отправителем;

c) исходные данные не были просмотрены третьей стороной в ходе передачи.

Обеспечение защиты на сетевом уровне имеет много преимуществ. Чаще всего приложения не нуждаются в изменениях, либо их требуется немного, поскольку они могут без проблем работать с любым протоколом, предусматривающим передачу данных на более высоком, чем сетевой, уровне, что сокращает количество вариантов реализации других протоколов безопасности на более высоких уровнях.

Поскольку протокол SCPM работает на сетевом уровне, он может использоваться для защиты любого протокола, инкапсулированного в сетевой пакет без каких-либо дополнительных требований.

6.5 Уровни применения протокола SCPM

Приложения, работающие на основе протокола SCPM, можно разделить на четыре уровня применения: администратор, пользователь, провайдер услуг и изготовитель. Каждое из применений можно проиллюстрировать следующим образом.

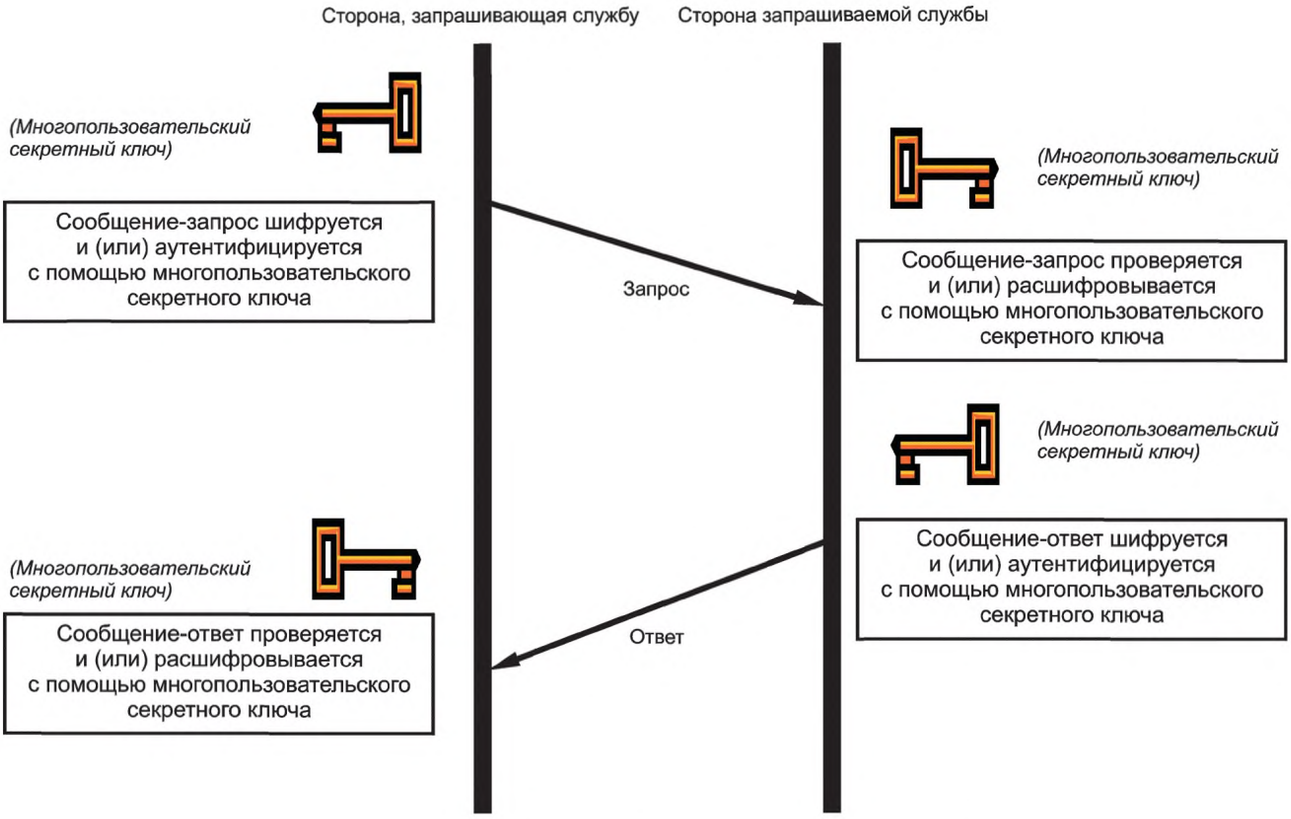

Рисунок 3 — Взаимодействие сторон на основе протокола SCPM

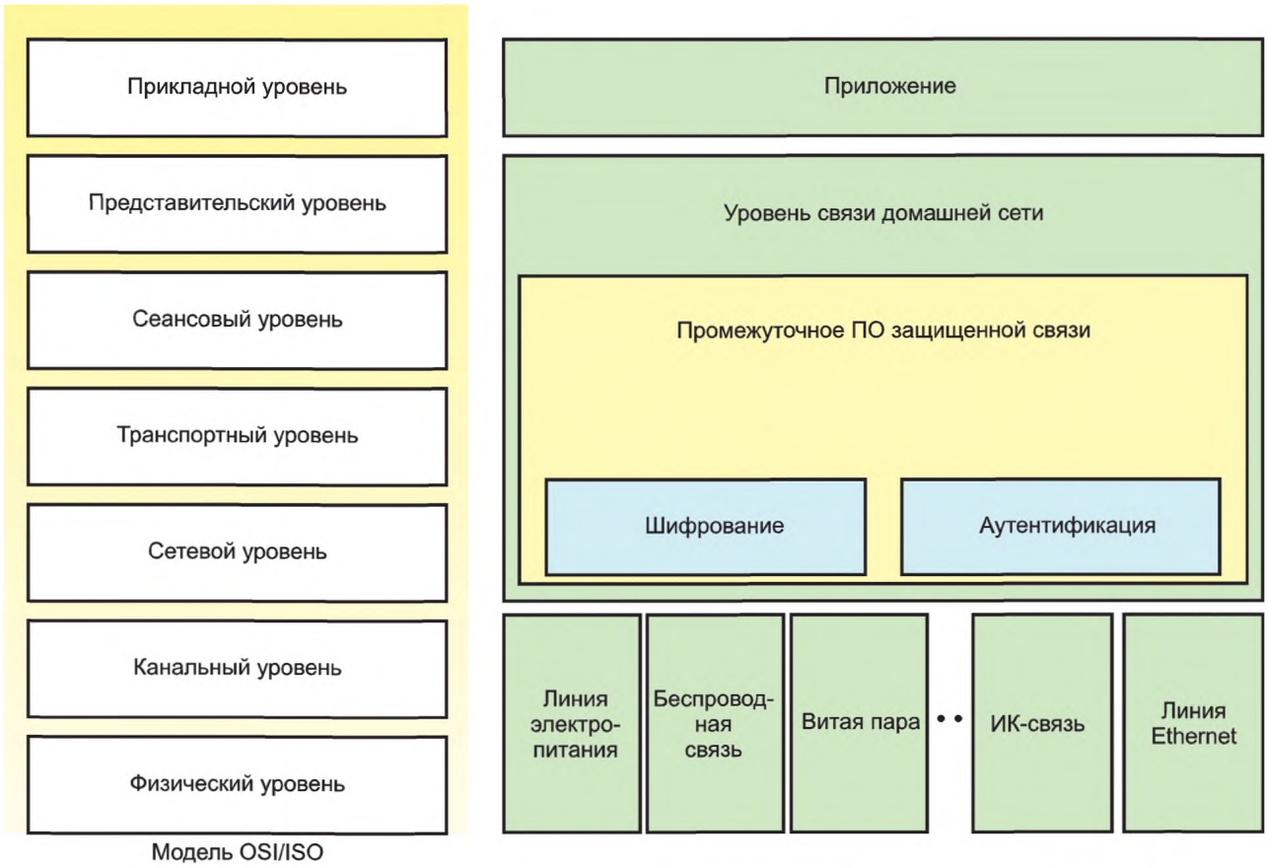

Рисунок 4 — Место протокола SCPM в домашней сети в соответствии с моделью OSI/ISO

Уровень администратора

К этому уровню относится владелец дома, который контролирует различные уровни доступа к устройствам. Например, процедуры начальной настройки ключа пользователя располагаются на уровне администратора.

На данном уровне службы конфиденциальности и (или) аутентификация выполняются по серийному ключу устройства. Серийный ключ настраивается в устройстве при изготовлении и указывается на наружном корпусе устройства. Владелец дома, который контролирует право доступа к устройству, использует серийный ключ при первоначальной настройке ключа пользователя для доступа к устройству.

Уровень пользователя

К данному уровню относятся лица, живущие в доме и использующие автоматизацию управления домашней сетью. Ключ пользователя устанавливается в устройстве администратором; для одного домена устанавливается один ключ пользователя. Если живущие в доме лица не желают разглашать информацию кому-либо, не входящему в круг семьи, сообщения связи должны быть защищены ключом пользователя.

Уровень провайдера услуг

Если владелец дома желает передать некоторые права доступа к устройству провайдеру услуг (при необходимости развернуть службы безопасности), связь между управляющим узлом и узлом устройства защищается ключом провайдера услуг, что предотвращает управление назначенными устройствами со стороны сторонних неуполномоченных провайдеров услуг.

Уровень изготовителя

Когда изготовители выполняют определенные операции, которые требуют защиты от перехвата сообщений злоумышленниками, сообщения связи можно защитить ключом изготовителя. Ключ изготовителя контролируется изготовителем устройства.

6.6 Ключи применения протокола SCPM

Настоящий стандарт определяет следующие пять ключей протокола SCPM.

Серийный ключ

Серийный ключ используется, когда службы конфиденциальности и (или) аутентификации выполняются на уровне администратора.

Ключ пользователя

Ключ пользователя используется, когда службы конфиденциальности и (или) аутентификация выполняются на уровне пользователя.

Ключ провайдера услуг

Ключ провайдера услуг используется, когда службы конфиденциальности и (или) аутентификации выполняются на уровне провайдера услуг.

Ключ изготовителя

Ключ изготовителя используется, когда службы конфиденциальности и (или)аутентификации выполняются на уровне изготовителя.

Мастер-ключ

В настоящем стандарте мастер-ключ — обобщенное название многопользовательского секретного ключа. После обновления общего ключа такой общий ключ называют «новый мастер-ключ», а общий ключ до обновления называют «предыдущий мастер-ключ».

7 Формат кадра защищенного сообщения

7.1 Общий кадр передачи данных

7.1.1 Общие положения

Подавляющее большинство пакетов данных, проходящих сегодня через сеть, соответствуют правилам и форматам, определенным стандартами. Типовой сетевой кадр, как правило, включает заголовок сообщения и данные информационного наполнения. Так, кадр IP включает заголовок IPv4/IPv6 и передаваемые данные. В частности, заголовок сообщения включает заголовок кадра, адрес источника и адрес назначения. Передаваемые данные включают размер данных и данные приложения, как показано на рисунке 5.

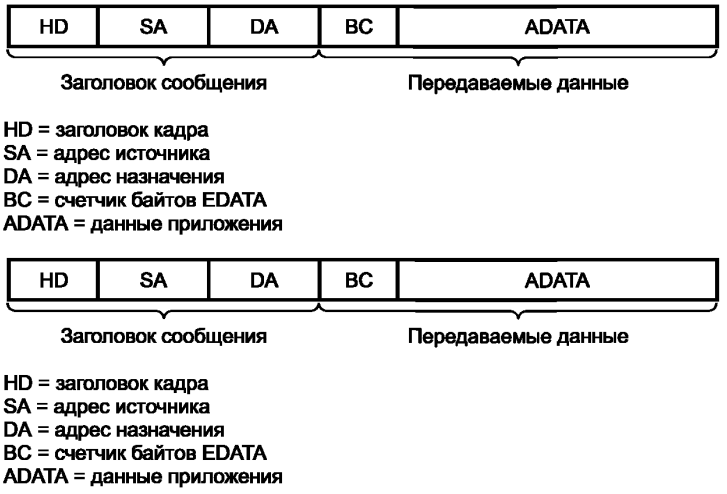

Рисунок 5 — Кадр обычного сообщения

7.1.2 Заголовок кадра (HD)

Заголовок содержит информацию о признаке, который указывает на то, является ли кадр сообщения защищенным или нет. Кроме того, он может нести другую возможную информацию, например способ передачи данных. Типовой моделью передачи данных для сетей является модель точка-точка, но также могут использоваться другие модели, например широкополосная или многоадресная модели.

7.1.3 Адрес источника (SA) и адрес назначения (DA)

Адрес источника представляет собой сетевой адрес источника, который сгенерировал данный кадр сообщения. Адрес назначения представляет собой сетевой адрес целевой хост-системы. Это может быть IP-адрес, MAC-адрес или любая форма адресации, предусмотренная для специфической передачи данных.

7.1.4 Счетчик байтов (BC)

Счетчик байтов показывает размер данных поля ADATA в байтах.

7.1.5 Данные приложения (ADATA)

Данные приложения — это поле переменной длины, которое несет информацию о запрашиваемом сервисе.

7.2 Структура защищенного кадра

7.2.1 Общие положения

Данные приложения далее делятся на несколько полей: защищенный заголовок (SHD), поле порядкового номера (SNF), счетчик байтов незашифрованной текстовой части данных (PBC), незашифрованные текстовые данные приложения (PADATA), код проверки блоков (BCC), холостое заполнение (PDG) и подпись проверки подлинности данных сообщения (MDAS). Следующие подклассы определяют каждое поле защищенного кадра. Некоторые поля могут быть необязательными (отмечены * на рисунке 6), что означает, что поле может отсутствовать, если данная опция не выбрана. Выбрана опция или нет, определяется в защищенном заголовке (SHD). Структура защищенного кадра показана на рисунке 6.

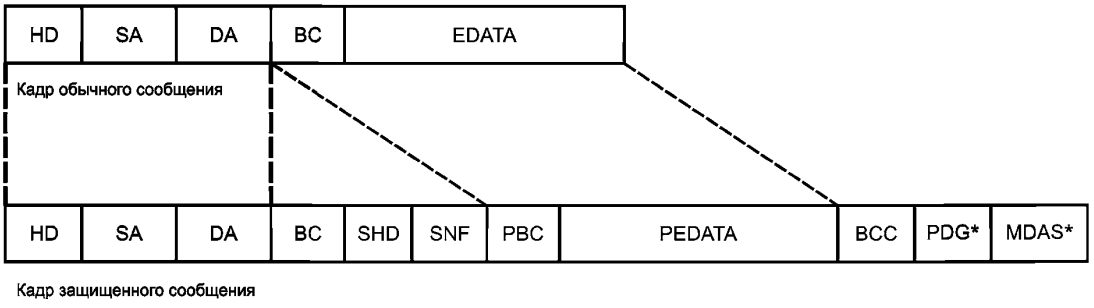

Рисунок 6 — Кадр защищенного сообщения

7.2.2 Защищенный заголовок (SHD)

Защищенный заголовок представляет собой 2-байтовое поле. На рисунке 7 показан формат данных в защищенном заголовке.

b3:b2:b1:b0	**Индекс ключа** b3:b2:b1:b0=0:0:0:0 — индекс серийного ключа b3:b2:b1:b0=0:0:0:1 — индекс ключа пользователя b3:b2:b1:b0=0:0:1:0 — индекс ключа изготовителя Прочие: с 0:0:1:1 по 1:1:1:1 — индекс ключа провайдера услуг
b4	1: используется для указания того, что сообщение зашифровано и аутентифицировано многопользовательским секретным ключом, который вычисляется алгоритмом Диффи-Хеллмана 0: b3:b2:b1:b0 — применяется индекс ключа
b5	Зарезервировано для будущего использования
b6	**Флаг службы аутентификации** (b7:b6=1:1 не допускается) 0: Сертификация включена 1: Сертификация отключена
b7	**Флаг службы шифрования** (b7:b6=1:1 не допускается) 0: Шифрование включено 1: Шифрование выключено
b8	**Тип сообщения** 0: Запрос 1: Ответ
b9~b11	Зарезервировано для будущего использования
b15:b14:b13:b12	**Ответ служб безопасности** b15:b14:b13:b12 = 0:0:0:0: успешно b15:b14:b13:b12 = 0:0:0:1: ошибка проверки SNF b15:b14:b13:b12 = 0:0:1:0: ошибка проверки сертификации b15:b14:b13:b12 = 0:1:0:0 ошибка расшифровки данных

Рисунок 7 — Формат данных защищенного заголовка (SHD)

Биты 0-3 используются для указания индекса ключа для различных применений (администратор, пользователь, провайдер услуг и изготовитель). Поскольку для бытовой техники возможны несколько услуг, индекс ключа провайдера услуг может быть в диапазоне от (b3:b2:b1:b0) = 0:0:1:1 до 1:1:1:1.

Чтобы обеспечить обновление мастер-ключа с использованием алгоритма Диффи-Хеллмана, для указания данного типа услуги используется бит 4. Если значение бита 4 задано равным 1, это означает, что данный кадр защищенного сообщения защищен многопользовательским секретным значением, вычисленным алгоритмом Диффи-Хеллмана.

Биты 6-7 показывают, включена ли служба безопасности. Если значение бита 6 задано равным 0, это означает, что в такой передаче данных включена служба аутентификации. Если значение бита 7 задано равным 0, это означает, что включена служба конфиденциальности. Биты 6 и 7 не должны одновременно равняться 1, так как если заголовок кадра сообщения указывает на то, что передача данных защищена, но не указана служба аутентификации или конфиденциальности, это приведет к конфликту со значением, указанным в поле заголовка.

Поскольку протокол SCPM представляет собой протокол типа «запрос-ответ», бит 8 указывает на свойство сообщения. Значение 0 указывает на сообщение типа «запрос» от запрашивающей стороны, а значение 1 указывает на сообщение типа «ответ» от запрашиваемой стороны.

Биты 12-15 используются для указания результата обработки сообщения-запроса и действительны в сообщении-ответе. Бит 12 указывает на коррекцию проверки поля SNF, бит 13 указывает на коррекцию проверки аутентификации, а бит 14 указывает на коррекцию прав доступа.

7.2.3 Поле порядкового номера (SNF)

Это 4-байтовое поле, которое содержит монотонно возрастающее значение счетчика (порядковый номер).

Данное поле является обязательным и всегда присутствует, даже если безопасная передача данных не включает службу антиповтора для данного кадра сообщения. Обработка поля порядкового

номера — в ответственности запрашиваемой службы. Исходное значение поля SNF может быть определено двумя способами — методом случайного выбора (для холодного или горячего пуска узла) или методом чтения и использования порядкового номера, хранящегося в постоянной памяти (только для горячего пуска). Запрашиваемая служба увеличивает порядковый номер на 1 и передает его в инициатор службы после успешной проверки подлинности.

Инициатор службы использует значение поля SNF в следующем сообщении-запросе к той же запрашиваемой службе.

7.2.4 Счетчик байтов незашифрованной текстовой части данных (PBC)

Счетчик PBC представляет собой 1-байтовое поле, указывающее количество байтов в незашифрованной текстовой части данных (PADATA).

7.2.5 Незашифрованные текстовые данные приложения (PADATA)

Незашифрованные текстовые данные приложения PADATA представляют собой поле переменной длины. Данное поле является обязательным и представляет целое число байт по длине. Максимальная длина поля PADATA составляет 255 байт.

7.2.6 Код проверки блоков (BCC)

Использование механизма кода проверки блоков (BCC) предназначено для обнаружения ошибок. Код BCC представляет собой 1-байтовое поле, в котором хранится итоговое значение, генерируемое путем выполнения операций с исключающим ИЛИ по поперечному контролю четности каждого поля. Данные, проверяемые BCC, включают поля: SA, DA, BC, SHD, SNF, PBC и PADATA. Данный код проверки не является криптографической контрольной величиной.

7.2.7 Холостое заполнение (PDG)

При использовании алгоритма шифрования, требующего, чтобы незашифрованный текст имел длину, точно кратную определенному количеству байт, например размеру блока блочного шифра, поле PDG используется для заполнения незашифрованного текста (состоящего из полей: PBC, PADATA и BCC) до размера, требуемого алгоритмом. Инициатор службы может добавлять два байта холостого заполнения. Для расширенного стандарта шифрования AES инициатор службы может добавлять от 0 до 15 байт холостого заполнения. Включение поля PDG не является обязательным, но все реализации должны поддерживать генерирование и использование холостого заполнения. Если требуются байты поля PDG, но алгоритм шифрования не указывает содержание холостого заполнения, тогда по умолчанию применяется следующая обработка данных. Поле PDG заполняется значением 0x00.

7.2.8 Подпись проверки подлинности данных сообщения (MDAS)

Подпись MDAS представляет собой поле переменной длины, длина которого указывается выбранной функцией аутентификации. Например, если применяется стандарт AES CBC-MAC со 128-битным ключом (см. ИСО/МЭК 10116), подпись MDAS представляет собой 16-байтовые данные. Поле MDAS — это значение, вычисляемое по кадру сообщения протокола SCPM, исключая заголовок (HD) и данные проверки подлинности данных (MDAS). Поле MDAS не является обязательным и включается только в случае, если служба аутентификации была выбрана и указана в поле SHD.

8 Реализация протокола SCPM

8.1 Алгоритмы и обработка данных

8.1.1 Общие положения

Несмотря на то, что и конфиденциальность, и аутентификация являются необязательными, должна быть выбрана как минимум одна из данных служб, а значит оба алгоритма шифрования и проверки подлинности не должны быть одновременно отключены.

8.1.2 Криптографические алгоритмы и криптовычисления

Используемый алгоритм шифрования указывается с распределением ключа. Протокол SCPM предназначен для использования с алгоритмами симметричного шифрования. Обязательным алгоритмом шифрования SCPM является AES. Зашифрованные поля включают поля: PBC, PADATA, BCC и PDG. На рисунке 8 показан пример с использованием алгоритма шифрования AES-CBC с длиной ключа 128-бит.

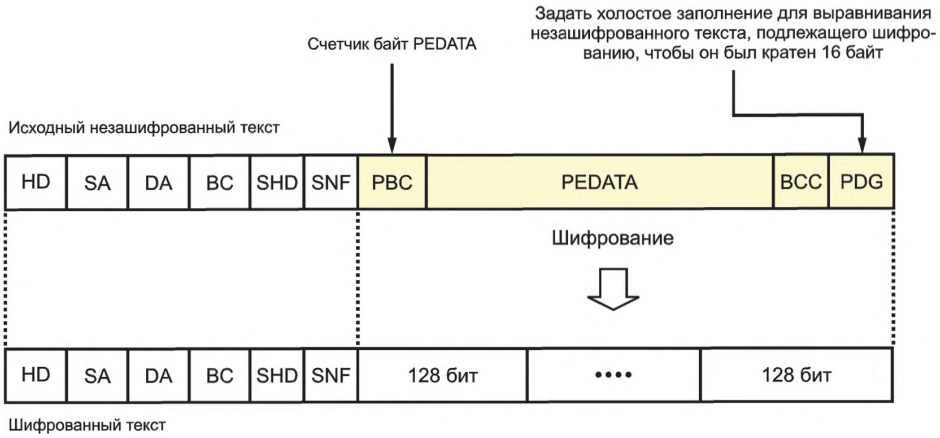

Рисунок 8 — Шифрование с применением алгоритма AES-CBC со 128-битным ключом

8.1.3 Алгоритмы аутентификации и вычисление данных аутентификации

Так же, как и для вышеупомянутых алгоритмов шифрования, алгоритмы проверки подлинности данных, используемые для вычисления данных аутентификации, должны быть специфицированы как алгоритмы с распределением ключей, которые принимают сообщение любого размера и генерируют выходное сообщение фиксированной длины. Обязательным алгоритмом проверки подлинности данных протокола SCPM является алгоритм AES. Он работает аналогично алгоритму шифрования и использует поле CBC-MAC для создания подписи, необходимой для проверки подлинности сообщения по блочному шифру. Данные аутентификации поступают из полей в кадре сообщения, а для получения необходимого значения существуют два варианта: 1) только аутентификация и 2) аутентификация после шифрования. На рисунке 9 показано, как вычисляются данные аутентификации. В случае выполнения только аутентификации данные аутентификации вычисляются от поля SA до поля BCC и вносятся в поле MDAS. В случае включения служб аутентификации и шифрования сначала выполняется обработка шифрования (из поля PBC в поле PDG), а аутентификация вычисляется от поля SA до зашифрованных данных и вносится в поле MDAS. Поле MDAS — это последние N байт защищенного кадра в целом, где N зависит от алгоритма аутентификации.

Для некоторых алгоритмов аутентификации строка байтов, по которой вычисляется значение данных аутентификации, должна быть кратна размеру блока, определяемому алгоритмами. Если длина строки байтов не соответствует требованиям алгоритма по размеру блока, в конце кадра аутентифицированного сообщения добавляется скрытое холостое заполнение (после поля BCC, если выполняется только служба аутентификации, и после шифрования данных, если используются службы аутентификации и конфиденциальности) перед внесением в поле MDAS. Данные байты холостого заполнения должны иметь нулевое значение, а размер блока определяется требованиями алгоритма. Холостое заполнение не передается с кадром сообщения.

8.1.4 Режим сцепления блоков шифртекста (CBC)

Все алгоритмы шифрования, используемые в SCPM, должны работать в режиме сцепления блоков шифртекста (CBC) (см. ИСО/МЭК 10116). CBC требует, чтобы количество данных, подлежащих шифрованию, было кратным размеру блока шифртекста. Требование выполняется путем добавления холостого заполнения в конце данных при необходимости, перед шифрованием. Холостое заполнение становится частью шифрованного текста кадра сообщения и удаляется инициируемой службой в ходе обработки входящего сообщения. Если данные уже кратны размеру блока шифра, холостое заполнение добавлять не требуется.

Шифры в режиме CBC также требуют наличия вектора инициализации (IV) во избежание генерирования нового ключа для каждого сеанса шифрования. Данный вектор инициализации генерируется из значения SNF и описан в 8.1.6.

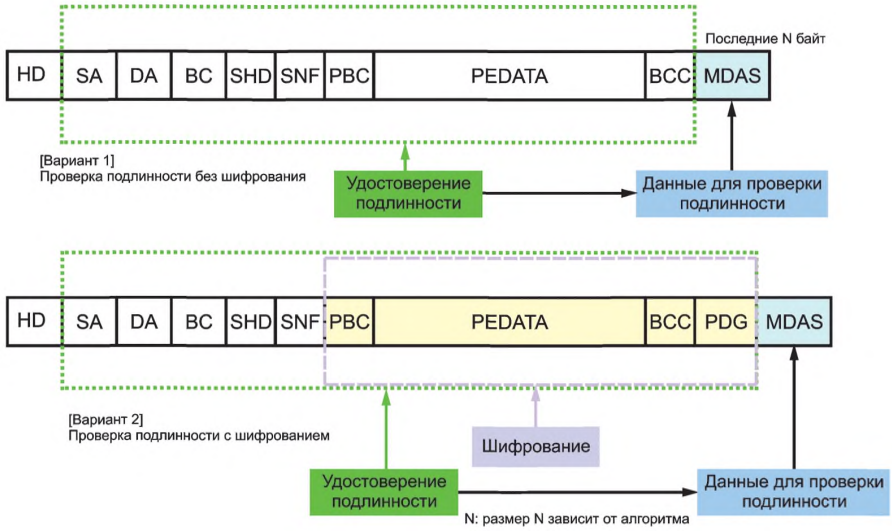

Рисунок 9 — Вычисление данных аутентификации

8.1.5 Инициализация и проверка значения поля SNF

Инициатор службы сохраняет значение поля SNF, связанное с инициируемой службой в предыдущем успешном ответе. Инициируемая служба контролирует/управляет полем SNF для каждого инициатора служб. Но для первого запроса или в случае потери значения поля SNF по каким-либо причинам, например из-за отключения питания, инициатор службы не сохраняет последовательный номер, и инициализация поля SNF должна выполняться вместе со службой аутентификации.

Сообщение-запрос включает произвольное значение поля SNF и отправляется на противоположную сторону, как показано на рисунке 10. Если не удается проверить поле SNF, запрашиваемая служба отвечает с использованием сгенерированного/сохраненного значения поля SNF, чтобы указать на ошибку проверки поля SNF. Инициатор службы получает значение поля SNF и отправляет сообщение об аутентификации с полученным значением поля SNF. Запрашиваемая служба проверяет сообщение и затем отправляет ответ об успешной аутентификации инициатору службы с новым значением поля SNF (увеличенным на 1).

8.1.6 Вычисление значения вектора инициализации (IV)

Применение режима CBC требует наличия четко заданного вектора инициализации (IV) N байт, при этом N зависит от алгоритма. Например, 16-байтовый вектор инициализации используется в шифровании алгоритмом AES-CBC с длиной ключа 128 бит. Данный вектор инициализации превосходит по значению защищенное (зашифрованное) информационное наполнение. Включение вектора инициализации в каждом кадре сообщения гарантирует, что возможно расшифрование каждого полученного кадра сообщения, даже если некоторые кадры сообщения выпали при передаче. Значение вектора инициализации является производным от поля SNF. Например, 16-байтовый вектор инициализации используется для шифрования алгоритмом AES-CBC. На рисунке 11 показана настройка значения вектора инициализации в случае 16-байтового IV.

8.2 Обработка кадра защищенного сообщения

8.2.1 Общие положения

Обработка кадра защищенного сообщения зависит от того, какие службы были включены.

Следующие подклассы иллюстрируют, как кадры сообщения обрабатываются в трех комбинациях:

a) включена только проверка подлинности данных (аутентификация);

b) включена только конфиденциальность;

c) включены и проверка подлинности данных, и аутентификация.

Обмен защищенными сообщениями между инициатором службы и запрашиваемой службой соответствует обмену в одноранговой сети. Если указанный сетевой адрес назначения является широковещательным адресом, запрашиваемая служба должна отказаться от сообщения.

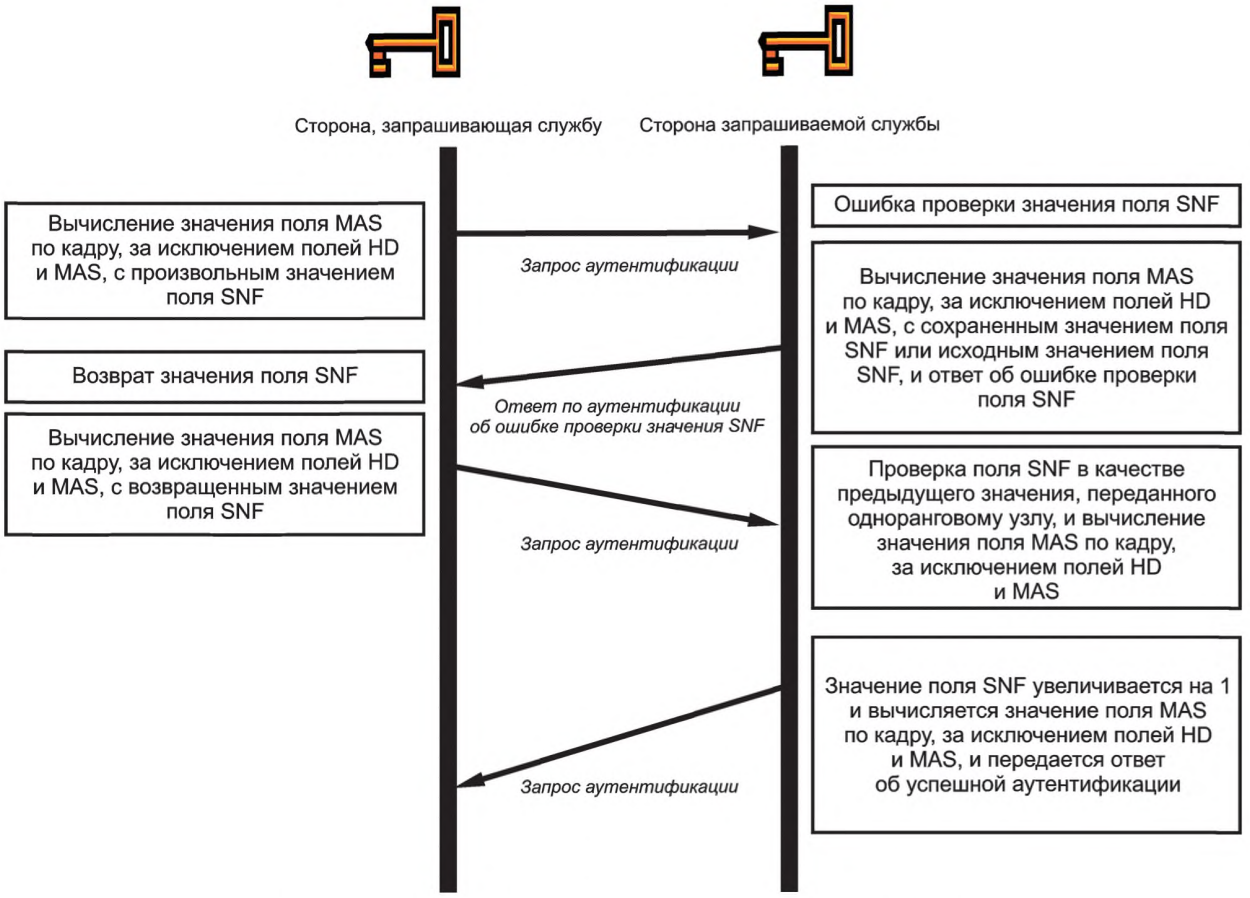

Рисунок 10 — Последовательность инициализации поля SNF



Рисунок 11 — Вычисление значения вектора инициализации (IV)

8.2.2 Обработка кадра сообщения только при проверке подлинности данных

На рисунке 12 показана последовательность проверки подлинности данных между инициатором службы и запрашиваемой службой.

Шаги (номера указывают последовательность) генерирования сообщения проверки подлинности данных от инициатора службы описываются следующим образом:

a) установка флага в поле SHD:

1) биты b0:b1:b2:b3 используются для указания индекса ключа, применяемого при передаче данных;

2) биты b6:b7 = 0:1 используются для указания на службу безопасности следующим образом: аутентификация включена, а шифрование выключено;

3) бит b8 = 0 используется для указания на то, что сообщение является запросом;

b) установка порядкового номера:

1) если порядковый номер из предыдущей передачи данных сохранился, используется именно он;

2) в противном случае (для первой передачи данных или если порядковый номер не сохранился), используется случайным образом выбранный произвольный порядковый номер, как описано в 7.2.3;

c) вычисление поля BCC;

d) вычисление поля MDAS по всему кадру сообщения, за исключением полей: HD и MDAS.

Проверка сообщения аутентификации запрашиваемой службой включает следующее шаги.

Шаг 1 Проверка порядкового номера.

Шаг 2 Проверка поля BCC.

Шаг 3 Проверка данных аутентификации.

Ответное сообщение готовится следующим образом, чтобы передать его инициатору услуг. Шаги (номера указывают последовательность) генерации ответных сообщений от запрашиваемой стороны описываются следующим образом:

e) установка флага в поле SHD:

1) биты b0:b1:b2:b3 используется для указания индекса ключа, применяемого при передаче данных, как и в соответствующем сообщении-запросе;

2) биты b6:b7 = 0:1 используется для указания на службу безопасности следующим образом: аутентификация включена, а шифрование выключено, как и в соответствующем сообщении-запросе;

3) бит b8 = 1 используется для указания на то, что сообщение является ответом;

4) запись результата ответа в биты: b12:b13:b14:b15 для указания на то, является проверка успешной или нет. Если проверка успешная, задаются следующие значения битов: b12:b13:b14:b15 = 0:0:0:0;

f) установка порядкового номера:

1) в случае успешного ответа ставится следующий порядковый номер (увеличенный на 1);

2) в случае ошибки ответа:

I) если порядковый номер, соответствующий данному инициатору службы, не существует, запрашиваемая служба должна поставить исходный порядковый номер в поле SNF в ответе инициатору службы;

II) в противном случае используется предыдущий отправленный порядковый номер;

g) установка данных информационного наполнения:

1) при ошибке проверки подлинности данных данные из запроса копируются и вставляются в поля PBC, PADATA и BCC из соответствующих полей сообщения-запроса;

2) при успешной проверке подлинности данных данные ответа и соответствующий размер данных вставляются в поля PADATA и PBC и вычисляется поле BCC;

h) вычисление поля MDAS по всему кадру сообщения, за исключением полей HD и MDAS.

На рисунке 12 показан пример кадров сообщений, использующих службу удостоверяющей подписи.

8.2.3 Обработка кадра сообщения только в режиме конфиденциальности

На рисунке 13 показана последовательность шифрования между инициатором службы и запрашиваемой службой.

Шаги по генерированию шифрованного сообщения от инициатора службы включают следующее (номера указывают последовательность):

a) установка флага в поле SHD:

1) биты b0:b1:b2:b3 используются для указания индекса ключа, применяемого при передаче данных;

2) биты b6:b7 = 1:0 используются для указания на службу безопасности следующим образом: аутентификация отключена, а шифрование включено;

3) бит b8 = 0 используется для указания на то, что сообщение является запросом;

b) установка произвольного номера в поле SNF;

c) вычисление поля BCC;

d) шифрование:

1) добавление необходимых данных холостого заполнения;

2) если используется алгоритм режима CBC, данные вектора инициации, действующие как вводные данные для алгоритма шифрования, вычисляются по значению поля SNF;

3) шифрование результата (поля: PBC, PADATA, BCC и PDG).

Шаги проверки шифрованного сообщения запрашиваемой службой включают следующее (номер указывает последовательность).

Шаг 1. Расшифрование данных.

Шаг 2. Проверка поля BCC.

Сообщение-ответ подготавливается для передачи инициатору службы следующим образом:

a) установка флага в поле SHD:

1) биты b0:b1:b2:b3 используются для указания индекса ключа, применяемого при передаче данных, как и в соответствующем сообщении-запросе;

2) биты b6:b7 = 1:0 используются для указания на службу безопасности следующим образом: аутентификация выключена, а шифрование включено, как и в соответствующем сообщении-запросе;

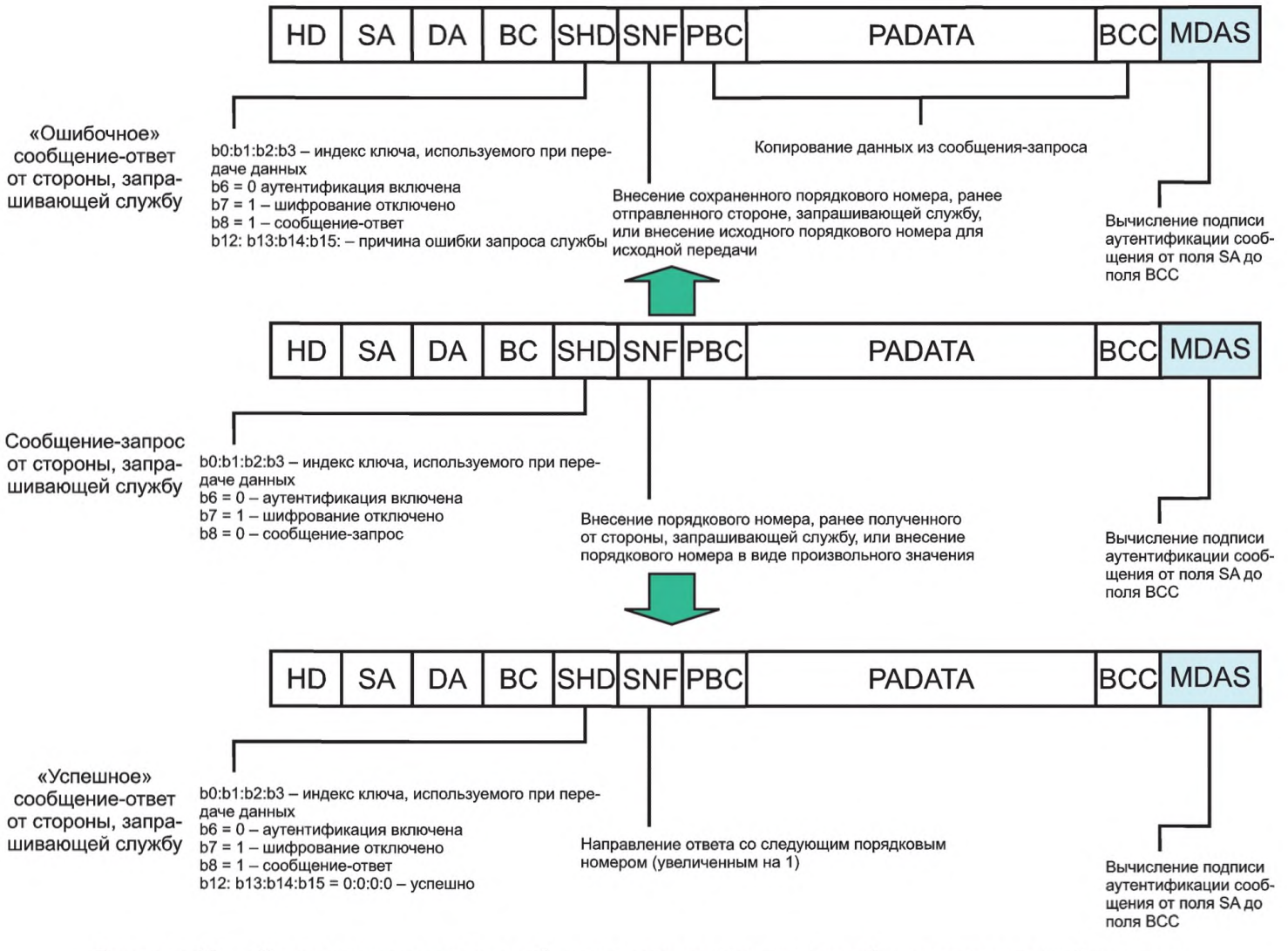

Рисунок 12 — Кадры защищенного сообщения, использующие службу удостоверяющей подписи

3) бит b8 = 1 используется для указания на то, что сообщение является ответом;

4) запись результата ответа в биты b12:b13:b14:b15 для указания на то, является проверка успешной или нет. Если проверка успешная, задаются следующие значения битов — b12:b13:b14:b15 = 0:0:0:0;

b) установка произвольного значения в поле SNF;

c) установка данных информационного наполнения:

1) при ошибке проверки шифрованные данные копируются из сообщения-запроса;

2) при успешной проверке данные ответа вносятся в поле PADATA, а соответствующий размер данных вносится в поле PBC и вычисляется поле BCC, затем выполняется шифрование полей: PBC, PADATA, BCC и данных холостого заполнения.

8.2.4 Обработка кадра сообщения при проверке подлинности данных и конфиденциальности

Когда одновременно включены служба аутентификации и служба конфиденциальности, для шифрованного текста проверяется подлинность данных, а нешифрованный текст с подтвержденными данными не шифруется. Это означает, что для кадров исходящих сообщений первым выполняется шифрование, а для кадров входящих сообщений первой выполняется аутентификация.

На рисунке 14 показаны процессы в инициаторе службы и запрашиваемой службе.

Шаги по генерированию шифрованного сообщения с подтвержденными данными от инициатора службы включают следующее. Описанный ниже порядок обработки упрощает быстрое обнаружение и отклонение повторных пакетов получателем перед расшифровкой пакета, таким образом потенциально снижая воздействия DoS атак:

a) установка флага в поле SHD:

1) биты b0:b1:b2:b3 используются для указания индекса ключа, применяемого при передаче данных;

2) биты b6:b7 = 0:0 используются для указания на службу безопасности следующим образом: аутентификация и шифрование включены;

3) бит b8 = 0 используется для указания на то, что сообщение является запросом;

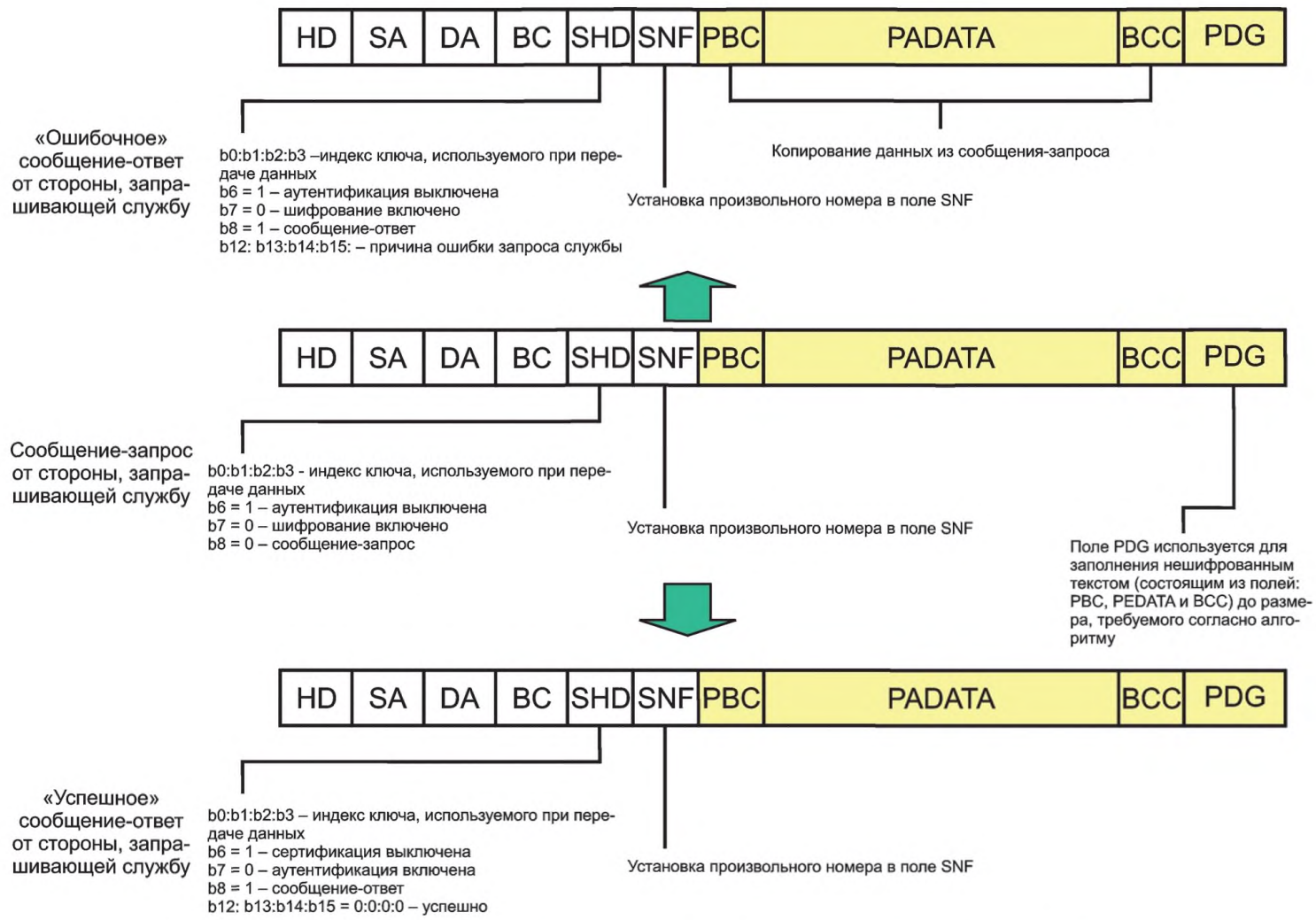

Рисунок 13 — Кадры защищенного сообщения, использующие службу шифрования

b) установка порядкового номера;

c) вычисление поля BCC;

d) шифрование:

1) добавление необходимых данных холостого заполнения;

2) если используется алгоритм режима CBC, данные вектора инициации, действующие как вводные данные для алгоритма шифрования, вычисляются по значению поля SNF;

3) шифрование результата (поля: PBC, PADATA, BCC и PDG);

e) вычисление данных аутентификации:

1) вычисление значения аутентификации от поля SA до шифрованных данных (включает поля: PBC, PADATA, BCC и PDG);

2) сохранение результата вычислений в поле MDAS.

Шаги по проверке зашифрованного и аутентифицированного сообщения включают следующее.

Шаг 1. Проверка значения поля SNF.

Шаг 2. Проверка значения поля MDAS.

Шаг 3. Расшифрование данных.

Шаг 4. Проверка значения поля BCC.

Сообщение-ответ подготавливается для передачи инициатору службы следующим образом. Шаги (номера указывают последовательность) генерирования сообщения-ответа от инициатора службы описываются следующим образом:

f) установка флага в поле SHD:

1) биты b0:b1:b2:b3 используются для указания индекса ключа, применяемого при передаче данных, как и в соответствующем сообщении-запросе;

2) биты b6:b7 = 0:0 используются для указания на службу безопасности следующим образом: аутентификация и шифрование включены, как и в соответствующем сообщении-запросе;

3) бит b8 = 1 используется для указания на то, что сообщение является ответом;

4) запись результата ответа в биты b12:b13:b14:b15 для указания на то, является проверка успешной или нет. Если проверка успешная, задается следующее значение битов — b12:b13:b14:b15 = 0:0:0:0;

g) установка порядкового номера запроса в поле SNF:

1) в случае успешного ответа, ставится следующий порядковый номер (увеличенный на 1);

2) в случае ошибки ответа;

I) если порядковый номер, соответствующий данному инициатору службы, не существует, запрашиваемая служба должна поставить исходный порядковый номер в поле SNF в ответе инициатору службы;

II) в противном случае, используется предыдущий отправленный порядковый номер;

h) установка данных информационного наполнения:

1) при ошибке проверки шифрованные данные полей: PBC, PADATA, BCC и PDG копируются из сообщения-запроса;

2) при успешной проверке данные ответа вносятся в поле PADATA, а соответствующий размер данных вносится в поле PBC и вычисляется поле BCC, затем выполняется шифрование полей: PBC, PADATA, BCC и данных холостого заполнения;

I) вычисление поля MDAS по всему кадру сообщения, за исключением полей: HD и MDAS.

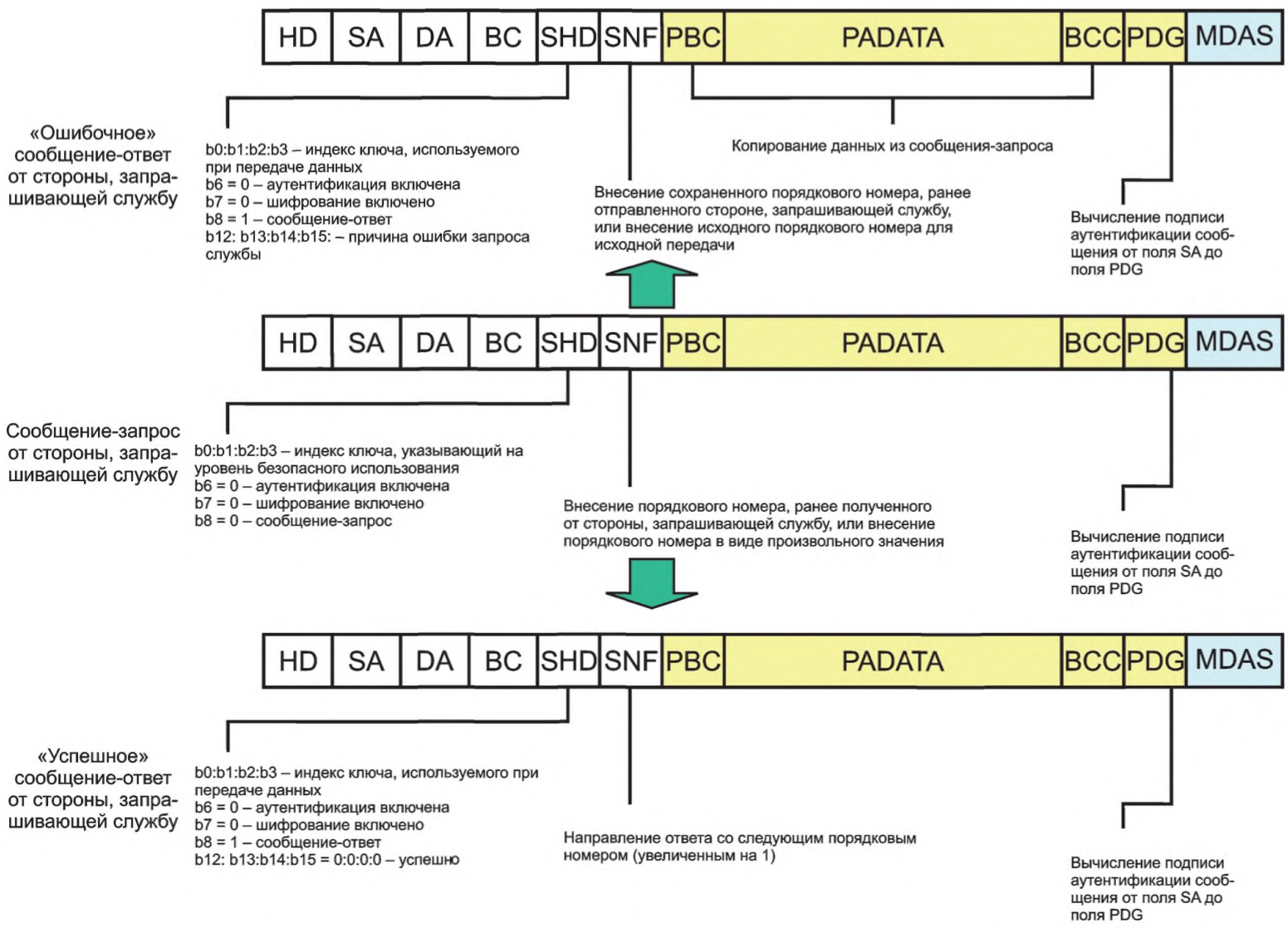

Рисунок 14 — Кадры защищенного сообщения, использующие службу шифрования и службу проверки подлинности данных

9 Управление ключами

9.1 Общие положения

Одним из преимуществ протокола SCPM является то, что механизм управления ключами также обеспечивается данным протоколом, то есть ключи, используемые в протоколе SCPM, им же и распределяются.

Для безопасной передачи данных изначально устанавливаются различные ключи, которые поразному используются в зависимости от типа ключа. Генерирование/распределение ключей контролируется и управляется «узлом установки ключа» (KSN). За хранение данных распределенных ключей отвечают домашние устройства. Ключи служат как общие секретные данные инициаторов служб и запрашиваемых служб. Протокол SCPM предполагает, что в одном домене присутствует только один узел установки ключей (KSN), и только один узел KSN распределяет ключи по домашним устройствам. Помимо этого узел KSN управляет ключом между узлом KSN и домашними устройствами. Когда узел KSN направляет различные ключи на домашние устройства, данные ключи должны быть зашифрованы.

Узел KSN играет важную роль в доставке, обновлении и хранении всех ключей. Узел KSN должен быть очень надежным устройством. Типовые операции по авторизации узла KSN описаны в приложении А.

9.2 Инициализация ключей

9.2.1 Инициализация ключа пользователя

Ключ пользователя — это общие секретные данные всех устройств в домене. Безопасная передача данных обеспечивается благодаря практике использования ключа пользователя, когда все лица, живущие в доме, используют автоматизацию управления домашней сетью. Если устройство хочет присоединиться к сети (новое зарегистрированное устройство), требуется инициализация ключа пользователя на данном устройстве, что выполняется путем доставки защищенного ключа пользователя на новое зарегистрированное устройство узлом KSN.

Перед такой инициализацией узлы обмениваются между собой предварительной версией общих «секретных» данных посредством определенных внеполосных механизмов. Процессы показаны на рисунке 15, а шаги описаны ниже:

a) узел KSN аутентифицирует администратора посредством специализированных механизмов, например, с помощью механизма PIN;

b) в качестве предварительной версии общих «секретных» данных необходимо использовать серийный ключ (который назначается изготовителем прибора) для нового зарегистрированного устройства и передать его в узел KSN с помощью определенных независимых средств, например серийный ключ нового зарегистрированного устройства вводится в узел KSN;

c) подготовка инициализации ключа пользователя на новом зарегистрированном устройстве:

1) поскольку это первая передача данных между узлом KSN и новым зарегистрированным устройством, общий согласованный (надежный) порядковый номер между ними двумя отсутствует, поэтому устройство должно случайным образом сгенерировать исходное значение порядкового номера и поставить его в поле RNS, как описано в 7.2.3;

2) если устройство имеет режим исходной установки, его необходимо переключить в данный режим;

d) узел KSN выдает запрос в виде нешифрованного текста на новое зарегистрированное устройство, чтобы определить алгоритм шифрования/аутентификации, поддерживаемый серийным ключом;

e) новое зарегистрированное устройство отвечает узлу KSN с помощью поддерживаемого алгоритма шифрования/аутентификации в виде нешифрованного текста;

f) узел KSN генерирует/возвращает ключ пользователя, сохраняет его со связанными атрибутами (длина ключа и алгоритм) в поле PADATA, далее шифрует/проверяет подлинность кадра сообщения-запроса инициализации ключа пользователя с помощью предварительного общего серийного ключа и предварительно согласованного алгоритма (указанного выше в разделах 4 и 5), а затем передает защищенный кадр сообщения на новое зарегистрированное устройство;

g) новое зарегистрированное устройство получает и проверяет команду на инициализацию ключа пользователя по серийному ключу и предварительно согласованному алгоритму (указанному выше в разделах 4 и 5);

h) если проверка прошла успешно, новое зарегистрированное устройство подготавливает ответ на инициализацию ключа пользователя путем увеличения порядкового номера на 1, копирования зашифрованных данных и проверки подлинности сообщения по его серийному ключу, и затем передает его в узел KSN. В результате узел KSN владеет информацией о том, получило ли новое зарегистрированное устройство ключ пользователя должным образом;

i) узел KSN получает и проверяет ответ по инициализации ключа пользователя, возвращает новый порядковый номер и подтверждает, что обмен прошел успешно.

Если узел KSN не получает ответ от нового зарегистрированного устройства, то он повторно передает защищенное сообщение с предыдущим переданным порядковым номером.

Обмен кадрами защищенного сообщения между узлом KSN и новым зарегистрированным устройством показан на рисунке 16. Сообщение-запрос инициализации ключа включает информацию защищенного заголовка (b0:b1:b2:b3 = 0:0:0:0 как индекс серийного ключа, b6:b7 = 0:0 как включенные аутентификация и шифрование, b8=0 как сообщение-запрос), порядковый номер и материалы ключа, содержащие ключ пользователя, длину ключа и связанный алгоритм, сохраненный в поле PADATA. Успешный ответ и ошибка ответа также показаны на рисунке 15. Различия между успешным ответом и ошибкой ответа следующие:

a) результат ответа будет указан в битах b12:b13:b14:b15 поля SHD;

b) если ответ успешный, значение поля SNF увеличивается на 1. В случае ошибки значение поля SNF остается таким же, что и в предыдущем ответе;

c) в случае ошибки ответа зашифрованные данные в сообщении-ответе копируются из сообщения-запроса, но данные аутентификации вычисляются от поля SA до шифрованных данных (включая поля: PBC, PADATA, BCC и PDG). В случае успешного ответа информация ответа вносится в поле PADATA.

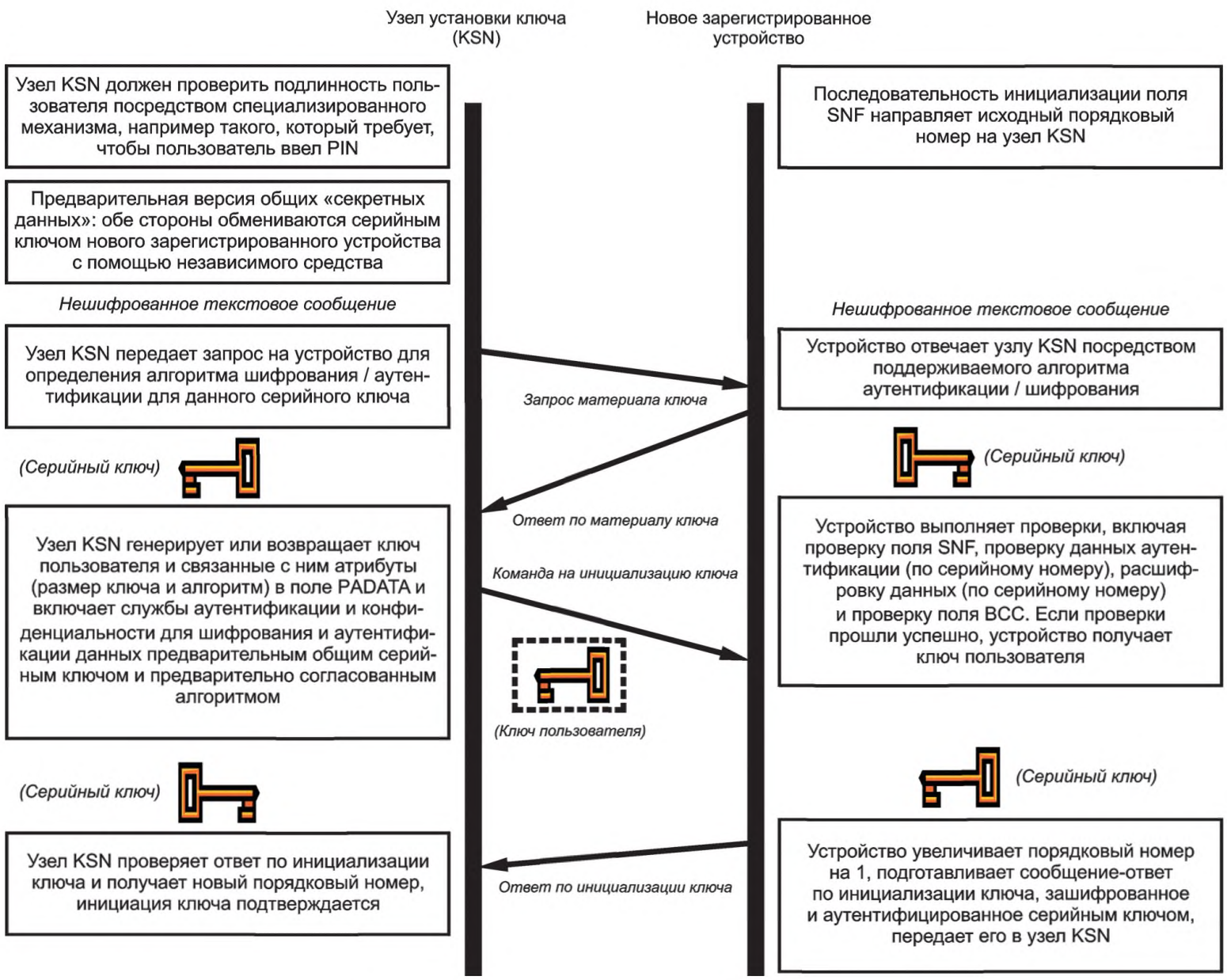

Рисунок 15 — Последовательности инициализации ключа пользователя

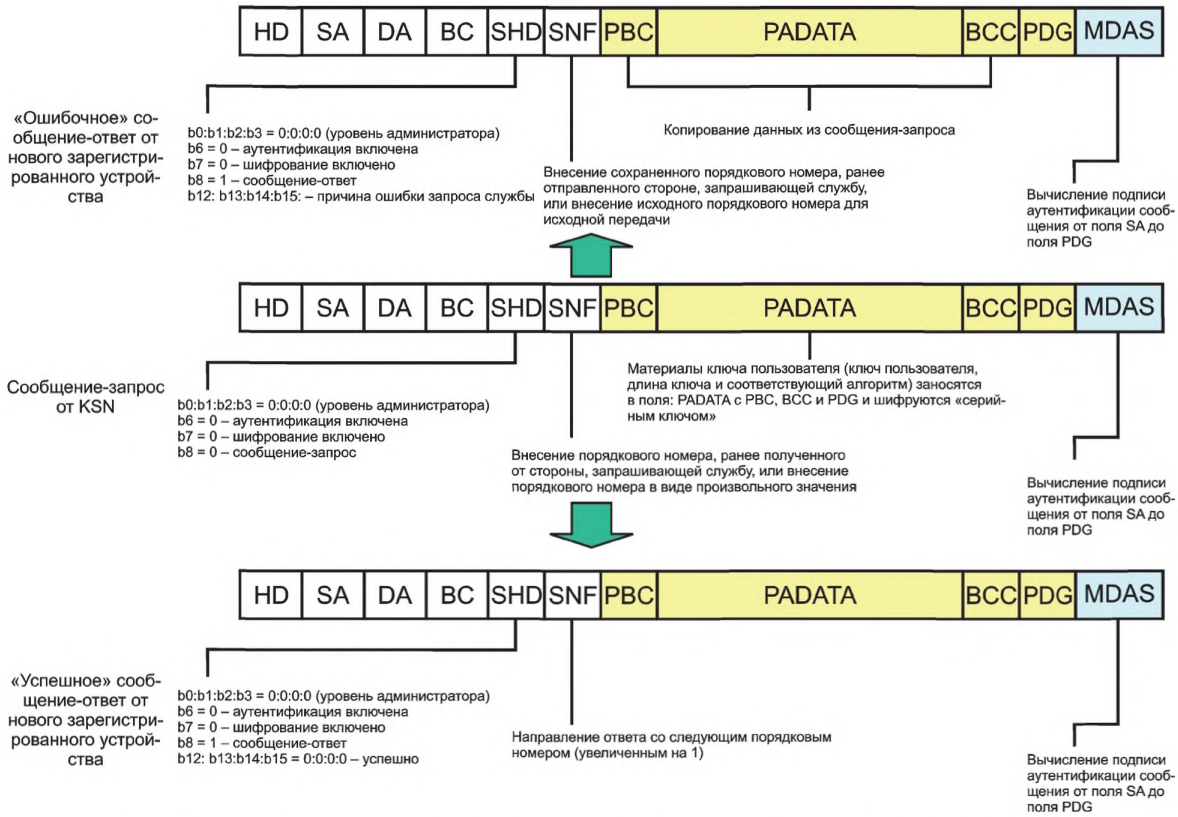

Рисунок 16 — Кадры защищенного сообщения об инициализации ключа пользователя

9.2.2 Инициализация ключа провайдера услуг

Ключи провайдера услуг представляют собой общие «секретные» данные управляющих узлов и узлов устройств. Доставка ключей провайдера услуг на новое зарегистрированное устройство с протоколом SCPM также выполняется узлом KSN. Предварительная версия общих секретных данных, ключ пользователя, используется для защиты доставки. Процессы показаны на рисунке 17, а шаги описаны ниже:

a) Узел KSN проверяет подлинность настройки ключа провайдера услуг посредством специализированных механизмов, например с помощью PIN;

b) Узел KSN генерирует/возвращает ключ провайдера услуг, сохраняет его со связанными атрибутами (длина ключа и алгоритм) в поле PADATA, включает службы аутентификации и конфиденциальности для шифрования/проверки подлинности данных запроса инициализации ключа провайдера услуг с помощью ключа пользователя и связанного с ним алгоритма, а затем передает его на новое зарегистрированное устройство;

c) Новое зарегистрированное устройство получает и проверяет команду на инициализацию ключа провайдера услуг с помощью ключа пользователя и связанного с ним алгоритма;

d) Если проверка прошла успешно, новое зарегистрированное устройство подготавливает ответ по инициализации ключа провайдера услуг путем увеличения порядкового номера на 1, шифрования данных ответа (поля: PBC, PADATA, BCC и PDG) и добавления данных аутентификации (поле MDAS) с помощью ключа пользователя и передает их на узел KSN;

e) Узел KSN получает и проверяет ответ по инициализации ключа провайдера услуг, возвращает новый порядковый номер и подтверждает, что обмен прошел успешно.

Если узел KSN не получает ответ от нового зарегистрированного устройства, узел KSN повторно передает защищенное сообщение с предыдущим переданным порядковым номером.

Обмен кадрами защищенного сообщения между узлом KSN и новым зарегистрированным устройством показан на рисунке 18 при указании индекса ключа в поле SHD, установленной в битах — b0:b1:b2:b3= = 0:0:0:1. Ключ провайдера услуг, длина ключа и связанный с ним алгоритм шифруются и сохраняются в поле PADATA. Состав сообщения-запроса и сообщения-ответа практически такой же, как и для инициализации ключа пользователя, за исключением различий в уровне применения и ключевых данных.

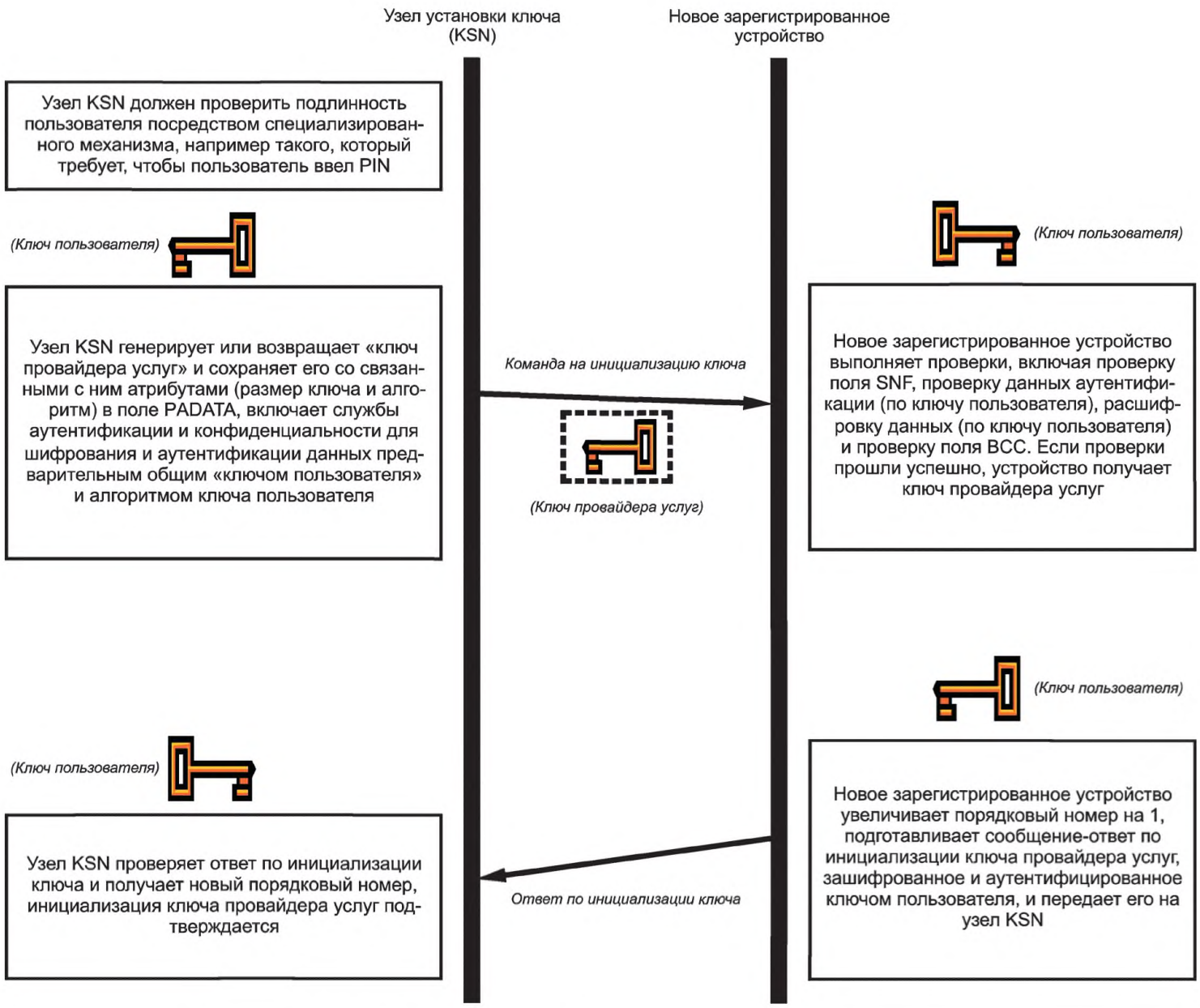

Рисунок 17 — Последовательности инициализации ключа провайдера услуг

9.2.3 Инициализация ключа изготовителя

Рекомендуется, чтобы ключ изготовителя был производным от результата функции хеширования личной информации и данных о свойствах устройства.

Особая система для установки ключа изготовителя для защищенной передачи данных на узел не предусмотрена.

9.3 Обновление мастер-ключа

9.3.1 Обновление мастер-ключа между узлом KSN и устройством

В протоколе SCPM конфиденциальность и проверка подлинности данных обеспечиваются посредством использования согласованного криптографического алгоритма, такого как AES. В настоящее время алгоритм AES считается стойким криптографическим алгоритмом, поскольку расчетное время взлома AES значительно больше, чем время взлома прочих алгоритмов, таких как DES. Длина ключей алгоритма DES составляет 56 бит. Ключи AES могут быть длиной 128, 192 и 256 бит. При стойкости AES в 128 бит число доступных ключей составляет в 10(**21) раз больше, чем предлагает алгоритм DES, а это означает, что, если существует метод, способный расшифровать ключ за одну секунду (хотя, на самом деле, «взломщики DES» обычно тратят несколько часов на расшифровку ключа DES), потребуется 149 триллионов лет на взлом 128-битного ключа AES, что непреодолимо с точки зрения современных технологий. Тем не менее, надежность защиты не может полностью зависеть от стойкости используемого алгоритма, на нее может влиять и человеческий фактор. В этом случае рекомендуется, чтобы периодически выполнялись операции по обновлению мастер-ключа во избежание возможных рисков нарушения безопасности. Однако разработчики могут найти баланс между эффективными практиками обеспечения безопасности и физическими ограничениями.

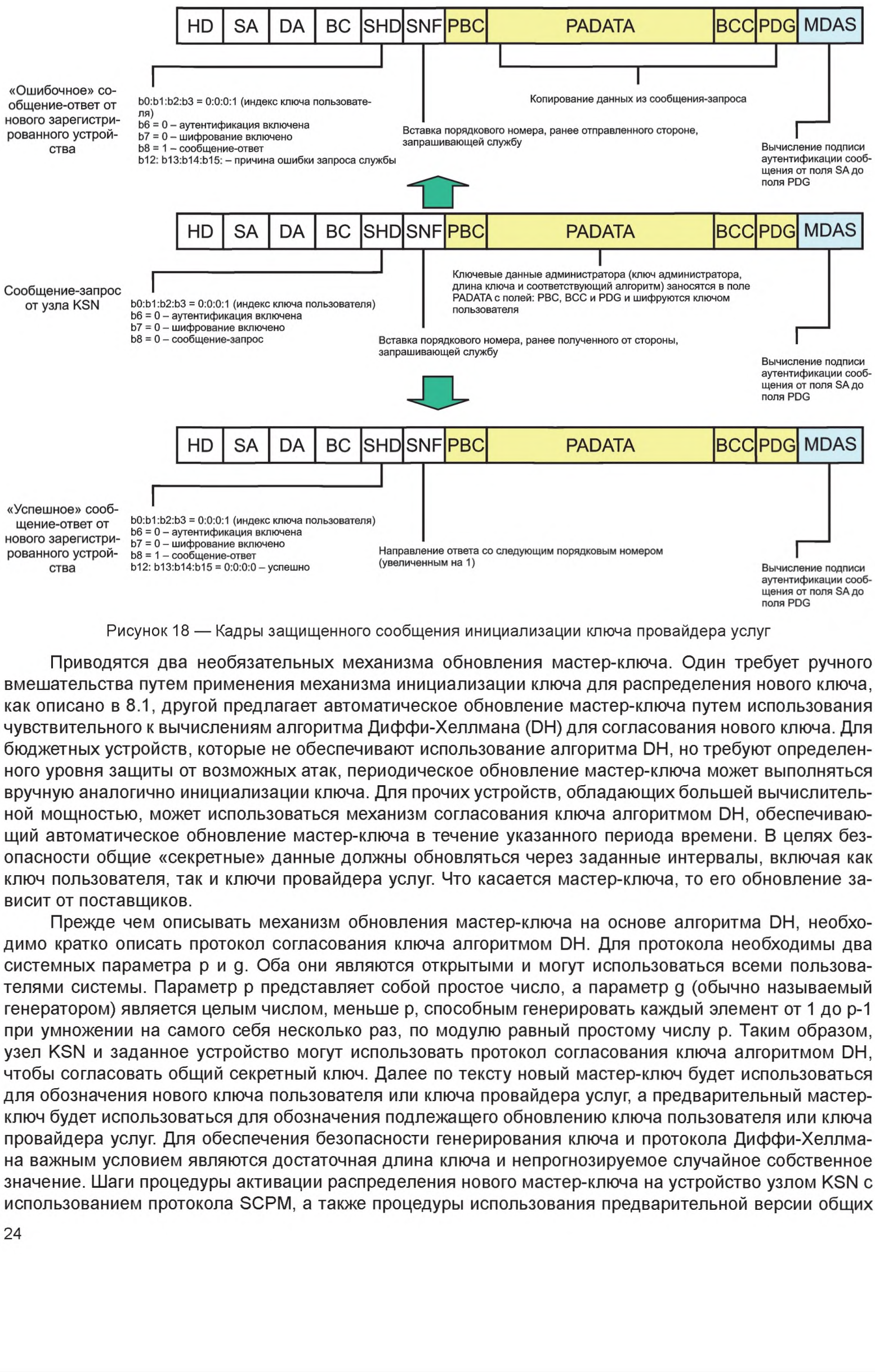

Рисунок 18 — Кадры защищенного сообщения инициализации ключа провайдера услуг

Приводятся два необязательных механизма обновления мастер-ключа. Один требует ручного вмешательства путем применения механизма инициализации ключа для распределения нового ключа, как описано в 8.1, другой предлагает автоматическое обновление мастер-ключа путем использования чувствительного к вычислениям алгоритма Диффи-Хеллмана (DH) для согласования нового ключа. Для бюджетных устройств, которые не обеспечивают использование алгоритма DH, но требуют определенного уровня защиты от возможных атак, периодическое обновление мастер-ключа может выполняться вручную аналогично инициализации ключа. Для прочих устройств, обладающих большей вычислительной мощностью, может использоваться механизм согласования ключа алгоритмом DH, обеспечивающий автоматическое обновление мастер-ключа в течение указанного периода времени. В целях безопасности общие «секретные» данные должны обновляться через заданные интервалы, включая как ключ пользователя, так и ключи провайдера услуг. Что касается мастер-ключа, то его обновление зависит от поставщиков.

Прежде чем описывать механизм обновления мастер-ключа на основе алгоритма DH, необходимо кратко описать протокол согласования ключа алгоритмом DH. Для протокола необходимы два системных параметра p и g. Оба они являются открытыми и могут использоваться всеми пользователями системы. Параметр p представляет собой простое число, а параметр g (обычно называемый генератором) является целым числом, меньше p, способным генерировать каждый элемент от 1 до p-1 при умножении на самого себя несколько раз, по модулю равный простому числу p. Таким образом, узел KSN и заданное устройство могут использовать протокол согласования ключа алгоритмом DH, чтобы согласовать общий секретный ключ. Далее по тексту новый мастер-ключ будет использоваться для обозначения нового ключа пользователя или ключа провайдера услуг, а предварительный мастер-ключ будет использоваться для обозначения подлежащего обновлению ключа пользователя или ключа провайдера услуг. Для обеспечения безопасности генерирования ключа и протокола Диффи-Хеллмана важным условием являются достаточная длина ключа и непрогнозируемое случайное собственное значение. Шаги процедуры активации распределения нового мастер-ключа на устройство узлом KSN с использованием протокола SCPM, а также процедуры использования предварительной версии общих

секретных данных, предварительного мастер-ключа, для аутентификации двух одноранговых узлов показаны на рисунке 19 и включают следующее:

a) узел KSN генерирует случайное значение закрытого ключа и для него вычисляет значение открытого ключа с использованием параметров p и g и закрытого ключа, после чего сохраняет вычисленное алгоритмом DH открытое значение ключа в поле PADATA, запускает службы аутентификации для проверки подлинности данных команды обмена с помощью предварительного мастер-ключа и затем передает открытое значение ключа на устройство;

b) устройство получает и проверяет команду обмена открытым значением ключа DH и значением предварительного мастер-ключа. Если проверка прошла успешно, устройство получает открытый ключ DH узла KSN;

c) устройство увеличивает порядковый номер на 1, подготавливает сообщение-ответ по обмену открытым значением ключа DH, аутентифицированное предварительным мастер-ключом, и передает его в узел KSN;

d) узел KSN проверяет ответ по обмену открытым значением и получает новый порядковый номер, обмен открытым значением ключа подтверждается;

e) устройство генерирует случайное собственное значение закрытого ключа и для него вычисляет значение открытого ключа с использованием параметров p и g и собственного значения, затем сохраняет вычисленное алгоритмом DH открытое значение в поле PADATA, включает службу проверки подлинности данных для аутентификации данных команды обмена открытым значением DH от предварительного мастер-ключа и затем передает ее на узел KSN;

f) узел KSN получает и проверяет команду обмена открытым значением ключа DH от предварительного мастер-ключа. Если проверка прошла успешно, узел KSN получает открытое значение ключа DH устройства;

g) узел KSN увеличивает порядковый номер на 1, подготавливает сообщение-ответ по обмену открытым значением ключа DH, аутентифицированное предварительным мастер-ключом, и передает его на устройство;

h) устройство проверяет ответ по обмену открытым значением ключа и получает новый порядковый номер, обмен открытым значением ключа подтверждается;

i) узел KSN вычисляет общий секретный ключ с помощью своего закрытого значения ключа и значения открытого ключа устройства. Устройство вычисляет общий секретный ключ с помощью своего закрытого значения ключа и открытого значения ключа узла KSN. Оба они извлекают одинаковое значение ключа по алгоритму DH, которое называют общим секретным ключом;

j) узел KSN генерирует/возвращает новый мастер-ключ, сохраняет его со связанными индексом ключа, размером ключа и алгоритмом в поле PADATA, запускает службы аутентификации и конфиденциальности для шифрования и проверки подлинности данных команды на обновление нового мастер-ключа с помощью общего секретного ключа, вычисленного по алгоритму DH, а затем передает его на устройство;

k) устройство получает и проверяет команду на обновление нового мастер-ключа от общего секретного ключа, вычисленного согласно алгоритму DH;

l) если проверки прошли успешно, устройство подготавливает ответ по обновлению нового мастер-ключа путем увеличения порядкового номера на 1, шифрования данных ответа (поля: PBC, PADATA, BCC и PDG) и добавления данных аутентификации (MDAS) от общего секретного ключа, после чего передает их на узел KSN;

m) узел KSN получает и проверяет ответ по обновлению нового мастер-ключа, возвращает новый порядковый номер и подтверждает, что обмен прошел успешно.

В перечислениях a)—h) два объекта (узел KSN и устройство) обмениваются открытым значением ключа DH с использованием предварительного мастер-ключа для взаимной проверки подлинности.

В пункте i) два объекта по отдельности вычисляют общий секретный ключ согласно алгоритму DH.

В пунктах k)—n) узел KSN распределяет новый мастер-ключ, защищенный вычисленным общим секретным ключом, а устройство проверяет его.

На рисунке 19 показано, что механизм обновления мастер-ключа состоит из трех круговых циклов передачи данных. Первый круговой цикл инициируется узлом KSN и аутентифицируется устройством для получения открытого значения ключа DH узла KSN. Второй круговой цикл инициируется устройством и аутентифицируется узлом KSN для получения открытого значения ключа DH устройства. После получения двумя объектами (узлом KSN и устройством) открытого значения ключа DH противоположного однорангового узла и использования алгоритма DH для вычисления общего секретного ключа третий круговой цикл выполняет передачу нового мастер-ключа.

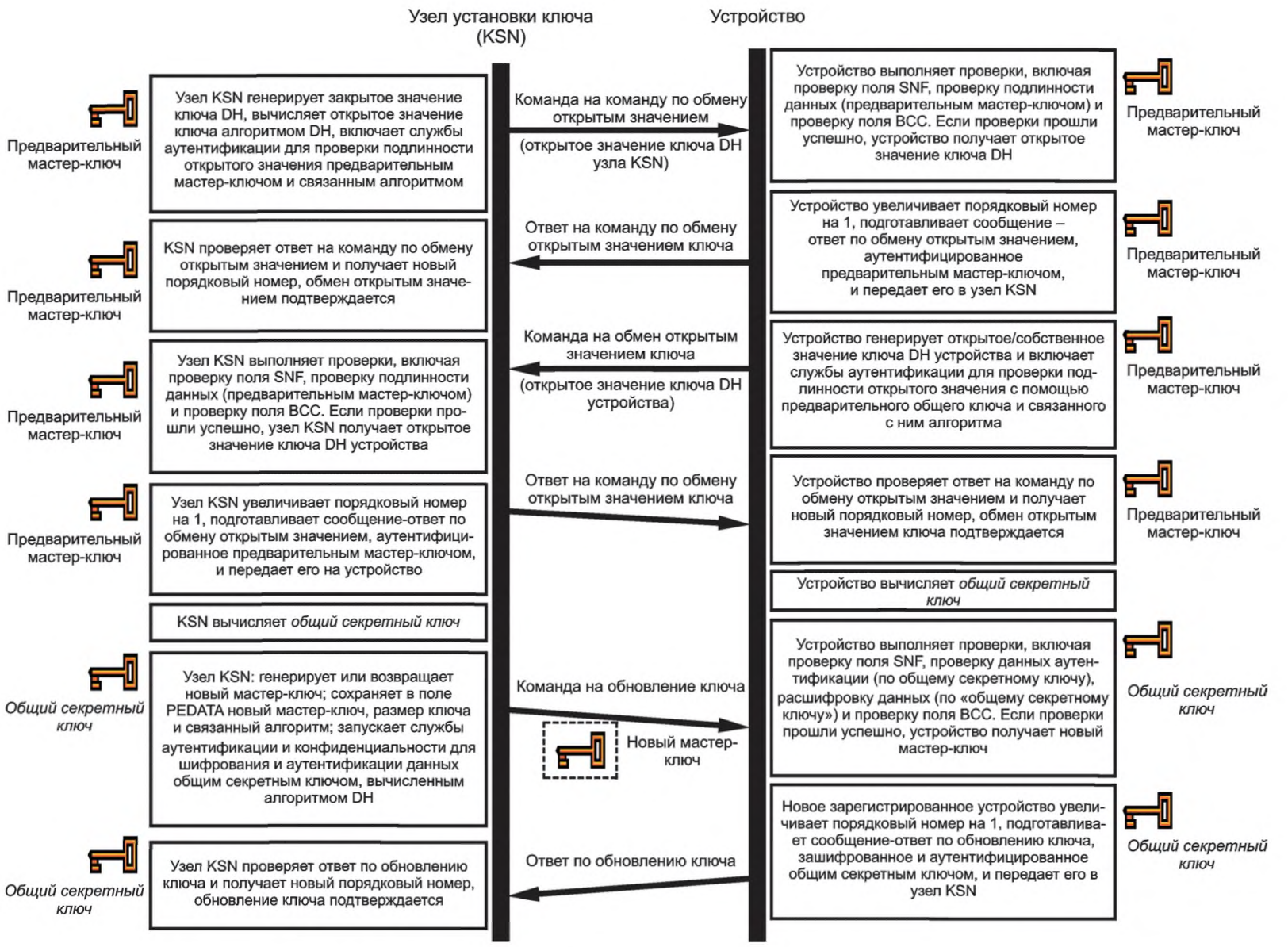

Рисунок 19 — Последовательность обновления мастер-ключа под контролем узла KSN с использованием алгоритма DH

На рисунке 20 показаны кадры сообщений первого кругового цикла, которыми обмениваются узел KSN и устройство. Команды по обмену открытым значением ключа включают информацию защищенного заголовка (b0:b1:b2:b3 = 0:0:0:1 как индекс ключа пользователя или 0:0:1:1 ~ 1:1:1:1 как индекс ключа провайдера услуг, b6:b7 = 0:1 для включенной аутентификации и выключенного шифрования, b8=0 для сообщения-запроса), индикатор, указывающий на то, что сообщение представляет собой обмен открытым значением ключа, а также включает открытое значение ключа DH, которое хранится в поле PADATA. Успешный ответ и ошибка ответа также показаны на рисунке 20. Различия между успешным ответом и ошибкой ответа следующие:

a) результат ответа будет указан в битах b12:b13:b14:b15 поля SHD;

b) если ответ успешный, значение поля SNF увеличивается на 1. В случае ошибки значение поля SNF остается таким же, что и в предыдущем ответе;

c) в случае ошибки ответа данные поля PADATA в сообщении-ответе копируются из сообщения-запроса, но данные аутентификации вычисляются от поля SA до шифрованных данных (включая поля: PBC, PADATA и BCC). В случае успешного ответа информация ответа вносится в поле PADATA.

Для второго кругового цикла кадр сообщения практически такой же, как на рисунке 20.

На рисунке 21 показаны кадры сообщений третьего кругового цикла, которыми обмениваются узел KSN и устройство. Команда на обновление мастер-ключа включает информацию защищенного заголовка (b0:b1:b2:b3 = 0:0:0:0 и b4 = 1 указывает на то, что сообщение защищено общим секретным ключом DH, вычисленным на предыдущем шаге, b6:b7 = 0:0 означает включенную проверку подлинности данных и включенное шифрование, b8=0 для сообщения-запроса), новый мастер-ключ, а также размер ключа и соответствующий алгоритм, хранящиеся в полях PADATA, PBC, PADATA, BCC и PDG, шифруются с помощью общего секретного ключа DH. Весь кадр сообщения, за исключением полей HD и MDAS, также аутентифицируется с помощью общего секретного ключа DH.

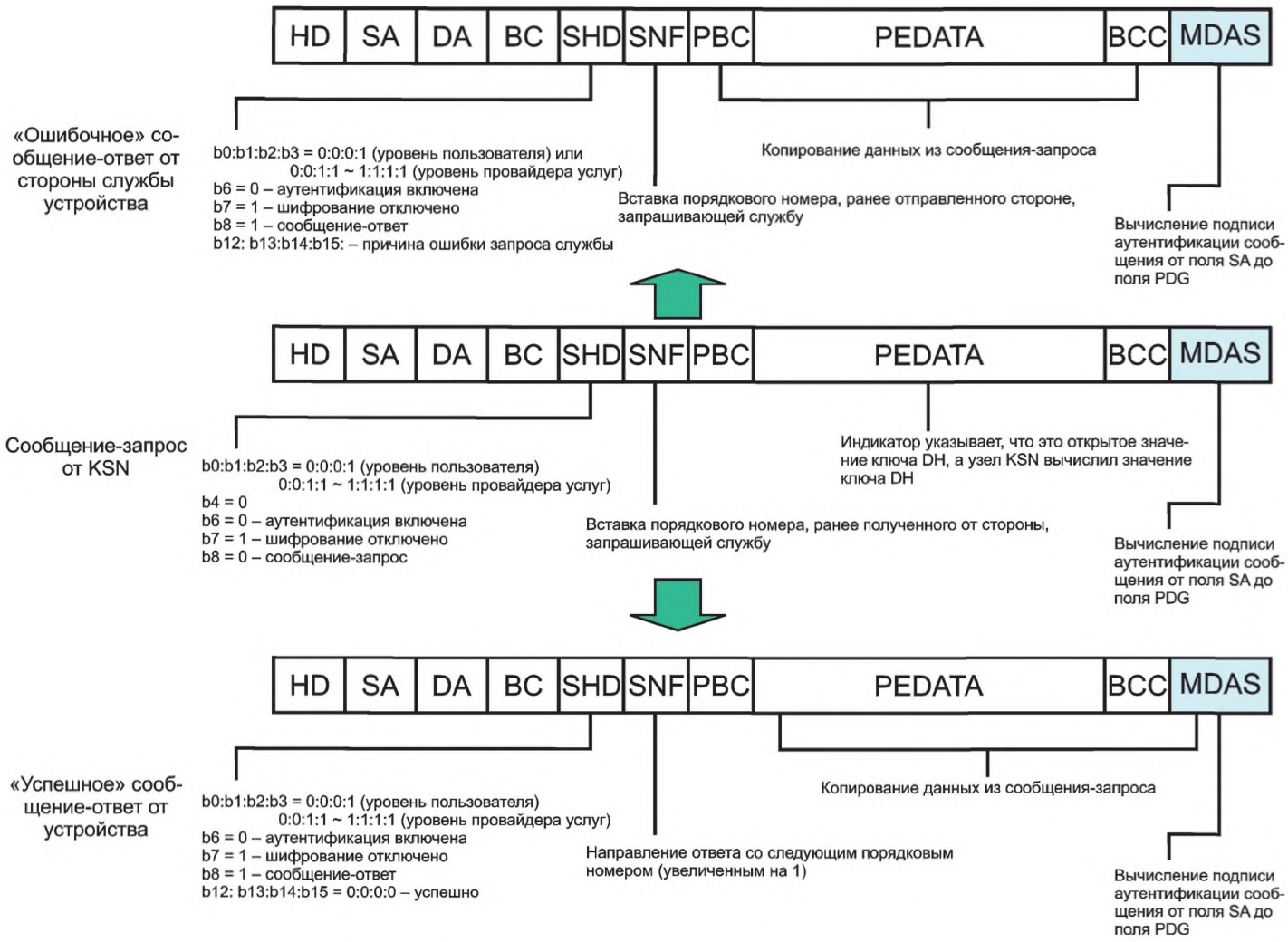

Рисунок 20 — Кадры защищенного сообщения по обновлению мастер-ключа. Обмен открытым значением ключа

Успешный ответ и ошибка ответа также показаны на рисунке 21. Различия между успешным ответом и ошибкой ответа следующие:

a) результат ответа будет указан в битах b12:b13:b14:b15 поля SHD;

b) если ответ успешный, значение поля SNF увеличивается на 1. В случае ошибки значение поля SNF остается таким же, что и в предыдущем ответе;

c) в случае ошибки ответа зашифрованные данные в сообщении-ответе копируются из сообщения-запроса, но данные аутентификации вычисляются от поля SA до шифрованных данных (включая поля: PBC, PADATA, BCC и PDG). В случае успешного ответа информация ответа вносится в поле PADATA.

9.3.2 Синхронизация ключа

Обновление мастер-ключа в некоторых случаях может вызвать проблемы с синхронизацией. Например, задержка по времени между устройствами при получении нового мастер-ключа при обновлении мастер-ключа может потенциально привести к несовместимости общих секретных ключей.

На рисунке 22 показан способ обеспечения синхронизации общих «секретных данных» двух узлов, где узел KSN играет центральную роль в контролировании переходных состояний ключа по каждому устройству.

Узел KSN сохраняет список (в соответствии с порядком ввода серийных ключей), в котором регистрируются все управляемые им устройства, затем обновляет ключи и выдает запросы на переход состояния на управляемые им устройства в соответствии с порядком в списке.

Устройство должно хранить два ключа (предварительный мастер-ключ и новый мастер-ключ) одновременно, пока не будет обеспечено полное обновление нового мастер-ключа на всех устройствах.

Узел KSN передает команду нового мастер-ключа, защищенную службами аутентификации данных и шифрования с помощью предварительного мастер-ключа, на управляемое устройство. Когда устройство получает запрос на обновления нового мастер-ключа, оно может получить новый мастер-ключ из кадра защищенного сообщения с помощью предварительного мастер-ключа и поменять его текущее состояние с нормального режима на режим «ключ получен».

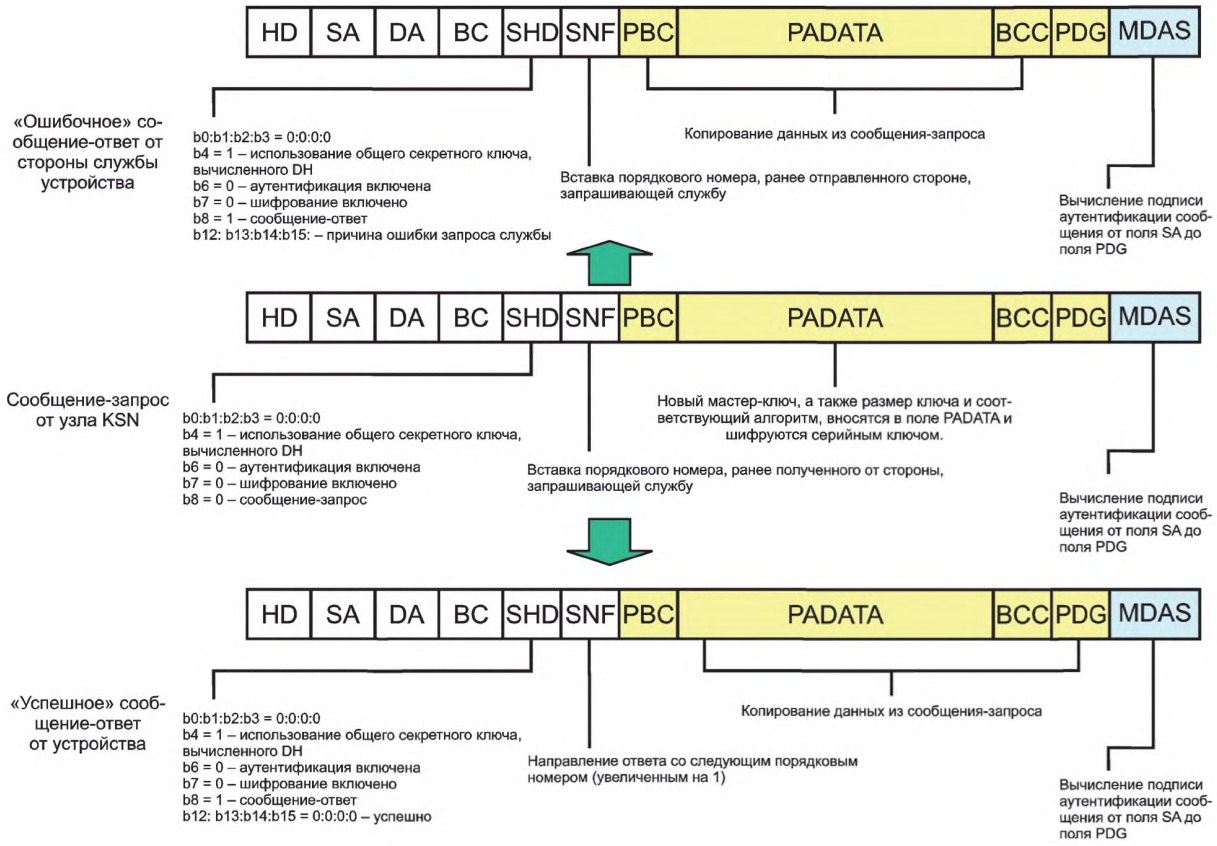

Рисунок 21 — Кадры защищенного сообщения по обновлению мастер-ключа. Обмен ключом с использованием общего секретного ключа DH

После того, как узел KSN подтвердит передачу запроса на обновление нового мастер-ключа всем управляемым устройствам, он будет передавать «запрос на переход состояния ключа: обновление», защищенный службами аутентификации данных и шифрования, используя предварительный мастер-ключ для всех устройств, которые могут принять запрос на обновление нового мастер-ключа. Когда устройство получит «запрос на переход состояния ключа: обновление», оно изменит свой текущий статус с «ключ получен» на «обновление».

Когда узел KSN подтвердит, что новый мастер-ключ установлен на управляемые им устройства, он направит «запрос на переход состояния ключа: нормальный режим», защищенный службами аутентификации данных и шифрования, используя предварительный мастер-ключ для всех управляемых им устройств для защиты устройств от хакеров. После получения и проверки запроса устройством оно изменит текущий статус с «обновление» на «нормальный режим».

На рисунке 23 показана схема изменения состояния ключа устройства. Три состояния: «нормальный режим», «ключ получен» и «обновление» описываются следующим образом:

a) нормальный режим: означает, что узел KSN уверен, что все управляемые им устройства получили самый новый ключ, этот ключ сохранен и используется в устройстве при связи с другими узлами;

b) ключ получен: указывает на то, что устройство получило запрос на обновление мастер-ключа от узла KSN и успешно приобрело новый мастер-ключ. Но из-за возможного асинхронного обновления мастер-ключа на всех устройствах в одном домене самый новый ключ может не сразу вступить в действие. Когда устройство выдает запрос о защищенной передаче данных, по-прежнему используется предварительный мастер-ключ. Но при интерпретации команды-запроса от других устройств может использоваться предварительный мастер-ключ либо новый мастер-ключ;

c) обновление ключа: узел KSN выдает запрос на переход состояния ключа: обновление на все устройства. Устройство переходит в данное состояние после получения запроса от узла KSN. В данном состоянии новый мастер-ключ используется, когда устройство выдает защищенную передачу данных. Но при интерпретации сообщения-запроса от других устройств может использоваться либо предварительный мастер-ключ, либо новый мастер-ключ;

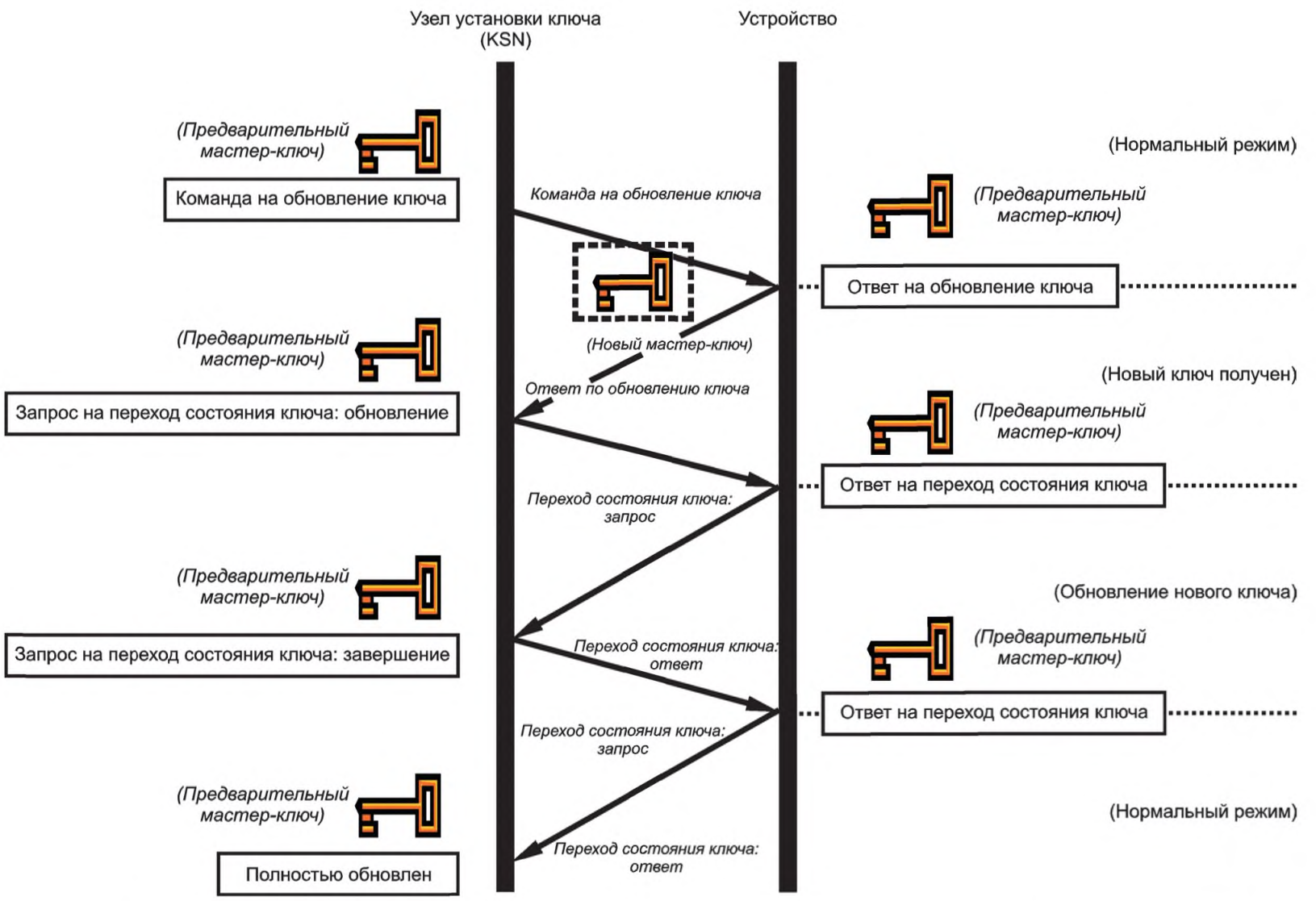

Рисунок 22 — Последовательность обновления мастер-ключа для синхронизации общих «секретных данных» двух узлов

d) нормальный режим: узел KSN выдает «запрос на переход состояния ключа: нормальный режим» на все устройства. Устройство переходит в данное состояние после получения запроса от узла KSN. Действующим ключом является самый новый ключ.

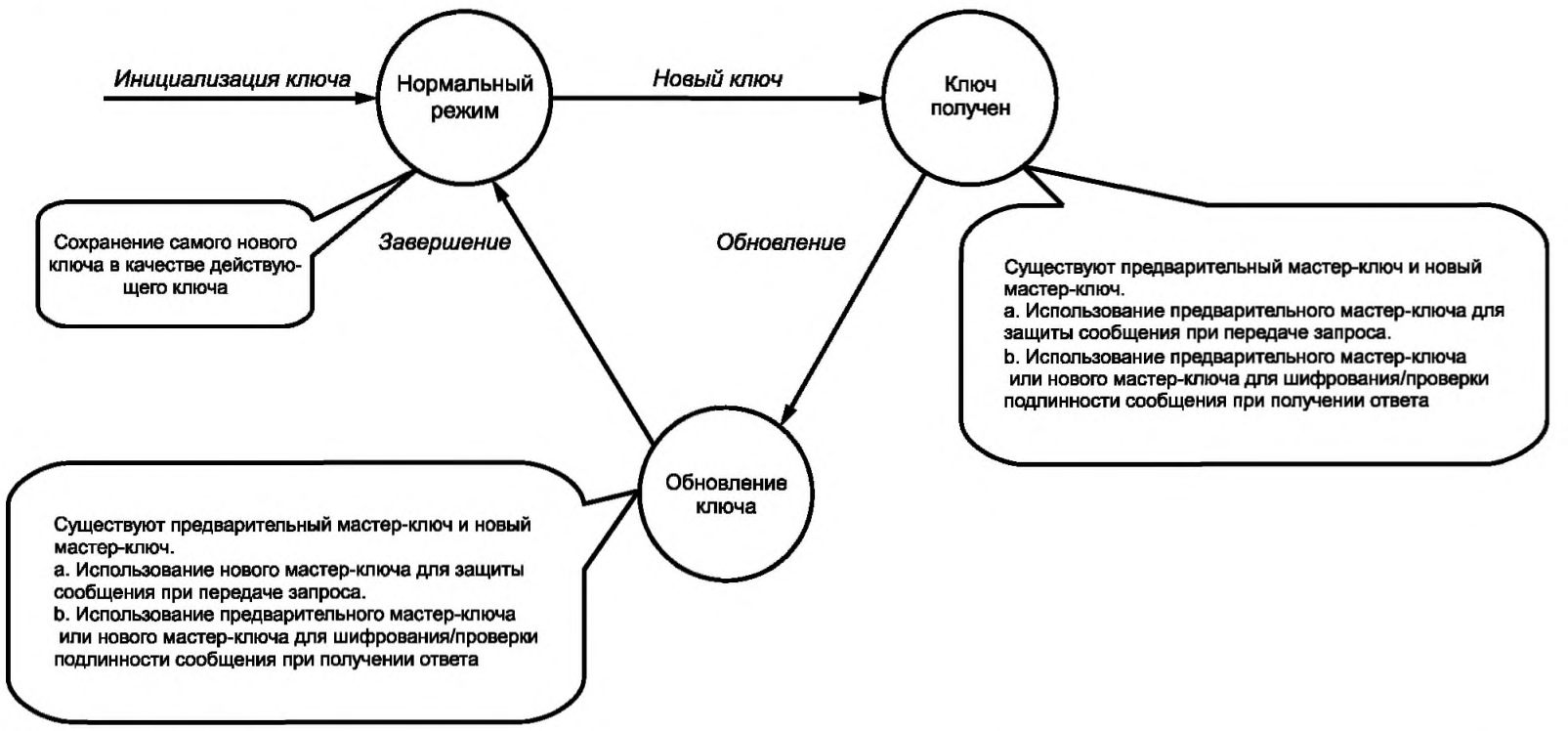

Рисунок 23 — Схема перехода устройства из одного состояния в другое состояние в ходе обновления мастер-ключа под контролем узла KSN

9.3.3 Запрос на обновление мастер-ключа от устройства

В случае длительного отключения устройства от сети питания общие «секретные» данные (ключ пользователя или ключи провайдера услуг) данного устройства и других устройств могут быть несовместимы, то есть общие «секретные» данные, сохраненные в устройстве, могут быть устаревшими. Они перестанут являться текущими ключами или предыдущими ключами, которыми владеет домен.

Как описано в 8.2.2, узел KSN сохраняет список, в который заносятся управляемые им устройства. Узел KSN также сохраняет в списке информацию соответствующего этапа (стадии разработки) о ключах для каждого устройства. В случае подключения устройства к сети после включения электропитания оно выдает запрос на обновление мастер-ключа на узел KSN, поскольку неизвестно, устарели ли ключи, которыми оно владеет. Далее старый ключ будет использован для определения различий с предварительным мастер-ключом. Последовательность описана ниже и показана на рисунке 24:

a) устройство выдает запрос на обновление мастер-ключа (ключа пользователя или ключей провайдера услуг) на узел KSN, защищенный службами проверки подлинности данных и конфиденциальности с использованием старого ключа, сохраненного в устройстве. Индекс ключей указан в битах — b0:b1:b2:b3 поля SHD;

b) узел KSN получает и проверяет запрос, подготавливает сообщение, содержащее новый мастер-ключ и связанный с ним размер ключа и алгоритм, а затем передает сообщение (защищенное службами проверки подлинности данных и конфиденциальности с использованием старого ключа, используемого устройством) на устройство;

c) устройство получает и проверяет сообщение, на которое отвечает узел KSN, получает новый мастер-ключ и затем отвечает защищенным ответом узлу KSN.

Для обеспечения безопасности узел KSN может установить безопасный срок для каждого поддерживаемого поколения ключей. Узел KSN может сбрасывать ключи с истекшим безопасным сроком. Если старые ключи не сохранились в узле KSN, узел не сможет проверить запрос на обновление мастер-ключа, который защищен старым ключом и направлен с устройства. В этом случае должна быть повторно выполнена инициализация ключа (см. 8.1).

Поскольку запрос обновления мастер-ключа выдается с устройства после включения питания устройства и подключения к сети, проблемы синхронизации обновления мастер-ключа (описанные в 8.2.3) не возникнут, так как узел KSN уже выполнил обновление мастер-ключа для других устройств, подключенных к сети. Переход состояния ключа устройства становится проще, как показано на рисунке 25.

Горячий пуск означает, что устройство снова включено в электросеть и подключается к домашней сети. Затем устройство выдает запрос на обновление мастер-ключа в узел KSN, защищенный старым ключом.

Состояние «ключ получен» указывает на то, что устройство получило команду на обновление мастер-ключа от узла KSN и успешно приобрело новый мастер-ключ. Самый новый ключ может не сразу вступить в действие. Старый ключ все еще может использоваться, когда устройство выдает защищенные сообщения. В этом случае при интерпретации команды-запроса от других устройств может использоваться старый ключ либо новый мастер-ключ.

Нормальный режим означает, что устройство отвечает посредством команды на обновление ключа в узел KSN. Действующим ключом является самый новый ключ.

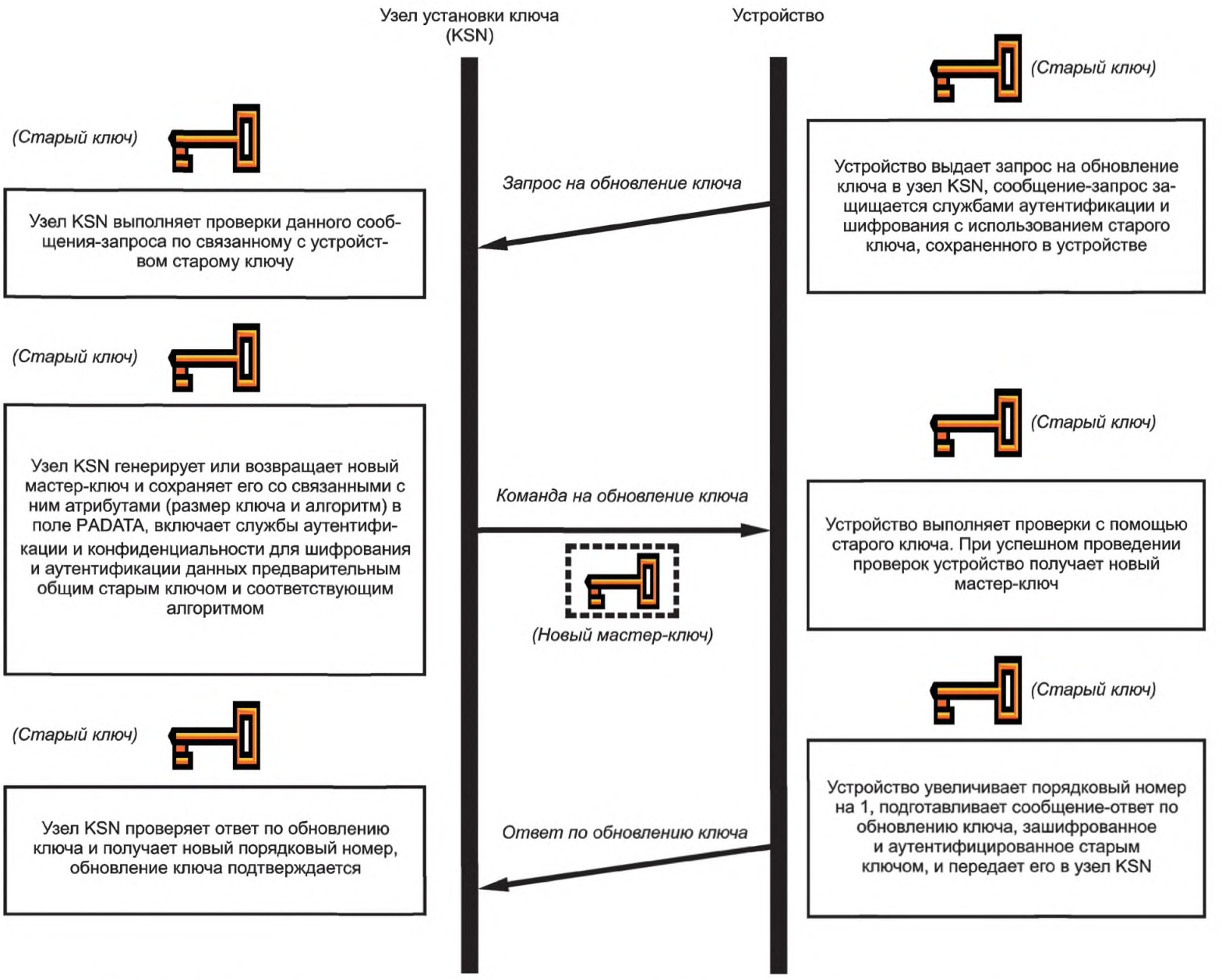

Рисунок 24 — Последовательность обновления мастер-ключа, запрашиваемого устройством

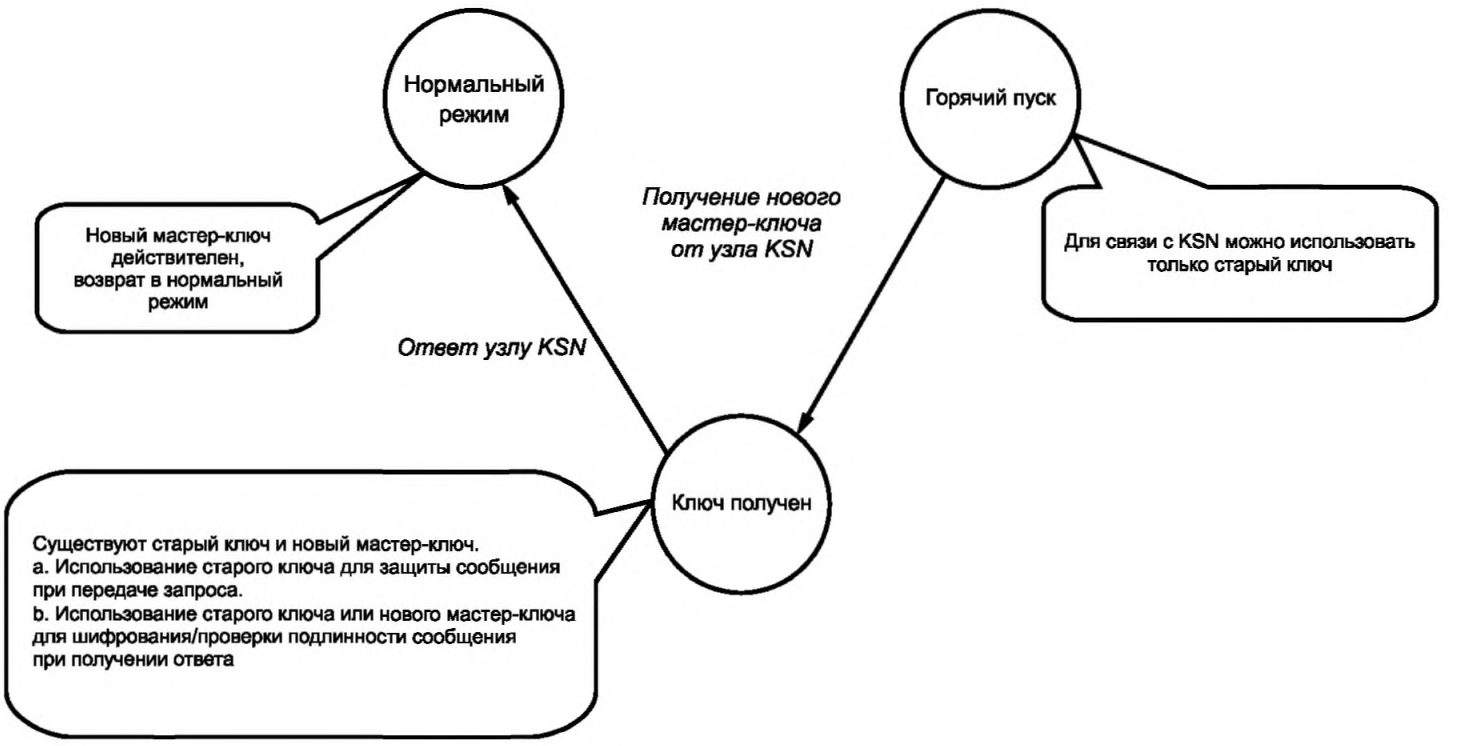

Рисунок 25 — Схема перехода устройства из одного состояния в другое состояние в ходе обновления мастер-ключа по запросу от устройства

Приложение А
(справочное)

Авторизация узла установки ключа

Как объяснялось в разделе 9, узел KSN играет важную роль в доставке, обновлении и хранении всех ключей. Узел KSN должен быть очень надежным устройством. Однако как владелец дома может обеспечить надежность данного узла? На рисунке А.1 показан пример проверки подлинности узла KSN поставщиком KSN, когда новый узел устанавливается и подключается к сети Интернет. Доверительные отношения передаются за счет доверия владельца дома поставщику KSN, а поскольку подлинность KSN надежно проверена поставщиком, владелец дома не будет сомневаться в надежности узла KSN. Аутентификация между узлом KSN и поставщиком должна осуществляться с помощью интернет-технологий обеспечения безопасности, таких как протокол SSL.

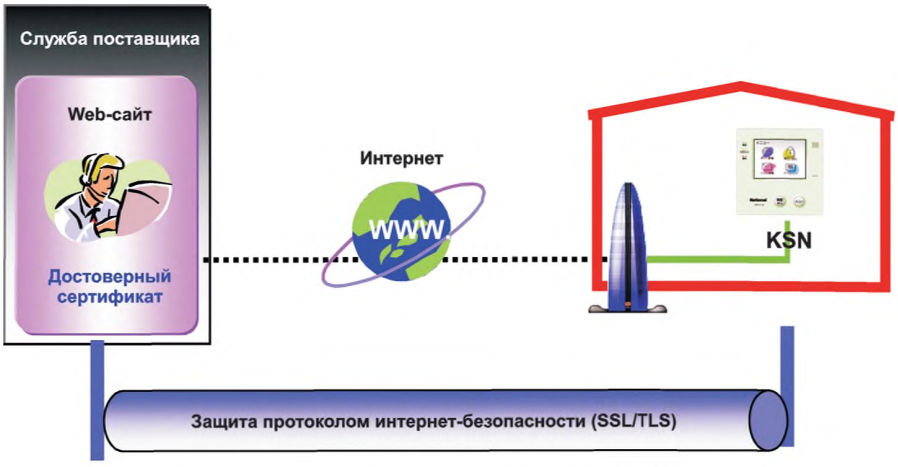

Рисунок А.1 — Пример аутентификации узла KSN

Приложение ДА
(справочное)

Сведения о соответствии ссылочного международного стандарта национальному стандарту Российской Федерации

Таблица ДА

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
ISO/IEC 10116	—	*
* Соответствующий национальный стандарт отсутствует. До его утверждения рекомендуется использовать перевод на русский язык данного международного стандарта. Перевод данного международного стандарта находится в Федеральном информационном фонде стандартов.		

Библиография

[1] ISO/IEC 9797-1 Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher (*Информационные технологии. Методы защиты. Коды проверки подлинности сообщения (*MAC). *Часть 1. Механизмы, использующие блочный шифр*)

[2] Dworkin, M., Recommendation for Block Cipher Modes of Operation: Methods and Techniques, NIST Special (Дворкин М. Рекомендации по режимам работы блочного шифра: методы и приемы // NIST Special)

[3] Black John and Rogaway Johnson Comments to NIST concerning AES Modes of Operations: A Suggestion for Handling Arbitrary-Length Messages with the CBC MAC (Блэк Дж., Рогавей Дж. Комментарии NIST по режимам работы AES: Предложение по обработке сообщений произвольной длины с использованием CBC MAC)

[4] NIST, FIPS PUB 197, Advanced Encryption Standard (AES), November 2001 (Симметричный алгоритм блочного шифрования (AES) // NIST, FIPS PUB 197, ноябрь 2001 г.)

УДК 004.056:006.354 ОКС 35.110, 35.200, 35.240.99

Ключевые слова: защита прав потребителя, единство измерений, конкурентоспособность, безопасность работ и услуг

БЗ 9—2018/80

Редактор *Н.А. Аргунова*
Технический редактор *В.Н. Прусакова*
Корректор *Е.Д. Дульнева*
Компьютерная верстка *Е.О. Асташина*

Сдано в набор 06.09.2018. Подписано в печать 27.09.2018. Формат 60×84 1/8. Гарнитура Ариал.
Усл. печ. л. 4,65. Уч.-изд. л. 4,21.
Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении ФГУП «СТАНДАРТИНФОРМ» для комплектования Федерального информационного фонда стандартов, 117418 Москва, Нахимовский пр-т, д. 31, к. 2.

gost.e-ecolog.ru gost.e-ecolog.ru

gost.e-ecolog.ru