ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО 9735-6— 2012

ЭЛЕКТРОННЫЙ ОБМЕН ДАННЫМИ В УПРАВЛЕНИИ, ТОРГОВЛЕ И НА ТРАНСПОРТЕ (EDIFACT)

Синтаксические правила для прикладного уровня

(версия 4, редакция 1)

Часть 6

Сообщение для защищенной аутентификации и защищенного квитирования (тип сообщения – AUTACK)

ISO 9735-6:2002
Electronic data interchange for administration, commerce and transport (EDIFACT) — Application level syntax rules (Syntax version number: 4, Syntax release number: 1) — Part 6: Secure authentication and acknowledgement message (message type – AUTACK)
(IDT)

Издание официальное

Москва
Стандартинформ
2014

gost.e-ecolog.ru

Предисловие

1 ПОДГОТОВЛЕН ЗАО «Проспект» совместно с Ассоциацией автоматической идентификации «ЮНИСКАН/ГС1 РУС» на основе собственного аутентичного перевода на русский язык международного стандарта, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 55 «Терминология, элементы данных и документация в бизнес-процессах и электронной торговле»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 20 ноября 2012 г. № 976-ст

4 Настоящий стандарт идентичен международному стандарту ИСО 9735-6:2002 «Электронный обмен данными в управлении, торговле и на транспорте (EDIFACT). Синтаксические правила для прикладного уровня (версия 4, редакция 1). Часть 6. Сообщение для защищенной аутентификации и защищенного квитирования (тип сообщения – AUTACK)» (ISO 9735-6:2002 «Electronic data interchange for administration, commerce and transport (EDIFACT) — Application level syntax rules (Syntax version number: 4, Syntax release number: 1) — Part 6: Secure authentication and acknowledgement message (message type – AUTACK)»).

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 ГОСТ Р 1.0—2012 (раздел 8). 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 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.ru).

Стандартинформ, 2014

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 Соответствие стандарту 1
3 Нормативные ссылки 1
4 Термины и определения 2
5 Правила использования сообщения для защищенной аутентификации и защищенного квитирования 2
Приложение А (справочное) Примеры сообщений AUTACK 8
Приложение В (справочное) Службы и алгоритмы защиты 31
Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов ссылочным национальным стандартам Российской Федерации 37
Библиография 38

Введение

Настоящий стандарт включает в себя правила прикладного уровня для структурирования данных в рамках обмена электронными сообщениями в открытой среде, с учетом требований пакетной или интерактивной обработки. Эти правила утверждены Европейской экономической комиссией Организации Объединенных Наций (UN/ECE) в качестве синтаксических правил электронного обмена данными в управлении, торговле и на транспорте (EDIFACT) и являются частью «Справочника по обмену торговыми данными Организации Объединенных Наций» (UNTDID[1)]), который содержит также рекомендации по разработке сообщений пакетного и интерактивного обмена.

Спецификации и протоколы связи не рассматриваются в настоящем стандарте.

Настоящий стандарт предоставляет дополнительные возможности защиты пакетных структур EDIFACT, т.е. сообщений, пакетов, групп или обменов, с помощью сообщения для защищенной аутентификации и защищенного квитирования.

Комплекс стандартов ИСО 9735 состоит из следующих частей под общим названием «Электронный обмен данными в управлении, торговле и на транспорте (EDIFACT). Синтаксические правила для прикладного уровня (версия 4, редакция 1)»:

— Часть 1. Синтаксические правила, общие для всех частей;

— Часть 2. Синтаксические правила, специфичные для пакетного ЭОД;

— Часть 3. Синтаксические правила, специфичные для интерактивного ЭОД;

— Часть 4. Сообщение синтаксического и служебного уведомления для пакетного ЭОД (тип сообщения — CONTRL);

— Часть 5. Правила защиты для пакетного ЭОД (аутентичность, целостность и неотказуемость источника);

— Часть 6. Сообщение для защищенной аутентификации и защищенного квитирования (тип сообщения — AUTACK);

— Часть 7. Правила защиты для пакетного ЭОД (конфиденциальность);

— Часть 8. Ассоциированные данные в ЭОД;

— Часть 9. Сообщение для управления ключами и сертификатами защиты (тип сообщения — KEYMAN);

— Часть 10. Справочники служебных синтаксических структур.

[1)] Сокращение от United Nations Trade Data Interchange Directory.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ЭЛЕКТРОННЫЙ ОБМЕН ДАННЫМИ В УПРАВЛЕНИИ, ТОРГОВЛЕ И НА ТРАНСПОРТЕ (EDIFACT)
Синтаксические правила для прикладного уровня
(версия 4, редакция 1)
Часть 6
Сообщение для защищенной аутентификации и защищенного квитирования
(тип сообщения – AUTACK)

Electronic data interchange for administration, commerce and transport (EDIFACT).
Application level syntax rules
(Syntax version number: 4, Syntax release number: 1).
Part 6. Secure authentication and acknowledgement message
(message type – AUTACK)

Дата введения – 2014—01—01

1 Область применения

В настоящем стандарте для обеспечения безопасности электронного обмена данными в управлении, торговле и на транспорте (EDIFACT) введено определение сообщения для защищенной аутентификации и защищенного квитирования – AUTACK.

2 Соответствие стандарту

Для соответствия обмена настоящему стандарту должен использоваться номер версии "4" в обязательном элементе данных 0002 (номер версии синтаксических правил) и номер редакции "01" в условном элементе данных 0076 (номер редакции синтаксических правил). Каждый из этих элементов данных входит в сегмент UNB (заголовок обмена). В обменах, в которых продолжает использоваться синтаксис более ранних версий, для различения соответствующих синтаксических правил необходимо указывать следующие номера версий:

- ИСО 9735:1988 - Номер версии синтаксических правил: 1;
- ИСО 9735:1988 (перепечатанный с изменениями в 1990 г.) - Номер версии синтаксических правил: 2;
- ИСО 9735:1988 с Изменением 1:1992 - Номер версии синтаксических правил: 3;
- ИСО 9735:1998 - Номер версии синтаксических правил: 4.

Соответствие стандарту означает, что соблюдены все его требования, включая опции. Если же поддерживаются не все опции, то в любом заявлении о соответствии должно содержаться положение, идентифицирующее опции, по которым декларируется соответствие.

Данные, используемые в обмене, признаются соответствующими настоящему стандарту, если их структура и представление отвечают синтаксическим правилам, определенным в настоящем стандарте.

Устройства, поддерживающие настоящий стандарт, признаются соответствующими ему, если они способны формировать и/или интерпретировать данные, структурированные и представленные в соответствии с требованиями настоящего стандарта.

Для соответствия требованиям настоящего стандарта необходимо также соответствие требованиям частей 1, 2, 5 и 10 комплекса стандартов ИСО 9735.

Положения других стандартов, указанных в настоящем стандарте, являются составными элементами критериев соответствия настоящему стандарту.

3 Нормативные ссылки

В настоящем стандарте использованы ссылки на следующие нормативные документы, положения которых необходимо учитывать при использовании настоящего стандарта. В случае ссылок на документы, у которых указана дата утверждения, необходимо пользоваться только указанной редакцией. В случае, когда дата утверждения не приведена, следует пользоваться последней редакцией ссылочных документов, включая любые поправки и изменения к ним.

Издание официальное

ИСО 9735-1:2002 Электронный обмен данными в управлении, торговле и на транспорте (EDIFACT). Синтаксические правила для прикладного уровня (версия 4, редакция 1). Часть 1. Синтаксические правила, общие для всех частей (ISO 9735-1:2002, Electronic data interchange for administration, commerce and transport (EDIFACT) — Application level syntax rules (Syntax version number: 4, Syntax release number: 1) — Part 1: Syntax rules common to all parts)

ИСО 9735-2:2002 Электронный обмен данными в управлении, торговле и на транспорте (EDIFACT). Синтаксические правила для прикладного уровня (версия 4, редакция 1). Часть 2. Синтаксические правила, специфичные для пакетного ЭОД (ISO 9735-2:2002, Electronic data interchange for administration, commerce and transport (EDIFACT) — Application level syntax rules (Syntax version number: 4, Syntax release number: 1) — Part 2: Syntax rules specific to batch EDI)

ИСО 9735-5:2002 Электронный обмен данными в управлении, торговле и на транспорте (EDIFACT). Синтаксические правила для прикладного уровня (версия 4, редакция 1). Часть 5. Правила защиты для пакетного ЭОД (аутентичность, целостность и неотказуемость источника) (ISO 9735-5:2002, Electronic data interchange for administration, commerce and transport (EDIFACT) — Application level syntax rules (Syntax version number: 4, Syntax release number: 1) — Part 5: Security rules for batch EDI (authenticity, integrity and non-repudiation of origin))

ИСО 9735-10:2002 Электронный обмен данными в управлении, торговле и на транспорте (EDIFACT). Синтаксические правила для прикладного уровня (версия 4, редакция 1). Часть 10. Справочники служебных синтаксических структур (ISO 9735-10:2002, Electronic data interchange for administration, commerce and transport (EDIFACT) — Application level syntax rules (Syntax version number: 4, Syntax release number: 1) — Part 10: Syntax service directories)

4 Термины и определения

В настоящем стандарте используются термины и определения, приведенные в ИСО 9735-1.

5 Правила использования сообщения для защищенной аутентификации и защищенного квитирования

5.1 Функциональное определение

AUTACK – это сообщение, аутентифицирующее переданные структуры либо обеспечивающее защищенное квитирование принятых структур, обменов, групп, сообщений или пакетов.

Сообщение для защищенной аутентификации и защищенного квитирования может использоваться:

a) для обеспечения защищенной аутентификации, целостности или неотказуемости источника сообщений, пакетов, групп или обменов;

b) для защищенного квитирования или обеспечения неотказуемости приема защищенных сообщений, пакетов, групп или обменов.

5.2 Сферы применения

Сообщение для защищенной аутентификации и защищенного квитирования (AUTACK) может использоваться как во внутренней, так и во внешней торговле. Оно разработано на основе распространенной практики в управлении, коммерции и на транспорте и не зависит от сферы бизнеса или промышленности.

5.3 Принципы

5.3.1 Общие положения

Применяемые процедуры защиты подлежат согласованию между торговыми партнерами и определению в соглашении об обмене.

Сообщение для защищенной аутентификации и защищенного квитирования (AUTACK) позволяет использовать службы защиты для других структур EDIFACT (сообщений, пакетов, групп или обменов) и обеспечивает защищенное квитирование защищенных структур EDIFACT. Оно может применяться для комбинаций структур EDIFACT, которые необходимо защитить при обмене данными между двумя сторонами.

Службы защиты обеспечиваются за счет применения механизмов шифрования к содержимому исходных структур EDIFACT. В результате формируется тело сообщения AUTACK, дополненное такими существенными данными, как указатели на использованные методы шифрования, контрольные номера структур EDIFACT и данные о дате и времени исходных структур.

В сообщении AUTACK должны использоваться стандартные группы заголовка и окончания защиты.

Сообщение AUTACK применимо к одному или нескольким сообщениям, пакетам или группам из одного или нескольких обменов, либо к одному или нескольким обменам. Например, на рисунке 1 показан обмен, при котором сообщение AUTACK передается совместно с одним или несколькими сообщениями.

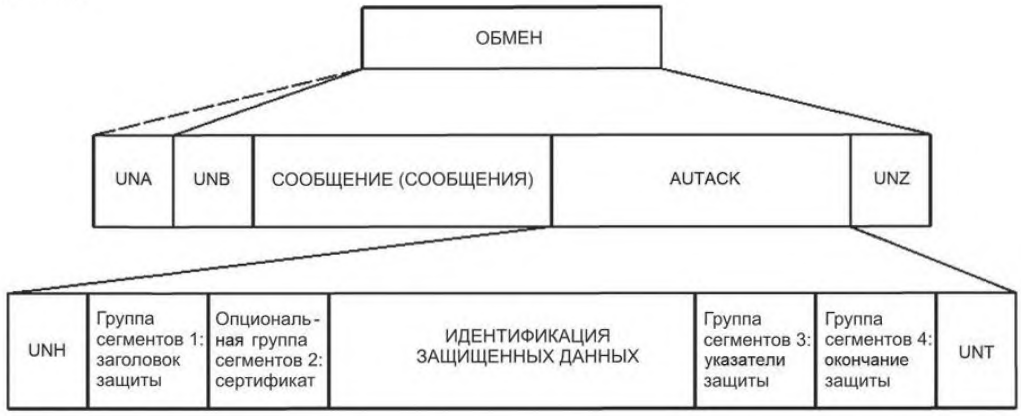


Рисунок 1 – Схема обмена, использующего защиту с помощью сообщения AUTACK на уровне сообщений

5.3.2 Использование AUTACK для аутентификации

5.3.2.1 Общие положения

Сообщение AUTACK, используемое в качестве сообщения для аутентификации, должно посылаться отправителем одной или нескольких различных структур EDIFACT либо стороной, уполномоченной этим отправителем. Цель использования данного сообщения – поддержка служб защиты, определенных в ИСО 9735-5, т.е. обеспечение аутентичности, целостности и неотказуемости источника соответствующих структур EDIFACT.

Сообщение для аутентификации AUTACK может быть реализовано двумя способами. В первом случае передаются хешированные значения тех структур EDIFACT, которые указаны в AUTACK и защищены самим этим сообщением, а во втором – только цифровые подписи структур EDIFACT, указанных в AUTACK.

5.3.2.2 Аутентификация с помощью хешированных значений структур EDIFACT

Защищаемая структура EDIFACT должна быть указана в одном из сегментов USX ("указатели защиты"). Для каждого сегмента USX должен быть как минимум один соответствующий сегмент USY ("защита по указателям") с результатом выполнения функции защиты, например, с хешированным значением указанной структуры EDIFACT.

Подробные сведения о выполняемой функции защиты должны входить в группу заголовка защиты AUTACK. Сегменты USY и USH для указанной в сообщении структуры EDIFACT должны быть связаны посредством имеющихся в них элементов данных контрольных номеров защиты.

Вся информация, передаваемая в сообщении AUTACK, должна быть защищена по крайней мере одной парой групп заголовка и окончания защиты.

Примечание – Сегмент USX используется в AUTACK для указания на одно или несколько сообщений, пакетов или групп в одном или нескольких обменах либо для указания на весь обмен. Для каждого сегмента USX в соответствующий сегмент USY входит результат применения к указанной структуре EDIFACT методов хеширования, аутентификации или обеспечения неотказуемости.

5.3.2.3 Аутентификация с помощью цифровых подписей структур EDIFACT

Защищаемая структура EDIFACT должна быть указана в одном из сегментов USX ("указатели защиты"). Для каждого сегмента USX должен быть как минимум один соответствующий сегмент USY ("защита по указателям") с цифровой подписью указанной структуры EDIFACT. Подробные сведения о выполняемой функции защиты должны входить в группу заголовка защиты AUTACK. Так как одна структура EDIFACT может быть защищена несколько раз, соответствующие сегменты USY и группы заголовка защиты должны быть связаны посредством имеющихся в них элементов данных контрольных номеров защиты.

Если в сообщении AUTACK содержится цифровая подпись указанной структуры EDIFACT (а не просто хешированное значение), то для самого сообщения AUTACK защита не требуется.

5.3.3 Использование AUTACK для квитирования

Сообщение AUTACK, используемое в качестве сообщения для квитирования, должно посылаться получателем одной или нескольких ранее принятых защищенных структур EDIFACT либо стороной, уполномоченной этим получателем. Целью является поддержка подтверждения приема, проверки целостности содержимого, обеспечения полноты принятой информации и/или неотказуемости приема соответствующих структур EDIFACT.

Функция квитирования должна использоваться только для защищенных структур EDIFACT. Защищенная структура EDIFACT должна быть указана в одном из сегментов USX ("указатели защиты"). Для каждого сегмента USX должен быть как минимум один соответствующий сегмент USY ("защита по указателям") с хешированным значением или цифровой подписью указанной структуры EDIFACT. Сегмент USY должен быть связан с группой заголовка защиты указанной структуры EDIFACT или с группой заголовка защиты сообщения AUTACK, которое обеспечивает защиту этой структуры, посредством элемента данных контрольного номера защиты. В заголовке защиты указанной структуры EDIFACT содержатся подробные сведения о функции защиты, выполненной отправителем исходного сообщения для указанной структуры EDIFACT.

В конце создания сообщения AUTACK для квитирования вся передаваемая в нем информация должна быть защищена по крайней мере одной парой групп заголовка и окончания защиты.

Сообщение AUTACK может также использоваться для отказа от квитирования в случае выявления проблем при проверке результатов защиты.

Примечание – Защищенное квитирование имеет смысл только для защищенных структур EDIFACT. Защита структур EDIFACT осуществляется с использованием либо интегрированных сегментов защиты (см. ИСО 9735-5), либо механизмов аутентификации AUTACK.

В сообщении AUTACK, используемом для квитирования, во избежание зацикливания, не должно быть требования возврата его получателем другого сообщения AUTACK для квитирования.

5.4 Определение сообщения

5.4.1 Пояснение формата сегмента данных

0010 **UNH, заголовок сообщения**

Служебный сегмент в начале сообщения, однозначно идентифицирующий это сообщение.

Код типа сообщения для защищенной аутентификациии защищенного квитирования – AUTACK.

Для указания назначения сообщения AUTACK, т.е. аутентификации, квитирования или отказа от квитирования, используется элемент данных с идентификатором функционального подтипа данного сообщения.

Сообщения для защищенной аутентификации и защищенного квитирования, соответствующие данному стандарту, должны содержать следующие данные в составном элементе данных S009 сегмента UNH:

Элемент данных	0065	AUTACK
	0052	4
	0054	1
	0051	UN

0020 **Группа сегментов 1: USH-USA-SG2 (группа заголовка защиты)**

Эта группа сегментов определяет используемые службу и механизмы защиты и содержит данные, необходимые для проверочных расчетов (по ИСО 9735-5).

В данной группе сегментов определяется служба защиты и алгоритм (алгоритмы), применяемые для сообщения AUTACK или для указанной в нем структуры EDIFACT.

Каждая группа заголовка защиты должна быть привязана к группе окончания защиты, а в некоторых случаях может быть привязана дополнительно и к сегментам USY.

0030 **USH, заголовок защиты**

Данный сегмент определяет службу защиты, используемую для сообщения/пакета, в которые он входит, либо для указанной структуры EDIFACT (согласно ИСО 9735-5).

Элемент данных службы защиты должен определять функцию защиты для сообщения AUTACK или для указанной структуры EDIFACT:

– службы защиты, обеспечивающие аутентификацию источника и неотказуемость источника сообщения, могут использоваться только для самого сообщения AUTACK;

– службы защиты, обеспечивающие целостность структуры EDIFACT, указанной в сообщении AUTACK, аутентификацию источника и неотказуемость источника этой структуры, должны использоваться только отправителем для защиты структур EDIFACT, указанных в сообщении AUTACK;

– службы защиты, обеспечивающие аутентификацию получателя и неотказуемость приема, должны использоваться только получателем защищенных структур EDIFACT для защищенного квитирования.

Должна быть задана область применения службы защиты согласно ИСО 9735-5. В сообщении AUTACK возможны четыре области применения службы защиты:

– первые две определены в разделе 5 ИСО 9735-5:2002;

– третья включает всю структуру EDIFACT между первым символом сообщения, пакета, группы или обмена (буквой “U”) и последним символом соответствующей структуры, включительно;

– четвертая область определяется пользователем в соответствии с соглашением между отправителем и получателем.

0040 **USA, Алгоритм защиты**

Данный сегмент определяет алгоритм защиты и технические аспекты использования этого алгоритма и содержит необходимые технические параметры (согласно ИСО 9735-5).

0050 **Группа сегментов 2: USC-USA-USR (группа сертификата)**

Данная группа сегментов содержит все данные, необходимые для проверки результатов применения методов защиты к сообщению/пакету, если используются асимметричные алгоритмы (согласно ИСО 9735-5).

0060 **USC, сертификат**

В этот сегмент входят регистрационные данные (удостоверение) владельца сертификата и данные об органе сертификации, которым был выдан сертификат (согласно ИСО 9735-5).

0070 **USA, алгоритм защиты**

Данный сегмент определяет алгоритм защиты и технические аспекты использования этого алгоритма и содержит необходимые технические параметры (согласно ИСО 9735-5).

0080 **USR, результат защиты**

В этом сегменте содержится результат выполнения функций защиты, примененных органом сертификации к сертификату (согласно ИСО 9735-5).

0090 **USB, идентификация защищенных данных**

Этот сегмент содержит идентификационные данные отправителя и получателя обмена, отметку времени для защиты AUTACK и обязательное указание на то, требуется ли защищенное квитирование от получателя сообщения AUTACK. Если оно требуется, то отправитель будет ожидать ответное сообщение квитирования AUTACK от получателя.

Данные об отправителе и получателе обмена, указываемые в USB, должны относиться к отправителю и получателю в том сеансе обмена, в котором используется AUTACK, с целью защиты данной информации.

0100 **Группа сегментов 3: USX-USY**

Данная группа сегментов используется для идентификации стороны обмена в процедуре защиты и для предоставления информации о защите указанной структуры EDIFACT.

0110 **USX, указатели защиты**

В данном сегменте содержатся указатели на сторону, вовлеченную в процедуру защиты.

Составной элемент данных даты и времени защиты может содержать данные о дате и времени формирования указанной структуры EDIFACT.

Если присутствует элемент 0020, но не присутствует ни один из элементов 0048, 0062 и 0800, то указатель относится ко всей структуре обмена.

Если присутствуют элементы 0020 и 0048, но не присутствуют элементы 0062 и 0800, то указатель относится к группе.

0120 **USY, защита по указателям**

Данный сегмент содержит элемент связи с группой заголовка защиты и результат применения служб защиты для указанной структуры EDIFACT, как предусмотрено в этой связанной группе заголовка защиты.

Если несколько структур EDIFACT защищены одной и той же службой защиты с одинаковыми параметрами защиты, то соответствующие им сегменты USY можно связать с одной группой заголовка защиты. В этом случае значение элемента связи между группой заголовка защиты и разными сегментами USY будет одним и тем же.

Если AUTACK используется для квитирования, то соответствующая группа заголовка защиты должна быть группой заголовка либо указанной структуры EDIFACT, либо сообщения AUTACK, которое служит для защиты последней, используя аутентификацию.

Значение элемента данных 0534 в сегменте USY должно совпадать со значением того же элемента в соответствующем сегменте USH, принадлежащего:

– текущему сообщению AUTACK, если оно служит для аутентификации (с помощью служб защиты, обеспечивающих аутентификацию источника указанной структуры EDIFACT, целостность

данной структуры или неотказуемость источника указанной структуры EDIFACT), либо

– самой указанной структуре EDIFACT или сообщению AUTACK с функцией аутентификации этой структуры, если используется функция квитирования (с помощью служб защиты, обеспечивающих неотказуемость приема или аутентификацию получателя).

0130 **Группа сегментов 4: UST-USR (группа окончания защиты)**

Данная группа сегментов содержит связь с группой сегментов заголовка защиты и результат выполнения функций защиты для сообщения/пакета (согласно ИСО 9735-5).

Сегмент USR может быть исключен, если группа окончания защиты связана с группой заголовка защиты, относящегося к указанной структуре EDIFACT. В этом случае соответствующие результаты выполнения функций защиты должны быть в сегментах USY, которые связаны с необходимой группой заголовка защиты.

0140 **UST, окончание защиты**

Данный сегмент устанавливает связь между группами сегментов заголовка защиты и окончания защиты. В нем приводится количество сегментов защиты, содержащихся в этих группах (согласно ИСО 9735-5).

0150 **USR, результат защиты**

В этом сегменте приводится результат выполнения функций защиты, указанных в связанной группе заголовка защиты, для сообщения/пакета (согласно ИСО 9735-5). Результат защиты в этом сегменте должен применяться к самому сообщению AUTACK.

0160 **UNT, окончание сообщения**

Это служебный сегмент, завершающий сообщение и содержащий полное число сегментов и контрольный справочный номер сообщения.

5.4.2 Структура сообщения

Таблица 1 – Таблица сегментов

POS	TAG	Name	S	R	Notes
0010	UNH	Заголовок сообщения	M	1	
0020	-----	Группа сегментов 1 ----------	M	99	-------+
0030	USH	Заголовок защиты	M	1	|
0040	USA	Алгоритм защиты	C	3	|
					|
0050	-----	Группа сегментов 2 ----------	C	2	----+ |
0060	USC	Сертификат	M	1	| |
0070	USA	Алгоритм защиты	C	3	| |
0080	USR	Результат защиты C	1		----+--+
0090	USB	Идентификация защищенных данных	M	1	
0100	-----	Группа сегментов 3 ----------	M	9999	----+
0110	USX	Указатели защиты	M	1	|
0120	USY	Защита по указателям	M	9	----+
0130	-----	Группа сегментов 4 ----------	M	99	----+
0140	UST	Окончание защиты	M	1	|
0150	USR	Результат защиты C	1		----+
0160	UNT	Окончание сообщения	M	1	

Обозначение

POS – порядковый номер позиции сегмента или группы сегментов в сообщении (с шагом 10 для возможности корректировок структуры сообщения в будущем);

TAG – тег сегмента;

Name – наименование;

S – статус сегмента (или группы сегментов), M - обязательный, C – условный;

R – максимальное число вхождений сегмента или группы сегментов;

Notes– примечания

Примечание – В тело сообщения AUTACK входит сегмент USB и группа сегментов 3.

Приложение А
(справочное)

Примеры сообщений AUTACK

А.1 Введение

В настоящем приложении приведены три примера, иллюстрирующие различные способы применения сообщения AUTACK.

В первом примере показано, как сообщение AUTACK используется для защиты ранее посланного сообщения с целью обеспечения неотказуемости источника. При этом требуется сообщение AUTACK для квитирования.

Во втором примере описано, как сообщение AUTACK может защитить два сообщения разными службами защиты: неотказуемость источника первого сообщения и аутентификацию источника второго сообщения.

В третьем примере иллюстрируется использование сообщения AUTACK для защищенного квитирования: приведено сообщение AUTACK для квитирования, запрошенного сообщением AUTACK в первом примере.

А.2 Пример 1. Служба неотказуемости источника, предоставляемая сообщением AUTACK

А.2.1 Описание ситуации

Банку А необходима служба защиты «неотказуемость источника» для платежных поручений Компании А, организуемая г-ном Смитом при превышении определенной суммы платежа.

В соглашении об обмене между сторонами установлено, что требуемая Банком А служба неотказуемости источника должна выполняться для этих платежных поручений г-ном Смитом из Компании А с использованием одной цифровой подписи.

По согласию обеих сторон для формирования этой цифровой подписи используется алгоритм RSA с 512-битовым ключом (асимметричный алгоритм), который применяется к значению хеш-функции, полученному с помощью алгоритма MD5.

Сертификат, удостоверяющий открытый ключ г-на Смита, выдан органом, которому доверяют обе стороны, – эмитентом сертификата.

Так как цифровая подпись платежного поручения PAYORD включается в сообщение AUTACK, то само сообщение AUTACK нет необходимости подписывать.

Сообщение PAYORD, защищенное сообщением AUTACK, было третьим сообщением в первом обмене, переданном г-ном Смитом Банку А. Оно было создано в 10:00:00, дата его создания – 1996.01.15.

Само сообщение AUTACK было пятым сообщением в обмене и было создано в 10:05:32, дата его создания – 1996.01.15.

Рассматриваются следующие сегменты защиты:

- USH для указания службы защиты, применяемой для сообщения PAYORD;
- USC-USA-USA-USA-USR – сертификат г-на Смита;
- USB;
- USX-USY с указателями защиты и результатами защиты (для сообщения PAYORD);
- UST без USR, со ссылкой на USH.

А.2.2 Элементы защиты

ЗАГОЛОВОК ЗАЩИТЫ	
СЛУЖБА ЗАЩИТЫ, КОДИРОВАННАЯ	Неотказуемость источника
КОНТРОЛЬНЫЙ НОМЕР ЗАЩИТЫ	Контрольный номер данного заголовка защиты:1
ТИП ОТВЕТА	Требуется квитирование: 1
ФУНКЦИЯ ФИЛЬТРАЦИИ	Все двоичные значения (подписи) фильтруются с использованием шестнадцатеричного фильтра
КОДИРОВАНИЕ ИСХОДНОГО НАБОРА ЗНАКОВ	Сообщение было закодировано с помощью набора 8-битовых знаков ASCII при генерации его подписи

СЕРТИФИКАТ	Сертификат г-на Смита
УЧЕТНЫЙ НОМЕР СЕРТИФИКАТА	Номер сертификата, назначенный органом AUTHORITY: 00000001.
ИДЕНТИФИКАЦИОННЫЕ ЭЛЕМЕНТЫ ЗАЩИТЫ Квалификатор стороны обеспечения защиты	Владелец сертификата (г-н Смит из Компании А)
ИДЕНТИФИКАЦИОННЫЕ ЭЛЕМЕНТЫ ЗАЩИТЫ Квалификатор стороны защиты Имя ключа	Эмитент сертификата (наименование органа, который генерировал сертификат г-на Смита: AUTHORITY) Открытый ключ AUTHORITY, который использовался для генерации сертификата г-на Смита: PK1
ВЕРСИЯ СИНТАКСИСА СЕРТИФИКАТА	Версия сертификата по справочнику служебных сегментов UN/EDIFACT
ФУНКЦИЯ ФИЛЬТРАЦИИ	Все двоичные значения (ключи и цифровые подписи) фильтруются с помощью шестнадцатеричного фильтра
КОДИРОВАНИЕ ИСХОДНОГО НАБОРА ЗНАКОВ	Удостоверение сертификата было закодировано с помощью набора 8-битовых знаков ASCII при генерации сертификата
СЛУЖЕБНЫЙ ЗНАК ДЛЯ ПОДПИСИ Квалификатор служебного знака для подписи Служебный знак для подписи	Служебный знак, использовавшийся при создании подписи Служебный знак – терминатор сегмента Значение “ ' ” (апостроф)
СЛУЖЕБНЫЙ ЗНАК ДЛЯ ПОДПИСИ Квалификатор служебного знака для подписи Служебный знак для подписи	Служебный знак, использовавшийся при создании подписи Служебный знак – разделитель элементов данных Значение “ + ” (знак "плюс")
СЛУЖЕБНЫЙ ЗНАК ДЛЯ ПОДПИСИ Квалификатор служебного знака для подписи	Служебный знак, использовавшийся при создании подписи Служебный знак – разделитель компонентных элементов данных

Служебный знак для подписи	Значение “ : ” (двоеточие)
СЛУЖЕБНЫЙ ЗНАК ДЛЯ ПОДПИСИ Квалификатор служебного знака для подписи Служебный знак для подписи	Служебный знак, использовавшийся при создании подписи Служебный знак – разделитель повторов Значение “ * ” (звездочка)
СЛУЖЕБНЫЙ ЗНАК ДЛЯ ПОДПИСИ Квалификатор служебного знака для подписи Служебный знак для подписи	Служебный знак, использовавшийся при создании подписи Служебный знак – знак освобождения Значение “ ? ” (вопросительный знак)
ДАТА И ВРЕМЯ ЗАЩИТЫ Дата и время	Время генерации сертификата Сертификат г-на Смита был сгенерирован 931215[1)] в 14:12:00
ДАТА И ВРЕМЯ ЗАЩИТЫ Дата и время	Начало срока действия сертификата Срок действия сертификата г-на Смита начинается с: 1996 01 01 000000[2)]
ДАТА И ВРЕМЯ ЗАЩИТЫ Дата и время	Окончание срока действия сертификата Срок действия сертификата г-на Смита заканчивается: 1996 12 31 235959[3)].

[1)] Представление даты соответствует оригиналу.
[2)] Представление даты и времени соответствует оригиналу.
[3)] Представление даты и времени соответствует оригиналу.

АЛГОРИТМ ЗАЩИТЫ	Асимметричный алгоритм, использовавшийся г-ном Смитом для подписи
АЛГОРИТМ ЗАЩИТЫ Область применения алгоритма Криптографический режим Алгоритм	 Используется алгоритм подписи владельца Ни один режим в данном случае не применим RSA, асимметричный алгоритм
ПАРАМЕТР АЛГОРИТМА Квалификатор параметра алгоритма Значение параметра алгоритма	 Определяет этот параметр в качестве открытой экспоненты для подтверждения подлинности подписи Открытый ключ г-на Смита
ПАРАМЕТР АЛГОРИТМА Квалификатор параметра алгоритма Значение параметра алгоритма	 Определяет этот параметр в качестве модуля для подтверждения подлинности подписи Модуль г-на Смита
ПАРАМЕТР АЛГОРИТМА Квалификатор параметра алгоритма Значение параметра алгоритма	 Определяет этот параметр в качестве длины модуля г-на Смита (в битах) Длина модуля г-на Смита 512 бит
АЛГОРИТМ ЗАЩИТЫ	Хеш-функция, используемая AUTHORITY для генерации сертификата г-на Смита
АЛГОРИТМ ЗАЩИТЫ Область применения алгоритма Криптографический режим Алгоритм	 Используется алгоритм хеширования издателя Хеш-функция, применяемая в ИСО 10118-2. Для получения хеш-кода двойной длины (128 бит) применялась хеш-функция с использованием алгоритма шифрования n-битовых блоков; значения инициализации: A = 01234567 B = 89ABCDEF C = FEDCBA98 D = 76543210 Выбран алгоритм MD5 для сокращения сообщений
АЛГОРИТМ ЗАЩИТЫ	Асимметричный алгоритм, использовавшийся AUTHORITY для подписи
АЛГОРИТМ ЗАЩИТЫ Область применения алгоритма Криптографический режим	 Используется алгоритм подписи издателя Ни один режим в данном случае не применим

Алгоритм	RSA, асимметричный алгоритм
ПАРАМЕТР АЛГОРИТМА Квалификатор параметра алгоритма Значение параметра алгоритма	 Определяет этот параметр в качестве открытой экспоненты для подтверждения подлинности подписи Открытый ключ AUTHORITY
ПАРАМЕТР АЛГОРИТМА Квалификатор параметра алгоритма Значение параметра алгоритма	 Определяет этот параметр в качестве модуля для подтверждения подлинности подписи Модуль AUTHORITY
ПАРАМЕТР АЛГОРИТМА Квалификатор параметра алгоритма Значение параметра алгоритма	 Определяет этот параметр в качестве длины модуля AUTHORITY (в битах) Длина модуля AUTHORITY 512 бит
РЕЗУЛЬТАТ ЗАЩИТЫ	Цифровая подпись сертификата

РЕЗУЛЬТАТ ПРОВЕРКИ Квалификатор контрольного значения Контрольное значение	Уникальное контрольное значение 1 512-битовая цифровая подпись с шестнадцатеричной фильтрацией
ИДЕНТИФИКАЦИЯ ЗАЩИЩЕННЫХ ДАННЫХ	
ТИП ОТВЕТА, КОДИРОВАННЫЙ	Требуется защищенное квитирование от Банка А
ДАТА И ВРЕМЯ ЗАЩИТЫ Дата и время Дата события Время события	Отметка времени AUTACK, связанная с защитой Отметка времени, дата: 1996 01 15[1)]. Отметка времени, время: 10:05:32.
ОТПРАВИТЕЛЬ ОБМЕНА Идентификатор отправителя обмена	Идентификатор отправителя обмена Идентификатор г-на Смита из Компании А
ПОЛУЧАТЕЛЬ ОБМЕНА Идентификатор получателя обмена	Идентификатор получателя обмена Идентификатор Банка А
УКАЗАТЕЛИ ЗАЩИТЫ	Указывают на объект защиты (платежное поручение PAYORD, связанное со службой неотказуемости источника) и на соответствующие дату и время
КОНТРОЛЬНЫЙ НОМЕР ОБМЕНА	Определяет контрольный номер, присвоенный отправителем обмену, включающему сообщение PAYORD: 1
ОТПРАВИТЕЛЬ ОБМЕНА Идентификатор отправителя обмена	Определяет отправителя обмена, включающего сообщение PAYORD: г-н Смит из Компании А
ПОЛУЧАТЕЛЬ ОБМЕНА Идентификатор получателя обмена	Определяет получателя обмена, включающего сообщение PAYORD: Банк А
КОНТРОЛЬНЫЙ НОМЕР СООБЩЕНИЯ	Определяет контрольный номер, присвоенный отправителем сообщению PAYORD: 3
ДАТА И ВРЕМЯ ЗАЩИТЫ Дата и время Дата события Время события	Связанная с защитой отметка времени, относящаяся к PAYORD Отметка времени, дата: 1996 01 15[1)] Отметка времени, время: 10:00:00

[1)] Представление даты соответствует оригиналу.

[1)] Представление даты соответствует оригиналу.

ЗАЩИТА ПО УКАЗАТЕЛЯМ	Определяет соответствующий заголовок (связанный с выполнением функций защиты для сообщения PAYORD) и результат выполнения функций защиты для сообщения PAYORD
КОНТРОЛЬНЫЙ НОМЕР ЗАЩИТЫ	Номер, связывающий результат проверки с соответствующим сегментом USH. В данном случае его значение:1
РЕЗУЛЬТАТ ПРОВЕРКИ Квалификатор контрольного значения Контрольное значение	 Уникальное контрольное значение: 1 512-битовая цифровая подпись (сообщения PAYORD) с шестнадцатеричной фильтрацией
ОКОНЧАНИЕ ЗАЩИТЫ	
КОНТРОЛЬНЫЙ НОМЕР ЗАЩИТЫ	Номер данного окончания защиты: 1
ЧИСЛО СЕГМЕНТОВ ЗАЩИТЫ	Число сегментов защиты: 7

А.3 Пример 2. Защита нескольких сообщений с помощью AUTACK

А.3.1 Описание ситуации

Банку А необходима служба защиты «неотказуемость источника» для платежных поручений Компании А, организуемая г-ном Смитом при превышении определенной суммы платежа. Если эта сумма не превышена, то запрашивается служба аутентификации источника сообщения.

В соглашении об обмене между сторонами установлено, что требуемая Банком А служба неотказуемости источника должна выполняться для этих платежных поручений г-ном Смитом из Компании А с использованием одной цифровой подписи. По согласию обеих сторон для формирования этой цифровой подписи используется алгоритм RSA с 512-битовым ключом (асимметричный алгоритм), который применяется к значению хеш-функции, полученному с помощью алгоритма MD5.

Кроме того, аутентификация источника сообщения достигается путем генерации «кода аутентификации сообщения» (MAC) на стороне отправителя с использованием симметричного алгоритма DES в соответствии с ИСО 8731-1.

Сертификат, удостоверяющий открытый ключ г-на Смита, выдан органом, которому доверяют обе стороны, – эмитентом сертификата.

Первое сообщение платежного поручения PAYORD защищено цифровой подписью в сообщении AUTACK. Это пятое сообщение первого обмена, переданного г-ном Смитом в Банк А. Оно было послано в 08:00:00, дата отсылки – 1996.01.15.

Второе сообщение PAYORD защищено кодом MAC в AUTACK. Это седьмое сообщение первого обмена. Оно было послано в тот же день в 09:00:00.

Само сообщение AUTACK, десятое в первом обмене, было послано в тот же день в 10:05:32.

Так как первое сообщение PAYORD защищено цифровой подписью, то подпись самого сообщения AUTACK не требуется.

Таким образом, имеются следующие сегменты защиты:

- USH для указания службы неотказуемости источника применительно к первому сообщению PAYORD;
- USC-USA-USA-USA-USR – сертификат г-наСмита;
- USH для указания службы аутентификации источника сообщения применительно ко второму сообщению PAYORD;
- USB;
- USX-USY с указателями защиты и результатом защиты (цифровой подписью) для первого сообщения PAYORD;
- USX-USY с указателями защиты и результатом защиты (MAC) для второго сообщения PAYORD;
- UST без USR, со ссылкой на первый сегмент USH;
- UST без USR, со ссылкой на второй сегмент USH.

А.3.2 Элементы защиты

ЗАГОЛОВОК ЗАЩИТЫ	Заголовок с данными о функции защиты, выполненной для указанного объекта (первого сообщения PAYORD)
СЛУЖБА ЗАЩИТЫ, КОДИРОВАННАЯ	Неотказуемость источника первого сообщения PAYORD
КОНТРОЛЬНЫЙ НОМЕР ЗАЩИТЫ	Контрольный номер данного заголовка защиты:1
ФУНКЦИЯ ФИЛЬТРАЦИИ	Все двоичные значения фильтруются с использованием шестнадцатеричного фильтра
КОДИРОВАНИЕ ИСХОДНОГО НАБОРА ЗНАКОВ	Сообщение было закодировано с помощью набора 8-битовых знаков ASCII при генерации его подписи
ИДЕНТИФИКАЦИОННЫЕ ЭЛЕМЕНТЫ ЗАЩИТЫ Квалификатор стороны обеспечения защиты	Отправитель сообщения (г-н Смит из Компании А)
ИДЕНТИФИКАЦИОННЫЕ ЭЛЕМЕНТЫ ЗАЩИТЫ Квалификатор стороны обеспечения защиты	Получатель сообщения (Банк А)
СЕРТИФИКАТ	Сертификат г-на Смита
НОМЕР СЕРТИФИКАТА	Номер сертификата, назначенный AUTHORITY: 00000001
ИДЕНТИФИКАЦИОННЫЕ ЭЛЕМЕНТЫ ЗАЩИТЫ Квалификатор стороны обеспечения защиты	Владелец сертификата (г-н Смит из Компании А)
ИДЕНТИФИКАЦИОННЫЕ ЭЛЕМЕНТЫ ЗАЩИТЫ Квалификатор стороны обеспечения защиты Имя ключа	Эмитент сертификата (наименование органа, который генерировал сертификат г-на Смита: AUTHORITY) Открытый ключ AUTHORITY, который использовался для генерации сертификата г-на Смита: PK1
ВЕРСИЯ СИНТАКСИСА СЕРТИФИКАТА	Версия сертификата по справочнику служебных сегментов UN/EDIFACT
ФУНКЦИЯ ФИЛЬТРАЦИИ	Все двоичные значения (ключи и цифровые подписи) фильтруются с помощью шестнадцатеричного фильтра
СЛУЖЕБНЫЙ ЗНАК ДЛЯ ПОДПИСИ	Служебный знак, использовавшийся при создании подписи

Квалификатор служебного знака для подписи Служебный знак для подписи	Служебный знак – терминатор сегмента Значение “ ' ” (апостроф)
СЛУЖЕБНЫЙ ЗНАК ДЛЯ ПОДПИСИ Квалификатор служебного знака для подписи Служебный знак для подписи	Служебный знак, использовавшийся при создании подписи Служебный знак – разделитель элементов данных. Значение “ + ” (знак "плюс")
СЛУЖЕБНЫЙ ЗНАК ДЛЯ ПОДПИСИ Квалификатор служебного знака для подписи Служебный знак для подписи	Служебный знак, использовавшийся при создании подписи. Служебный знак – разделитель компонентных элементов данных Значение “ : ” (двоеточие)
СЛУЖЕБНЫЙ ЗНАК ДЛЯ ПОДПИСИ Квалификатор служебного знака для подписи Служебный знак для подписи	Служебный знак, использовавшийся при создании подписи Служебный знак – разделитель повторов Значение “ * ” (звездочка)
СЛУЖЕБНЫЙ ЗНАК ДЛЯ ПОДПИСИ Квалификатор служебного знака для подписи Служебный знак для подписи	Служебный знак, использовавшийся при создании подписи Служебный знак – знак освобождения Значение “ ? ” (вопросительный знак)
ДАТА И ВРЕМЯ ЗАЩИТЫ Дата и время	Время генерации сертификата Сертификат г-на Смита был сгенерирован: 931215[1)] в 14:12:00
ДАТА И ВРЕМЯ ЗАЩИТЫ Дата и время	Начало срока действия сертификата Срок действия сертификата г-на Смита начинается с: 1996 01 01 000000[2)]
ДАТА И ВРЕМЯ ЗАЩИТЫ Дата и время	Окончание срока действия сертификата Срок действия сертификата г-на Смита заканчивается: 1996 12 31 235959[3)]
АЛГОРИТМ ЗАЩИТЫ	Асимметричный алгоритм, использовавшийся г-ном Смитом для подписи

[1)] Представление даты соответствует оригиналу.
[2)] Представление даты и времени соответствует оригиналу.
[3)] Представление даты и времени соответствует оригиналу.

АЛГОРИТМ ЗАЩИТЫ Область применения алгоритма Криптографический режим Алгоритм	 Используется алгоритм подписи владельца Ни один режим в данном случае не применим RSA, асимметричный алгоритм
ПАРАМЕТР АЛГОРИТМА Квалификатор параметра алгоритма Значение параметра алгоритма	 Определяет этот параметр в качестве открытой экспоненты для подтверждения подлинности подписи Открытый ключ г-на Смита
ПАРАМЕТР АЛГОРИТМА Квалификатор параметра алгоритма Значение параметра алгоритма	 Определяет этот параметр в качестве модуля для подтверждения подлинности подписи Модуль г-на Смита
ПАРАМЕТР АЛГОРИТМА Квалификатор параметра алгоритма Значение параметра алгоритма	 Определяет этот параметр в качестве длины модуля г-на Смита (в битах) Длина модуля г-на Смита 512 бит
АЛГОРИТМ ЗАЩИТЫ	Хеш-функция, используемая AUTHORITY для генерации сертификата г-на Смита
АЛГОРИТМ ЗАЩИТЫ Область применения алгоритма Криптографический режим Алгоритм	 Используется алгоритм хеширования эмитента Хеш-функция CD, применяемая в ИСО 10118-2 Для получения хеш-кода двойной длины (128 бит) применялась хеш-функция с использованием алгоритма шифрования n-битовых блоков; значения инициализации: A = 01234567 B = 89ABCDEF C = FEDCBA98 D = 76543210 Выбран алгоритм MD5 для сокращения сообщений
АЛГОРИТМ ЗАЩИТЫ	Асимметричный алгоритм, использовавшийся AUTHORITY для подписи
АЛГОРИТМ ЗАЩИТЫ Область применения алгоритма Криптографический режим Алгоритм	 Используется алгоритм подписи эмитента Ни один режим в данном случае не применим RSA, асимметричный алгоритм
ПАРАМЕТР АЛГОРИТМА Квалификатор параметра алгоритма	 Определяет этот параметр в качестве открытой экспоненты для подтверждения подлинности подписи

Значение параметра алгоритма	Открытый ключ AUTHORITY
ПАРАМЕТР АЛГОРИТМА Квалификатор параметра алгоритма Значение параметра алгоритма	Определяет этот параметр в качестве модуля для подтверждения подлинности подписи Модуль AUTHORITY
ПАРАМЕТР АЛГОРИТМА Квалификатор параметра алгоритма Значение параметра алгоритма	Определяет этот параметр в качестве длины модуля AUTHORITY (в битах) Длина модуля AUTHORITY 512 бит

РЕЗУЛЬТАТ ЗАЩИТЫ	Цифровая подпись сертификата
РЕЗУЛЬТАТ ПРОВЕРКИ Квалификатор контрольного значения Контрольное значение	 Уникальное контрольное значение: 1 512-битовая цифровая подпись с шестнадцатеричной фильтрацией
ЗАГОЛОВОК ЗАЩИТЫ	Заголовок с данными о функции защиты, выполненной для указанного объекта (второго сообщения PAYORD)
СЛУЖБА ЗАЩИТЫ, КОДИРОВАННАЯ	Аутентификация источника второго сообщения PAYORD
КОНТРОЛЬНЫЙ НОМЕР ЗАЩИТЫ	Контрольный номер данного заголовка: 2
ФУНКЦИЯ ФИЛЬТРАЦИИ	Все двоичные значения фильтруются с использованием шестнадцатеричного фильтра
ИДЕНТИФИКАЦИОННЫЕ ЭЛЕМЕНТЫ ЗАЩИТЫ Квалификатор стороны обеспечения защиты	 Отправитель сообщения (г-н Смит из Компании А)
ИДЕНТИФИКАЦИОННЫЕ ЭЛЕМЕНТЫ ЗАЩИТЫ Квалификатор стороны обеспечения защиты	 Получатель сообщения (Банк А)
АЛГОРИТМ ЗАЩИТЫ	
АЛГОРИТМ ЗАЩИТЫ Область применения алгоритма Криптографический режим Алгоритм	 Для аутентификации источника сообщения используется симметричный алгоритм Код MAC, вычисленный в соответствии с ИСО 8731-1 Использовался алгоритм DES
ПАРАМЕТР АЛГОРИТМА Квалификатор параметра алгоритма Значение параметра алгоритма	 Указываются такие параметры данного алгоритма, как имя симметричного ключа, обмен которым произошел ранее 1234567890ABCDEF
ИДЕНТИФИКАЦИЯ ЗАЩИЩЕННЫХ ДАННЫХ	
ТИП ОТВЕТА, КОДИРОВАННЫЙ	От Банка А квитирование не требуется

ДАТА И ВРЕМЯ ЗАЩИТЫ Дата и время Дата события Время события	Отметка времени AUTACK, связанная с защитой Отметка времени, дата: 1996 01 15[1)] Отметка времени, время: 10:05:32
ОТПРАВИТЕЛЬ ОБМЕНА Идентификатор отправителя обмена	Идентификатор отправителя обмена Идентификатор г-на Смита из Компании А
ПОЛУЧАТЕЛЬ ОБМЕНА Идентификатор получателя обмена	Идентификатор получателя обмена Идентификатор Банка А
УКАЗАТЕЛИ ЗАЩИТЫ	Указывают на объект защиты (второе сообщение PAYORD)
КОНТРОЛЬНЫЙ НОМЕР ОБМЕНА	Определяет контрольный номер, присвоенный отправителем обмену, включающему второе сообщение PAYORD: 1
ОТПРАВИТЕЛЬ ОБМЕНА Идентификатор отправителя обмена	Определяет отправителя обмена, включающего сообщение PAYORD: г-н Смит из Компании А
ПОЛУЧАТЕЛЬ ОБМЕНА Идентификатор получателя обмена	Определяет получателя обмена, включающего сообщение PAYORD: Банк А
КОНТРОЛЬНЫЙ НОМЕР СООБЩЕНИЯ	Определяет контрольный номер, присвоенный отправителем второму сообщению PAYORD: 7
ДАТА И ВРЕМЯ ЗАЩИТЫ Дата события Время события	Отметка времени защиты, дата: 1996 01 15[1)] Отметка времени защиты, время: 09:00:00
ЗАЩИТА ПО УКАЗАТЕЛЯМ	Определяет соответствующий заголовок (связанный с выполнением функций защиты для второго сообщения PAYORD) и результат выполнения функций защиты
КОНТРОЛЬНЫЙ НОМЕР ЗАЩИТЫ	Номер, связывающий результат проверки с соответствующим сегментом USH. В данном случае его значение: 2
РЕЗУЛЬТАТ ПРОВЕРКИ	

[1)] Представление даты соответствует оригиналу.

Квалификатор контрольного значения Контрольное значение	MAC (Код аутентификации сообщения) 12345678 – значение из 4 байт
УКАЗАТЕЛИ ЗАЩИТЫ	Указывают на объект защиты (первое сообщение PAYORD) и соответствующую дату и время
КОНТРОЛЬНЫЙ НОМЕР ОБМЕНА	Определяет контрольный номер, присвоенный отправителем обмену, включающему сообщение PAYORD: 1
ОТПРАВИТЕЛЬ ОБМЕНА Идентификатор отправителя обмена	Определяет отправителя обмена, включающего сообщение PAYORD: г-н Смит из Компании А
ПОЛУЧАТЕЛЬ ОБМЕНА Идентификатор получателя обмена	Определяет получателя обмена, включающего сообщение PAYORD: Банк А
КОНТРОЛЬНЫЙ НОМЕР СООБЩЕНИЯ	Определяет контрольный номер, присвоенный отправителем первому сообщению PAYORD: 5
ДАТА И ВРЕМЯ ЗАЩИТЫ Дата события Время события	Отметка времени защиты, дата: 1996 01 15[1)] Отметка времени защиты, время: 08:00:00
ЗАЩИТА ПО УКАЗАТЕЛЯМ	Определяет соответствующий заголовок (связанный с выполнением функций защиты для первого сообщения PAYORD) и результат выполнения функций защиты
КОНТРОЛЬНЫЙ НОМЕР ЗАЩИТЫ	Номер, связывающий результат проверки с соответствующим сегментом USH. В данном случае его значение:1
РЕЗУЛЬТАТ ПРОВЕРКИ Квалификатор контрольного значения Контрольное значение	Уникальное контрольное значение 1 512-битовая цифровая подпись (первого сообщения PAYORD) с шестнадцатеричной фильтрацией
ОКОНЧАНИЕ ЗАЩИТЫ	
КОНТРОЛЬНЫЙ НОМЕР ЗАЩИТЫ	Номер данного окончания защиты: 2
ЧИСЛО СЕГМЕНТОВ ЗАЩИТЫ	Число сегментов защиты 2
ОКОНЧАНИЕ ЗАЩИТЫ	

[1)] Представление даты соответствует оригиналу.

КОНТРОЛЬНЫЙ НОМЕР ЗАЩИТЫ	Номер данного окончания защиты: 1
ЧИСЛО СЕГМЕНТОВ ЗАЩИТЫ	Число сегментов защиты 7

А.4 Пример 3. Защищенное квитирование полученного сообщения с помощью AUTACK

А.4.1 Описание ситуации

В примере 1 сообщение AUTACK использовалось отправителем (г-ном Смитом из Компании А) предыдущего сообщения PAYORD. В AUTACK был запрос на квитирование от Банка А.

В данном примере показано, как сообщение AUTACK используется для защищенного квитирования.

Сторонами было принято, что сообщения AUTACK для защищенного квитирования будут защищаться цифровой подписью для обеспечения неотказуемости источника.

Сообщение AUTACK, созданное 1996.01.16 в 11:00:00, было двадцатым сообщениемв обмене.

Имеются следующие сегменты защиты:

- USH для указания службы защиты, используемой для сообщения AUTACK;
- USH для указания службы защиты, используемой для квитируемого объекта;
- USC-USA(3)-USR – сертификат Банка А;
- USB – для данных сообщения AUTACK;
- USX-USY – для указателей на квитируемый объект и цифровую подпись;
- UST – для окончания защиты, без сегмента USR;
- UST-USR – для защиты самого сообщения AUTACK.

А.4.2 Элементы защиты

ЗАГОЛОВОК ЗАЩИТЫ	
СЛУЖБА ЗАЩИТЫ, КОДИРОВАННАЯ	Неотказуемость источника
КОНТРОЛЬНЫЙ НОМЕР ЗАЩИТЫ	Номер данного заголовка защиты:1
ФУНКЦИЯ ФИЛЬТРАЦИИ	Все двоичные значения фильтруются с использованием шестнадцатеричного фильтра
КОДИРОВАНИЕ ИСХОДНОГО НАБОРА ЗНАКОВ	Сообщение было закодировано с помощью набора 8-битовых знаков ASCII во время генерации кода MAC
ИДЕНТИФИКАЦИОННЫЕ ЭЛЕМЕНТЫ ЗАЩИТЫ Квалификатор стороны обеспечения защиты	Отправитель сообщения (сторона, генерирующая цифровую подпись): Банк А
ИДЕНТИФИКАЦИОННЫЕ ЭЛЕМЕНТЫ ЗАЩИТЫ Квалификатор стороны обеспечения защиты	Получатель сообщения (сторона, проверяющая цифровую подпись): г-н Смит из Компании А
ПОРЯДКОВЫЙ НОМЕР ЗАЩИТЫ	Порядковый номер защиты данного сообщения: 20
ДАТА И ВРЕМЯ ЗАЩИТЫ Дата события Время события	 Отметка времени защиты, дата: 1996.01.16 Отметка времени защиты, время: 11:00:00
СЕРТИФИКАТ	Сертификат Банка А
НОМЕР СЕРТИФИКАТА	Номер сертификата, назначенный AUTHORITY: 00000010

ИДЕНТИФИКАЦИОННЫЕ ЭЛЕМЕНТЫ ЗАЩИТЫ Квалификатор стороны обеспечения защиты	Владелец сертификата (Банк А)
ИДЕНТИФИКАЦИОННЫЕ ЭЛЕМЕНТЫ ЗАЩИТЫ Квалификатор стороны обеспечения защиты Имя ключа	Эмитент сертификата (наименование органа, который генерировал сертификат Банка А: AUTHORITY) Открытый ключ AUTHORITY, который использовался для генерации сертификата Банка А: PK1
ВЕРСИЯ СИНТАКСИСА СЕРТИФИКАТА	Версия сертификата по справочнику служебных сегментов UN/EDIFACT
ФУНКЦИЯ ФИЛЬТРАЦИИ	Все двоичные значения (ключи и цифровые подписи) фильтруются с помощью шестнадцатеричного фильтра
КОДИРОВАНИЕ ИСХОДНОГО НАБОРА ЗНАКОВ	Удостоверение сертификата было закодировано с помощью набора 8-битовых знаков ASCII при генерации сертификата
СЛУЖЕБНЫЙ ЗНАК ДЛЯ ПОДПИСИ Квалификатор служебного знака для подписи Служебный знак для подписи	Служебный знак, использовавшийся при создании подписи Служебный знак – терминатор сегмента Значение “ ' ” (апостроф)
СЛУЖЕБНЫЙ ЗНАК ДЛЯ ПОДПИСИ Квалификатор служебного знака для подписи Служебный знак для подписи	Служебный знак, использовавшийся при создании подписи Служебный знак – разделитель элементов данных Значение “ + ” (знак "плюс")
СЛУЖЕБНЫЙ ЗНАК ДЛЯ ПОДПИСИ Квалификатор служебного знака для подписи Служебный знак для подписи	Служебный знак, использовавшийся при создании подписи Служебный знак – разделитель компонентных элементов данных Значение “ : ” (двоеточие)
СЛУЖЕБНЫЙ ЗНАК ДЛЯ ПОДПИСИ Квалификатор служебного знака для подписи	Служебный знак, использовавшийся при создании подписи Служебный знак – разделитель повторов

Служебный знак для подписи	Значение “ * ” (звездочка)
СЛУЖЕБНЫЙ ЗНАК ДЛЯ ПОДПИСИ Квалификатор служебного знака для подписи Служебный знак для подписи	Служебный знак, использовавшийся при создании подписи Служебный знак – знак освобождения Значение “ ? ” (вопросительный знак)
ДАТА И ВРЕМЯ ЗАЩИТЫ Дата и время	Время генерации сертификата Сертификат Банка А был сгенерирован 1995 12 31[1)] в 14:00:00
ДАТА И ВРЕМЯ ЗАЩИТЫ Дата и время	Начало срока действия сертификата Срок действия сертификата Банка А начинается с: 1996 01 01 000000[2)]
ДАТА И ВРЕМЯ ЗАЩИТЫ Дата и время	Окончание срока действия сертификата Срок действия сертификата Банка А заканчивается:1996 12 31 235959[2)]
АЛГОРИТМ ЗАЩИТЫ	Асимметричный алгоритм, используемый Банком А для подписи
АЛГОРИТМ ЗАЩИТЫ Область применения алгоритма Криптографический режим Алгоритм	 Используется алгоритм подписи владельца Ни один режим в данном случае не применим RSA, асимметричный алгоритм
ПАРАМЕТР АЛГОРИТМА Квалификатор параметра алгоритма Значение параметра алгоритма	 Определяет этот параметр в качестве открытой экспоненты для подтверждения подлинности подписи Открытый ключ Банка А

[1)] Представление даты соответствует оригиналу.
[2)] Представление даты и времени соответствует оригиналу.

ПАРАМЕТР АЛГОРИТМА Квалификатор параметра алгоритма Значение параметра алгоритма	 Определяет этот параметр в качестве модуля для подтверждения подлинности подписи Модуль Банка А
ПАРАМЕТР АЛГОРИТМА Квалификатор параметра алгоритма Значение параметра алгоритма	 Определяет этот параметр в качестве длины модуля Банка А (в битах) Длина модуля Банка А 512 бит
АЛГОРИТМ ЗАЩИТЫ	Хеш-функция, используемая AUTHORITY для генерации сертификата Банка А
АЛГОРИТМ ЗАЩИТЫ Область применения алгоритма Криптографический режим Алгоритм	 Используется алгоритм хеширования эмитента Хеш-функция, применяемая в ИСО 10118-2. Для получения хеш-кода двойной длины (128 бит) применялась хеш-функция с использованием алгоритма шифрования n-битовых блоков; значения инициализации: A = 01234567 B = 89ABCDEF C = FEDCBA98 D = 76543210 Выбран алгоритм MD5 для сокращения сообщений
АЛГОРИТМ ЗАЩИТЫ	Асимметричный алгоритм, используемый AUTHORITY для подписи
АЛГОРИТМ ЗАЩИТЫ Область применения алгоритма Криптографический режим Алгоритм	 Используется алгоритм подписи эмитента Ни один режим в данном случае не применим RSA, асимметричный алгоритм
ПАРАМЕТР АЛГОРИТМА Квалификатор параметра алгоритма Значение параметра алгоритма	 Определяет этот параметр в качестве открытой экспоненты для подтверждения подлинности подписи Открытый ключ AUTHORITY
ПАРАМЕТР АЛГОРИТМА Квалификатор параметра алгоритма Значение параметра алгоритма	 Определяет этот параметр в качестве модуля для подтверждения подлинности подписи Модуль AUTHORITY
ПАРАМЕТР АЛГОРИТМА Квалификатор параметра алгоритма	 Определяет этот параметр в качестве длины модуля AUTHORITY (в битах)

Значение параметра алгоритма	Длина модуля AUTHORITY 512 бит
РЕЗУЛЬТАТ ЗАЩИТЫ	Цифровая подпись сертификата
РЕЗУЛЬТАТ ПРОВЕРКИ Квалификатор контрольного значения Контрольное значение	Уникальное контрольное значение: 1 512-битовая цифровая подпись с шестнадцатеричной фильтрацией
ЗАГОЛОВОК ЗАЩИТЫ	Заголовок с данными о функции защиты, выполненной для указанного объекта квитирования (PAYORD)
СЛУЖБА ЗАЩИТЫ, КОДИРОВАННАЯ	Неотказуемость источника
КОНТРОЛЬНЫЙ НОМЕР ЗАЩИТЫ	Номер данного заголовка защиты:2
ФУНКЦИЯ ФИЛЬТРАЦИИ	Все двоичные значения (подписи) фильтруются с использованием шестнадцатеричного фильтра
КОДИРОВАНИЕ ИСХОДНОГО НАБОРА ЗНАКОВ	Сообщение было закодировано с помощью набора 8-битовых знаков ASCII при генерации его подписи

ИДЕНТИФИКАЦИЯ ЗАЩИЩЕННЫХ ДАННЫХ	
ДАТА И ВРЕМЯ ЗАЩИТЫ	Отметка времени защиты для этого сообщения AUTACK: дата: 1996.01.16, время: 11:00:00
ОТПРАВИТЕЛЬ ОБМЕНА Идентификатор отправителя обмена	Идентификация отправителя обмена Идентификатор Банка А
ПОЛУЧАТЕЛЬ ОБМЕНА Идентификатор получателя обмена	Идентификация получателя обмена Идентификатор г-на Смита из Компании А
УКАЗАТЕЛИ ЗАЩИТЫ	Указывают на объект защиты (квитируемое сообщение) и соответствующую дату и время
КОНТРОЛЬНЫЙ НОМЕР ОБМЕНА	Определяет контрольный номер обмена для квитируемого сообщения PAYORD: 1
ОТПРАВИТЕЛЬ ОБМЕНА Идентификатор отправителя обмена	Определяет отправителя обмена, в который входило квитируемое сообщение: г-н Смит из Компании А
ПОЛУЧАТЕЛЬ ОБМЕНА Идентификатор получателя обмена	Определяет получателя обмена, в который входило квитируемое сообщение: Банк А
КОНТРОЛЬНЫЙ НОМЕР СООБЩЕНИЯ	Определяет контрольный номер, присвоенный отправителем квитируемому сообщению: 3 (см. пример 1)
ДАТА И ВРЕМЯ ЗАЩИТЫ	Отметка времени защиты для сообщения PAYORD: дата:1996.01.15, время 10:00:00
ЗАЩИТА ПО УКАЗАТЕЛЯМ	
КОНТРОЛЬНЫЙ НОМЕР ЗАЩИТЫ	Определяет соответствующий заголовок: 2
РЕЗУЛЬТАТ ПРОВЕРКИ Квалификатор контрольного значения Контрольное значение	Уникальное контрольное значение: 1 512-битовая цифровая подпись с шестнадцатеричной фильтрацией для квитируемого сообщения PAYORD
ОКОНЧАНИЕ ЗАЩИТЫ	
КОНТРОЛЬНЫЙ НОМЕР ЗАЩИТЫ	Номер данного окончания защиты: 2
ЧИСЛО СЕГМЕНТОВ ЗАЩИТЫ	Число сегментов защиты: 3
ОКОНЧАНИЕ ЗАЩИТЫ	
КОНТРОЛЬНЫЙ НОМЕР ЗАЩИТЫ	Номер данного окончания защиты: 1
ЧИСЛО СЕГМЕНТОВ ЗАЩИТЫ	Число сегментов защиты: 7
РЕЗУЛЬТАТ ЗАЩИТЫ	

РЕЗУЛЬТАТ ПРОВЕРКИ	
Квалификатор контрольного значения	Уникальное контрольное значение: 1
Контрольное значение	512-битовая цифровая подпись с шестнадцатеричной фильтрацией для сообщения AUTACK

Приложение В
(справочное)

Службы и алгоритмы защиты

В.1 Цель и область применения

В настоящем приложении приведены примеры возможных комбинаций элементов данных и значений кодов в группах сегментов защиты. Эти примеры выбраны для иллюстрации широко используемых методов защиты, основанных на международных стандартах.

В настоящем приложении представлен лишь небольшой набор комбинаций. Приведенные алгоритмы и режимы шифрования не должны считаться предписанием. Пользователю предлагается выбирать методы, адекватные угрозам безопасности, от которых он хочет защититься.

Цель данного приложения – предоставить пользователю, уже выбравшему методы защиты, универсальную отправную точку для разработки решения, подходящего для конкретной задачи.

Для лучшего восприятия содержание разбито на три раздела, каждый из которых описывает основные принципы использования защиты.

Три набора комбинаций, представленные в настоящем приложении:

1) комбинации с использованием симметричных алгоритмов и сообщения AUTACK для указанных защищаемых структур;

2) комбинации с использованием асимметричных алгоритмов и сообщения AUTACK для указанных защищаемых структур;

3) комбинации с использованием сообщения AUTACK для квитирования.

Список кодов, используемых в матрицах (подмножество полного списка кодов)

0501	Служба защиты, кодированная	0505	Функция фильтрации, кодированная
1	Неотказуемость источника	6	Фильтр EDC UN/EDIFACT
2	Аутентификация источника сообщения		
9	Целостность указанной структуры EDIFACT		

0523	Область применения алгоритма, кодированная	0527	Алгоритм, кодированный
1	Хеширование владельцем	1	DES (Data Encryption Standard) - стандарт шифрования данных
2	Симметричное шифрование владельцем	10	RSA (Rivest, Shamir, Adleman)- алгоритм Ривеста-Шамира-Адлемана
3	Подпись органом сертификации (CA)	37	MAC (Message Authentication Code) - код аутентификации сообщения
4	Хеширование органом сертификации (CA)	40	MDC2 (Modification Detection Code) - код обнаружения изменений
6	Подпись владельцем	42	HDS2 (Hash functions)- хеш-функции

0531	Квалификатор параметра алгоритма	0563	Квалификатор контрольного значения
12	Модуль	1	Уникальное контрольное значение
13	Экспонента		
14	Длина модуля		

0577	Квалификатор стороны защиты
1	Отправитель сообщения
2	Получатель сообщения
3	Владелец сертификата
4	Аутентифицирующая сторона

Используемые сокращения

a, b, c, d - представления контрольного номера защиты;
CA - орган сертификации;
Enc-Key - зашифрованный ключ;
Hash - значение хеш-функции;
Key-N - имя ключа;
MAC - код аутентификации сообщения;
Mod - модуль;
Mod-L - длина модуля;
PK/CA - открытый ключ органа сертификации;
Pub-K - открытый ключ;
Sig - подпись.

B.2 Комбинации с использованием симметричных алгоритмов и сообщения AUTACK для указанных объектов защиты

Матрица, приведенная в таблице B.1, устанавливает отношения для следующих конкретных ситуаций:

– защита указанного логического объекта обеспечивается сообщением AUTACK (ИСО 9735-6);

– используется только симметричный алгоритм;

– предоставляемыми службами защиты являются аутентификация источника указанной структуры EDIFACT (на примере указанного сообщения) и аутентификация источника сообщения AUTACK. Аутентификация источника указанной структуры обеспечивается контролем целостности этой структуры в сочетании с аутентификацией источника сообщения AUTACK;

– целостность указанной структуры EDIFACT обеспечивается использованием хеш-функции, основанной на алгоритме DES в режиме MDC согласно ИСО/МЭК 10118-2. У отправителя и получателя нет общего секретного ключа. Хешированное значение передается в сообщении AUTACK, и защита этого значения обеспечивается защитой сообщения AUTACK;

– аутентификация источника сообщения AUTACK реализуется с помощью вычисления MAC (кода аутентификации сообщения) для сообщения AUTACK. В этом примере используется алгоритм DES в режиме CBC с секретным ключом, который известен получателю сообщения, и при этом передается только имя ключа. Данный пример соответствует требованиям ИСО 8731-1;

– хотя у отправителя и получателя общие ключи, но механизмы шифрования не были полностью согласованы заранее. Поэтому для всех алгоритмов и режимов шифрования используются явные имена;

– приводятся только поля защиты, связанные с актуальными методами защиты, алгоритмами и режимами шифрования.

Таблица В.1 – Матрица отношений при использовании только симметричных алгоритмов

Тег	Наименование	S (статус)	R (максимальное число повторов)	Целостность указанной структуры EDIFACT по ИСО/МЭК 10118-2	Аутентификация источника сообщения AUTACK по ИСО 8731-1	Примечания
SG 1		M	99	Один для каждой службы защиты		
USH	ЗАГОЛОВОК ЗАЩИТЫ	M	1			
0501	СЛУЖБА ЗАЩИТЫ, КОДИРОВАННАЯ	M	1	9	2	
0534	КОНТРОЛЬНЫЙ НОМЕР ЗАЩИТЫ	M	1	a	b	1
0505	ФУНКЦИЯ ФИЛЬТРАЦИИ, КОДИРОВАННАЯ	C	1	6	6	
S500	ИДЕНТИФИКАЦИОННЫЕ ЭЛЕМЕНТЫ ЗАЩИТЫ	C	2			
0577	Квалификатор стороны защиты	M		1	1	2
0538	Имя ключа	C			Key-N	3
S500	ИДЕНТИФИКАЦИОННЫЕ ЭЛЕМЕНТЫ ЗАЩИТЫ	C	2			
0577	Квалификатор стороны защиты	M		2	2	4
USA	АЛГОРИТМ ЗАЩИТЫ	C	3			
S502	АЛГОРИТМ ЗАЩИТЫ	M	1			
0523	Область применения алгоритма, кодированная	M		1	2	
0525	Криптографический режим, кодированный	C		—	—	
0527	Алгоритм, кодированный	C		40	37	
USB	ИДЕНТИФИКАЦИЯ ЗАЩИЩЕННЫХ ДАННЫХ	M	1	Ссылка на защищаемые структуры данных		
SG 3		M	9999			
USX	УКАЗАТЕЛИ ЗАЩИТЫ	M	1			
USY	ЗАЩИТА ПО УКАЗАТЕЛЯМ	M	9			
0534	КОНТРОЛЬНЫЙ НОМЕР ЗАЩИТЫ	M	1	a	—	5
S508	РЕЗУЛЬТАТ ПРОВЕРКИ	C	2			
0563	Квалификатор контрольного значения	M		1		
0560	Контрольное значение	C		Hash		6
SG 4		M	99			
UST	ОКОНЧАНИЕ ЗАЩИТЫ	M	1			
0534	КОНТРОЛЬНЫЙ НОМЕР ЗАЩИТЫ	M	1	a	b	7
0588	ЧИСЛО СЕГМЕНТОВ ЗАЩИТЫ	M	1			
USR	РЕЗУЛЬТАТ ЗАЩИТЫ	C	1			

Тег	Наименование	S (статус)	R (максимальное число повторов)	Целостность указанной структуры EDIFACT по ИСО/МЭК 10118-2	Аутентификация источника сообщения AUTACK по ИСО 8731-1	Примечания
S508	РЕЗУЛЬТАТ ПРОВЕРКИ	M	2			
0563	Квалификатор контрольного значения	M			1	
0560	Контрольное значение	C			MAC	8

1 – Один заголовок защиты ссылается на окончание защиты AUTACK, а другой – на сегмент защиты по указателям.
2 – Отправитель сообщения.
3 – Имя общего секретного ключа получателя и отправителя AUTACK.
4 – Получатель сообщения.
5 – Ссылается на один из заголовков защиты.
6 – Значение хеш-функции для указанной структуры EDIFACT, которое защищено кодом MAC, вычисленным для сообщения AUTACK.
7 – Ссылается на один из заголовков защиты.
8 – Код MAC, вычисленный для сообщения AUTACK.

В.3 Комбинации с использованием асимметричных алгоритмов и сообщения AUTACK для указанных объектов защиты

Матрица, приведенная в таблице В.2, устанавливает отношения для следующих конкретных ситуаций:

– защита указанного логического объекта обеспечивается сообщением AUTACK (ИСО 9735-6);

– предоставляемыми службами защиты являются обеспечение неотказуемости источника указанной структуры EDIFACT и обеспечение неотказуемости источника сообщения AUTACK. Неотказуемость источника указанной структуры EDIFACT обеспечивается контролем целостности этой структуры в сочетании с неотказуемостью источника сообщения AUTACK;

– используется асимметричный алгоритм RSA;

– для хеш-функции используется алгоритм DES в режиме MDC. Та же хеш-функция служит для расчета хешированного значения защищаемой структуры EDIFACT и сообщения AUTACK;

– предполагается, что обмен сертификатами ранее не выполнялся;

– в сегменте USC явно идентифицированы хеш-функция и функция для вычисления подписи, используемые органом сертификации для подписи сертификата. Открытый ключ этого органа, необходимый для проверки сертификата, уже известен получателю. На него есть ссылка по имени в сегменте USC;

– прилагается только один сертификат: второй сертификат нужен, только если используется открытый ключ получателя.

Таблица В.2 – Матрица отношений при использовании асимметричных алгоритмов

Тег	Наименование	S (статус)	R (максимальное число повторов)	Целостность указанной структуры EDIFACT по ИСО/МЭК 10118-2	Неотказуемость источника сообщения AUTACK (RSA)	Примечания
SG 1		M	99	Один для каждой службы-защиты		
USH	ЗАГОЛОВОК ЗАЩИТЫ	M	1			
0501	СЛУЖБА ЗАЩИТЫ, КОДИРОВАННАЯ	M	1	9	1	1
0534	КОНТРОЛЬНЫЙ НОМЕР ЗАЩИТЫ	M	1	c	d	
0505	ФУНКЦИЯ ФИЛЬТРАЦИИ, КОДИРОВАННАЯ	C	1	6	6	
S500	ИДЕНТИФИКАЦИОННЫЕ ЭЛЕМЕНТЫ ЗАЩИТЫ	C	2			
0577	Квалификатор стороны защиты	M		1	1	2
S500	ИДЕНТИФИКАЦИОННЫЕ ЭЛЕМЕНТЫ ЗАЩИТЫ	C	2			
0577	Квалификатор стороны защиты	M		2	2	3
USA	АЛГОРИТМ ЗАЩИТЫ	C	3			
S502	АЛГОРИТМ ЗАЩИТЫ	M	1			
0523	Область применения алгоритма, кодированная	M		1	1	4
0525	Криптографический режим, кодированный	C		—	—	
0527	Алгоритм, кодированный	C		40	40	
SG 2		C	2		Только один: сертификат отправителя	
USC	СЕРТИФИКАТ	M	1			
0536	НОМЕР СЕРТИФИКАТА	C	1		Номер этого сертификата	

Продолжение таблицы В.2

Тег	Наименование	S (статус)	R (максимальное число повторов)	Целостность указанной структуры EDIFACT по ИСО/МЭК 10118-2	Неотказуемость источника сообщения AUTACK (RSA)	Примечания
S500	ИДЕНТИФИКАЦИОННЫЕ ЭЛЕМЕНТЫ ЗАЩИТЫ	C	2		(владелец сертификата)	
0577	Квалификатор стороны защиты	M			3	5
S500	ИДЕНТИФИКАЦИОННЫЕ ЭЛЕМЕНТЫ ЗАЩИТЫ	C	2		(сторона, выполняющая аутентифика-цию)	
0577	Квалификатор стороны защиты	M			4	6
0538	Имя ключа	C			(имя PK/CA)	
USA	АЛГОРИТМ ЗАЩИТЫ	C	3		(функция подписи отправителя)	
S502	АЛГОРИТМ ЗАЩИТЫ	M	1			
0523	Область применения алгоритма, кодированная	M			6	7
0527	Алгоритм, кодированный	C			10	
S503	ПАРАМЕТР АЛГОРИТМА	C	9		(длина модуля)	
0531	Квалификатор параметра алгоритма	M			14	
0554	Значение параметра алгоритма	M			Mod-L	
S503	ПАРАМЕТР АЛГОРИТМА	C	9		(модуль)	
0531	Квалификатор параметра алгоритма	M			12	
0554	Значение параметра алгоритма	M			Mod	
S503	ПАРАМЕТР АЛГОРИТМА	C	9		(открытая экспонента)	
0531	Квалификатор параметра алгоритма	M			13	
0554	Значение параметра алгоритма	M			Pub-K	
USA	АЛГОРИТМ ЗАЩИТЫ	C	3		(хеш-функция CA для подписи сертификата)	
S502	АЛГОРИТМ ЗАЩИТЫ	M	1			
0523	Область применения алгоритма, кодированная	M			4	8
0525	Криптографический режим, кодированный	C			—	
0527	Алгоритм, кодированный	C			42	
USA	АЛГОРИТМ ЗАЩИТЫ	C	3		(функция генерации подписи CA для подписи сертификата)	
S502	АЛГОРИТМ ЗАЩИТЫ	M	1			
0523	Область применения алгоритма, кодированная	M			3	9
0527	Алгоритм, кодированный	C			10	
USR	РЕЗУЛЬТАТ ЗАЩИТЫ	C	1			
S508	РЕЗУЛЬТАТ ПРОВЕРКИ	M	2			11
0563	Квалификатор контрольного значения	M			1	
0560	Контрольное значение	C			Sig	

Окончание таблицы В.2

Тег	Наименование	S (статус)	R (максимальное число повторов)	Целостность указанной структуры EDIFACT по ИСО/МЭК 10118-2	Неотказуемость источника сообщения AUTACK (RSA)	Примечания
USB	ИДЕНТИФИКАЦИЯ ЗАЩИЩЕННЫХ ДАННЫХ	M	1	Ссылка на защищенные структуры данных		
SG 3		M	9999			
USX	УКАЗАТЕЛИ ЗАЩИТЫ	M	1			
USY	ЗАЩИТА ПО УКАЗАТЕЛЯМ	M	9			
0534	КОНТРОЛЬНЫЙ НОМЕР ЗАЩИТЫ	M	1	c	—	
S508	РЕЗУЛЬТАТ ПРОВЕРКИ	C	2			11
0563	Квалификатор контрольного значения	M		1	—	
0560	Контрольное значение	C		Hash	—	
SG 4		M	99			
UST	ОКОНЧАНИЕ ЗАЩИТЫ	M	1			
0534	КОНТРОЛЬНЫЙ НОМЕР ЗАЩИТЫ	M	1	c	d	
0588	ЧИСЛО СЕГМЕНТОВ ЗАЩИТЫ	M	1			
USR	РЕЗУЛЬТАТ ЗАЩИТЫ	C	1			
S508	РЕЗУЛЬТАТ ПРОВЕРКИ	M	2			11
0563	Квалификатор контрольного значения	M			1	
0560	Контрольное значение	C		—	Sig	

1 – Подразумевается, что аутентификация источника сообщения и целостность сообщения AUTACK включены в службу неотказуемости источника. Неотказуемость источника указанной структуры EDIFACT обеспечивается целостностью этой структуры в сочетании с неотказуемостью источника сообщения AUTACK.
2 – Отправитель сообщения.
3 – Получатель сообщения.
4 – Хеш-функция, значение которой вычислено отправителем для защищенной структуры.
6 – Владелец сертификата: идентификационные данные должны быть теми же, что и в сегменте USH.
(элементе данных S500) для отправителя сообщения.
7 – Сторона, выполняющая аутентификацию: орган сертификации (CA).
8 – Функция генерации подписи отправителя.
9 – Хеш-функция CA.
10 – Функция генерации подписи CA.
11 – Для некоторых алгоритмов генерации подписи (например, DSA) требуется два параметра результата.

В.4 Комбинации с использованием сообщения AUTACK для квитирования

Возможные комбинации для квитирования с помощью сообщений AUTACK соответствуют описанным выше случаям. В частности:

- для USH 0501, код 6 (аутентификация приема), применимы комбинации из матрицы 1;
- для USH 0501, код 5 (неотказуемость приема), применимы комбинации из матрицы 2.

Возможны и необходимы комбинации для других кодов.

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов ссылочным национальным стандартам Российской Федерации

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
ИСО 9735-1:2002	IDT	ГОСТ Р ИСО 9735-1–2012 «Электронный обмен данными в управлении, торговле и на транспорте (EDIFACT). Синтаксические правила для прикладного уровня (версия 4, редакция 1). Часть 1. Синтаксические правила, общие для всех частей»
ИСО 9735-2:2002	IDT	ГОСТ Р ИСО 9735-2–2012 «Электронный обмен данными в управлении, торговле и на транспорте (EDIFACT). Синтаксические правила для прикладного уровня (версия 4, редакция 1). Часть 2. Синтаксические правила, специфичные для пакетного ЭОД»
ИСО 9735-5:2002	IDT	ГОСТ Р ИСО 9735-5–2012 «Электронный обмен данными в управлении, торговле и на транспорте (EDIFACT). Синтаксические правила для прикладного уровня (версия 4, редакция 1). Часть 5. Правила защиты для пакетного ЭОД (аутентичность, целостность и неотказуемость источника)»
ИСО 9735-10:2002		*

* 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 технических регламентов и стандартов.

Примечание: В настоящей таблице использовано следующее условное обозначение степени соответствия стандартов:

IDT – идентичные стандарты.

Библиография

[1] ИСО 8731-1:1987[1)], Операции банковские. Утвержденные алгоритмы аутентификации сообщений. Часть 1. DEA (ISO 8731-1:1987, Banking — Approved algorithms for message authentication — Part 1: DEA)

[2] ИСО/МЭК 10118-2:2000[2)], Информационные технологии. Методы защиты. Хеш-функции. Часть 2. Хеш-функции с использованием алгоритма шифрования n-битными блоками (ISO/IEC 10118-2:2000, Information technology — Security techniques — Hash-functions — Part 2: Hash-functions using a n-bit block cipher)

[1)] Отменен. Действует ИСО 16609:2004.

[2)] Отменен. Действует ИСО/МЭК 10118-2:2010.

УДК 658.6/.9:002.006.354 ОКС 35.240.60

Ключевые слова: электронный обмен данными, синтаксические правила, EDIFACT

Подписано в печать 01.08.2014. Формат 60x84 1/8.
Усл. печ. л. 5,12. Тираж 48 экз. Зак. 2918.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

ФГУП «СТАНДАРТИНФОРМ»

123995 Москва, Гранатный пер., 4.

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

gost.e-ecolog.ru