ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО 9735-7— 2016

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

Синтаксические правила для прикладного уровня (версия 4, редакция 1)

Часть 7

Правила защиты для пакетного EDI (конфиденциальность)

(ISO 9735-7:2002, IDT)

Издание официальное

Москва
Стандартинформ
2016

gost.e-ecolog.ru

Предисловие

1 ПОДГОТОВЛЕН Автономной некоммерческой организацией «Институт безопасности труда» (АНО «ИБТ») на основе собственного перевода на русский язык англоязычной версии 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 30 ноября 2016 г. № 1899-ст

4 Настоящий стандарт идентичен международному стандарту ИСО 9735-7:2002 «Электронный обмен данными в управлении, торговле и на транспорте (EDIFACT). Синтаксические правила для прикладного уровня (версия 4, редакция 1). Часть 7. Правила защиты для пакетного EDI (конфиденциальность)» (ISO 9735-7:2002 [«Electronic data interchange for administration, commerce and transport (EDIFACT) — Application level syntax rules (Syntax version number 4, Syntax release number 1) — Part 7: Security rules for batch EDI (confidentiality)», 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 ежемесячном информационном указателе «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, 2016

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 и определения . . . 2
4 Соответствие данному стандарту . . . 2
5 Правила обеспечения конфиденциальности EDI . . . 2
5.1 Конфиденциальность EDIFACT . . . 2
5.2 Принципы использования . . . 7
Приложение А (справочное) Примеры защиты сообщения . . . 9
Приложение В (справочное) Пример процесса обработки . . . 11
Приложение С (справочное) Служба и алгоритмы обеспечения конфиденциальности . . . 13
Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов национальным стандартам Российской Федерации . . . 19
Библиография . . . 20

Введение

Данная часть стандарта 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 ООН (UN/ECE) в качестве синтаксических правил организации электронного обмена данными в управлении, торговле и на транспорте (EDIFACT) и являются частью «Каталога ООН по информационному обмену в сфере торговли» (UNTDID), который содержит также рекомендации по разработке сообщений пакетного и интерактивного обмена.

Эта часть может использоваться в любых приложениях, но сообщения, к которым применяются указанные правила, могут определяться только как сообщения типа EDIFACT, если они соответствуют другим рекомендациям, правилам и справочникам в UNTDID. К сообщениям UN/EDIFACT — пакетным или интерактивным — должны применяться соответствующие правила построения сообщений. Эти правила поддерживаются в UNTDID.

Спецификации и протоколы обмена сообщениями в рамках данной части не рассматриваются.

Часть 7 — это новая часть, добавленная в стандарт 9735. Она создает дополнительную возможность обеспечения конфиденциальности структур данных EDIFACT, например таких, как сообщение, пакет, группа или информационный обмен.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

Синтаксические правила для прикладного уровня (версия 4, редакция 1)

Часть 7

Правила защиты для пакетного EDI (конфиденциальность)

Electronic data interchange for administration, commerce and transport (EDIFACT). Application level syntax rules (Syntax version number 4, Syntax release number 1). Part 7. Security rules for batch EDI (confidentiality)

Дата введения — 2017—09—01

1 Область применения

Настоящая часть стандарта, касающаяся безопасности пакетного EDIFACT, охватывает защиту уровня сообщений/пакетов, уровня групп и уровня информационного обмена посредством обеспечения их конфиденциальности в соответствии с принятыми механизмами защиты.

2 Нормативные ссылки

Приведенные ниже нормативные документы содержат положения, на которые даются ссылки в настоящем тексте и которые, следовательно, становятся положениями данной части стандарта. Для датированных (жестких) ссылок применимо только указываемое издание: никакие его последующие изменения или редакции не применимы. Однако участникам договоров, в которых используется настоящая часть, рекомендуется изучить возможность применения самых последних изданий ссылочных документов, указанных ниже. Применительно к недатированным ссылочным документам (с плавающими ссылками) действующим остается самое последнее издание нормативного документа. Членами ISO и IEC ведутся реестры действующих международных стандартов.

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 [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 9735-2:2002, 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 [Электронный обмен данными в управлении, торговле и на транспорте (EDIFACT). Синтаксические правила для прикладного уровня (версия 4, редакция 1). Часть 2. Специфика синтаксических правил для пакетного EDI]

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) [Электронный обмен данными в управлении, торговле и на транспорте (EDIFACT). Синтаксические правила для прикладного уровня (версия 4, редакция 1). Часть 5. Правила безопасности для пакетного EDI (подлинность, целостность и невозможность отказа отправителя от авторства сообщения]

ISO 9735-10:2002, Electronic data interchange for administration, commerce and transport (EDIFACT). Application level syntax rules (Syntax version number 4, Syntax release number 2). Part 10. Syntax service directories [Электронный обмен данными в управлении, торговле и на транспорте (EDIFACT). Синтаксические правила для прикладного уровня (версия 4, редакция 1). Часть 10. Каталоги синтаксической службы]

Издание официальное

ISO/IEC 10181-5:1996, Information technology — Open Systems Interconnection — Security frameworks for open systems. Part 5. Confidentiality framework (Информационные технологии. Взаимодействие открытых систем. Основы безопасности для открытых систем. Часть 5. Основы конфиденциальности)

3 Термины и определения

В настоящем стандарте применены термины по ИСО 9735-1.

4 Соответствие данному стандарту

Для соответствия обмена этой части в его обязательном элементе 0002 (номер версии синтаксических правил) должен использоваться номер версии "4", а в условно-обязательном элементе данных 0076 (номер редакции синтаксических правил) должен указываться номер редакции «01», причем каждый из этих номеров появляется в сегменте UNB (заголовок обмена); однако в обменах, где продолжает использоваться синтаксис, определенный в более ранних версиях, для различения соответствующих синтаксических правил друг от друга и от правил, определенных в данной части, должны использоваться 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 и его Изменение 1:1992 — Номер версии синтаксических правил: 3

ИСО 9735:1998 — Номер версии синтаксических правил: 4

Соответствие стандарту означает, что соблюдены все его требования, включая все возможные 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, если их структура и представление отвечают синтаксическим правилам, определенным в данной части стандарта ИСО 9735.

Устройства, поддерживающие настоящую часть стандарта ИСО 9735, признаются соответствующими ему, если эти устройства способны формировать и/или интерпретировать данные, структурированные и представленные в соответствии с требованиями этого стандарта.

Соответствие требованиям настоящей части предполагает обязательное соответствие частям 1, 2, 5 и 10 стандарта ИСО 9735.

Положения смежных стандартов, на которые делается ссылка в настоящей части ИСО 9735, являются составными элементами критериев соответствия.

5 Правила обеспечения конфиденциальности EDI

5.1 Конфиденциальность EDIFACT

5.1.1 Общие положения

Угрозы безопасности, свойственные процессам передачи данных EDIFACT, и службы защиты, связанные с устранением этих угроз, описываются в приложениях A и B стандарта ИСО 9735-5:2002.

В данном подразделе представлено техническое решение по формированию структур EDIFACT, обеспечиваемых защитой конфиденциальности.

Конфиденциальность структуры EDIFACT (сообщения, пакета, группы или обмена) должна обеспечиваться путем шифрования тела сообщения, объекта, сообщений/пакетов или сообщений/пакетов/групп, соответственно, наряду с любыми другими защитными группами сегментов заголовка и концевика, с использованием надлежащего криптографического алгоритма. Эти шифрованные данные могут отфильтровываться для использования в сетях секретной связи.

5.1.2 Конфиденциальность пакетного EDI

5.1.2.1 Конфиденциальность процедуры информационного обмена

На рисунке 1 представлена структура одного обмена, защищенного с помощью механизма обеспечения конфиденциальности. Рекомендация служебной строки (UNA), сегмент заголовка обмена (UNB) и сегмент концевика обмена (UNZ) шифрованием не затрагиваются.

В случае применения процедуры сжатия данных она должна осуществляться перед шифрованием.

Алгоритм и параметры шифрования, сжатия и фильтрации определяются в группе сегментов заголовка системы безопасности (защиты).

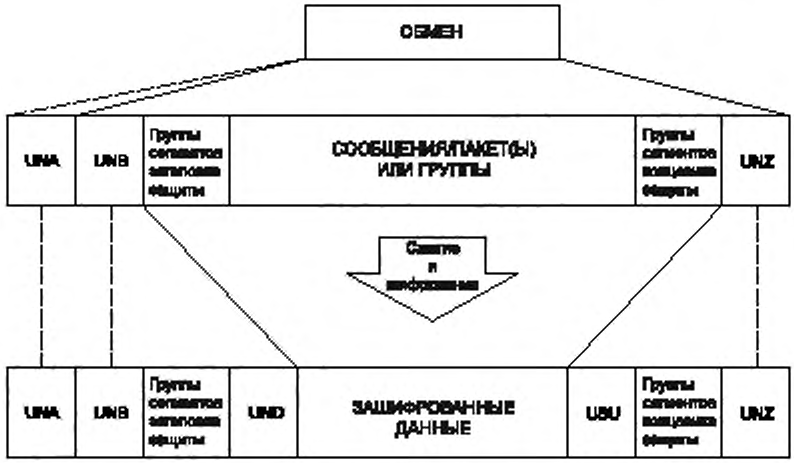


Рисунок 1 — Схематическое представление структуры EDI с зашифрованным информационным наполнением (сообщения/пакеты или группы)

5.1.2.2 Конфиденциальность группы

На рисунке 2 представлена структура обмена, содержащего одну шифрованную группу, которая была зашифрована также и для других служб безопасности (защиты). Шифрование не повлияло на сегмент заголовка группы (UNG) и сегмент концевика группы (UNE).

В случае применения процедуры сжатия данных она должна осуществляться перед шифрованием.

Алгоритм и параметры шифрования, сжатия и фильтрации определяются в группе сегментов заголовка системы безопасности (защиты).

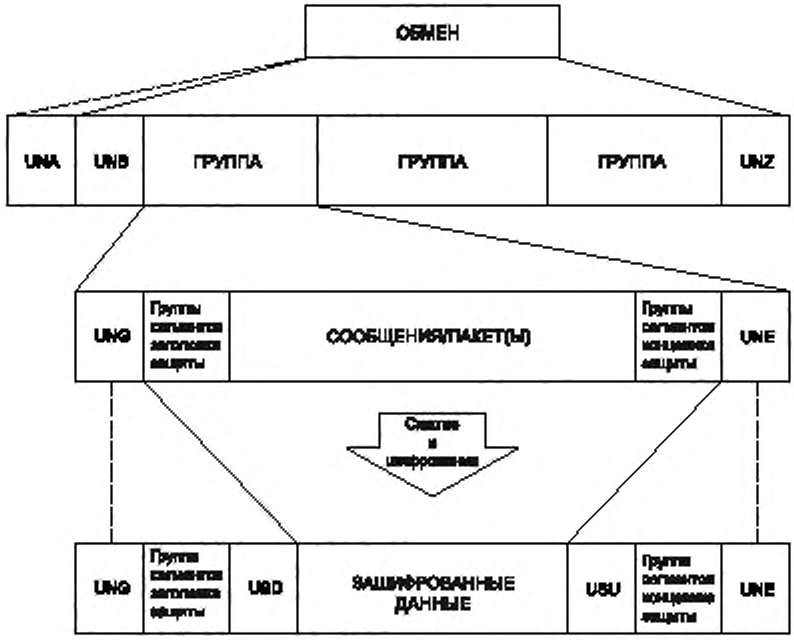


Рисунок 2 — Схематическое представление структуры обмена, содержащего одну группу, информационное наполнение которой (тело группы и ассоциируемые с ним группы сегментов заголовка и концевика защиты) было зашифровано

5.1.2.3 Конфиденциальность сообщения

На рисунке 3 представлена структура обмена, содержащего одно шифрованное сообщение, которое было зашифровано также и для другой службы безопасности. Шифрование не повлияло на сегмент заголовка сообщения (UNH) и сегмент концевика сообщения (UNT).

В случае применения процедуры сжатия данных эта процедура должна осуществляться перед шифрованием.

Алгоритм и параметры шифрования, сжатия и фильтрации определяются в группе сегментов заголовка системы безопасности (защиты).

5.1.2.4 Конфиденциальность пакета

На рисунке 4 представлена структура обмена, содержащего один шифрованный пакет, который был зашифрован также для другой службы защиты. Шифрование не повлияло на сегмент заголовка пакета (UNO) и сегмент концевика пакета (UNP).

В случае применения процедуры сжатия данных она должна осуществляться перед шифрованием.

Алгоритм и параметры шифрования, сжатия и фильтрации определяются в группе сегментов заголовка защиты.

5.1.3 Структура сегмента заголовка и концевика системы шифрования данных

Таблица 1 — Группы сегментов заголовка и концевика системы безопасности

МЕТКА	Наименование	S	R
———	Группа сегментов 1 ———	C	99
USH	Заголовок защиты	M	1
USA	Алгоритм защиты	C	3
———	Группа сегментов 2 ———	C	2
USC	Сертификат	M	1
USA	Алгоритм защиты	C	3
USR	Результат защиты	C	1
USD	Заголовок системы шифрования данных Зашифрованные данные	M	1
USU	Концевик системы шифрования данных	M	1
———	Группа сегментов n ———	C	99
UST	Концевик защиты	M	1
USR	Результат защиты	C	1

Примечание — Сегменты USH, USA, USC, USR и UST определяются стандартом ISO 9735-10. В настоящей части стандарта ISO 9735 они не детализируются.

5.1.4 Детализация сегмента данных n

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

Группа сегментов, идентифицирующая службу защиты и применяемые механизмы обеспечения безопасности; содержит данные, необходимые для выполнения вычислений, связанных с контролем достоверности.

Для обеспечения конфиденциальности должна использоваться только одна группа сегментов заголовка системы безопасности:

USH — заголовок системы обеспечения защиты

Сегмент, определяющий службу безопасности, используемую для обеспечения конфиденциальности структуры EDIFACT, в которую включен данный сегмент (как описано в стандарте ISO 9735-5)

USA — алгоритм защиты

Сегмент, идентифицирующий алгоритм обеспечения безопасности и его техническую реализацию и содержащий необходимые технические параметры. Это могут быть алгоритмы, применяемые к телу сообщения, объекту, сообщениям/пакетам или сообщениям/пакетам/группам. Такие алгоритмы должны быть патентованными симметричными, патентованными сжимающими или патентованными сжимающими с контролем целостности.

Асимметричные алгоритмы не должны вызываться непосредственно в сегменте USA внутри группы сегментов 1, а могут появляться только внутри группы сегментов 2, которая активизируется сегментом USC.

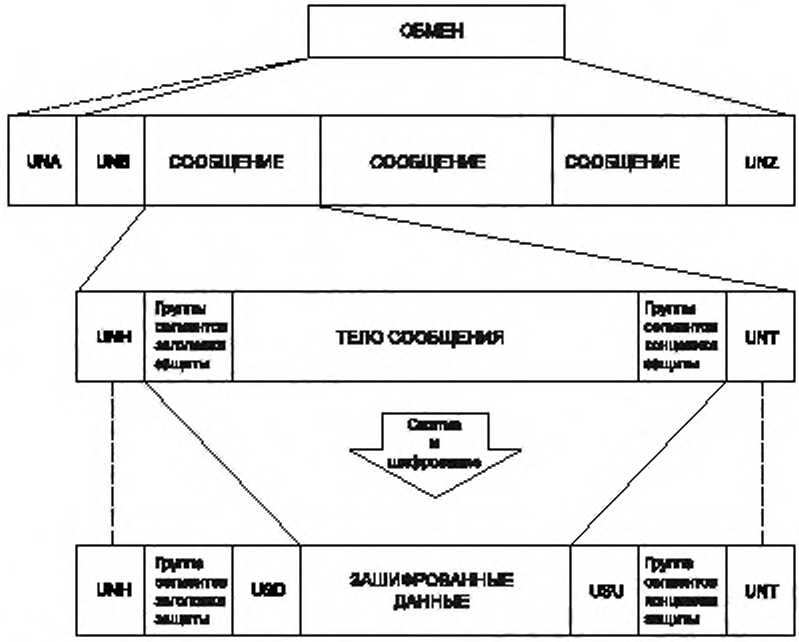


Рисунок 3 — Схематическое представление структуры обмена, содержащего одно сообщение, информационное наполнение которого (тело сообщения и связанные с ним группы сегментов заголовка и концевика защиты) было зашифровано

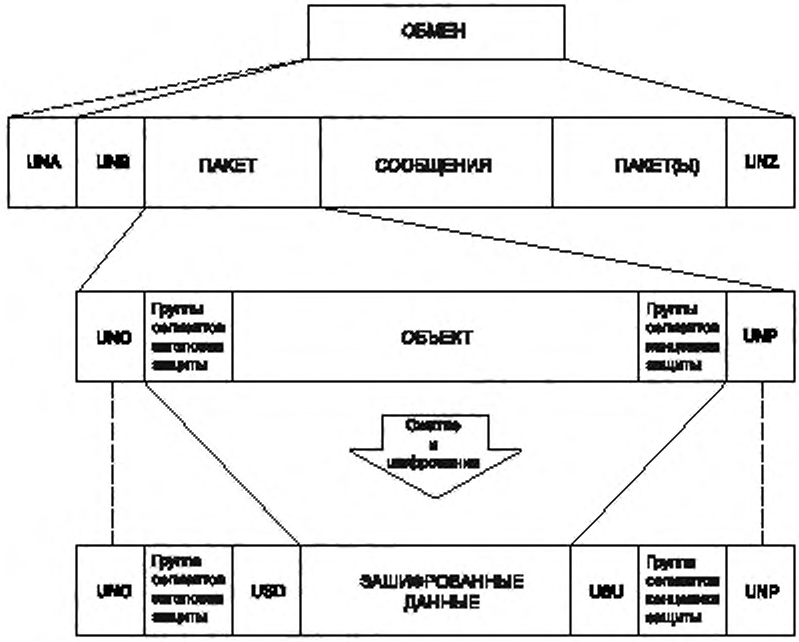


Рисунок 4 — Схематическое представление структуры обмена с одним пакетом, информационное наполнение которого (объект и ассоциируемые с ним группы сегментов заголовка и концевика защиты) были зашифрованы

Если перед шифрованием применяется алгоритм сжатия (компрессии) данных, то имеющийся сегмент USA используется для задания алгоритма и дополнительного режима функционирования. В этом сегменте могут задаваться значения добавочных параметров — например, исходное дерево каталогов.

Если же применяется компрессия, а используемый алгоритм сжатия не имеет встроенного механизма контроля целостности, то присутствующий сегмент USA предоставляет возможность задать такой механизм. Конкретное значение параметра целостности вычисляется по сжатому тексту до начала его шифрования. Местоположение (т.е. октетное смещение) параметра контроля целостности внутри сжатых данных может задаваться как значение параметра. Величина смещения параметра контроля целостности (выраженная в октетах) задается косвенно алгоритмом контроля целостности.

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

Группа сегментов, содержащая данные, которые необходимы для контроля подлинности методов защиты структуры EDIFACT при использовании асимметричных алгоритмов (в соответствии с требованиями ISO 9735-5).

Сегмент USC — сертификат

Сегмент, который содержит мандат владельца сертификата и идентифицирует сертификационный орган, выдавший этот сертификат (в соответствии с требованиями ISO 9735-5).

USA — алгоритм защиты

Сегмент, идентифицирующий алгоритм обеспечения безопасности и его техническую реализацию и содержащий необходимые технические параметры защиты (согласно требованиям ISO 9735-5).

Сегмент USR — результат защиты

Сегмент, содержащий результат применения функций защиты к идентифицированному сертификату (в соответствии с ISO 9735-5).

USD — заголовок системы шифрования данных

Этот сегмент задает объем сжатых (опционально), зашифрованных и отфильтрованных (опционально) данных, выраженный числом октетов. Может быть также задан ссылочный номер для идентификации зашифрованной структуры EDIFACT. При наличии такого номера он должен быть одним и тем же в сегментах USD и USU.

В случае использования операции дополнения незначащей информацией может быть определено число добавленных октетов.

Зашифрованные данные

В этой части находятся данные, зашифрованные с помощью алгоритмов и механизмов, определенных в группе сегментов заголовка системы обеспечения безопасности.

Сегмент USU — концевик системы шифрования данных

Этот сегмент задает длину сжатых (опционально), зашифрованных и отфильтрованных (опционально) данных, выраженную числом октетов. Может быть также задан ссылочный номер для идентификации зашифрованной структуры EDIFACT. При наличии такого номера он должен быть одним и тем же в сегментах USD и USU.

Группа сегментов n: UST-USR (группа сегментов концевика системы защиты)

Группа, содержащая ссылку на группу сегментов заголовка системы безопасности и на результат применения защитных функций к структуре EDIFACT (в соответствии с ISO 9735-5).

Сегмент UST — концевик системы защиты

Сегмент, который является связующим звеном между группой заголовка системы безопасности и группой сегментов ее концевика и устанавливает суммарное число защитных сегментов, содержащихся в этих группах с добавлением к нему сегментов USD и USU.

Сегмент USR — результат защиты

Сегмент, содержащий результат применения к структуре EDIFACT функций защиты, заданных в группе заголовка системы безопасности (как это определено в ISO 9735-5). Этот сегмент не должен быть задействован в службе обеспечения конфиденциальности.

5.1.5 Использование заголовка и концевика системы шифрования данных для обеспечения конфиденциальности

Структура EDIFACT, преобразуемая в зашифрованные данные, упаковывается в «оболочку» между заголовком и концевиком службы шифрования данных. Зашифрованные данные и соответствующие группы сегментов заголовка и концевика замещают собой первоначальное тело сообщения, объект или группы сообщений/пакетов. Заголовок и концевик зашифрованной структуры EDIFACT применяемой процедурой шифрования не затрагиваются.

Зашифрованные данные должны начинаться сразу за разделителем после сегмента USD, задающего длину зашифрованных данных, выраженную числом октетов. Зашифрованные данные сопровождаются сегментом USU, вновь задающим их длину, которая должна быть такой же, как и в сегменте USD.

5.1.6 Использование групп сегментов заголовка и концевика системы шифрования данных для обеспечения конфиденциальности

Как определено стандартом ISO 9735-5, для этого необходимо включить одну группу сегментов заголовка системы безопасности, определяющую конфиденциальность, и одну группу сегментов концевика. Группа сегментов концевика системы безопасности, используемая для обеспечения конфиденциальности, должна содержать только сегмент UST.

Как только структура EDIFACT зашифрована, ей больше не должны предоставляться никакие другие услуги системы защиты.

5.2 Принципы использования

5.2.1 Множественные услуги системы безопасности

Если помимо обеспечения конфиденциальности одновременно требуется получение нескольких других услуг системы безопасности, они должны предоставляться в соответствии с правилами, установленными стандартом ISO 9735-5, до шифрования структуры EDIFACT отправляющей стороной. Принимающая сторона должна при этом выполнить соответствующие операции контроля достоверности после дешифрования структуры EDIFACT.

5.2.2 Конфиденциальность

Конфиденциальность структуры EDIFACT должна обеспечиваться согласно принципам, изложенным в стандарте ISO/IEC 10181-5.

Услуга по обеспечению конфиденциальности должна определяться в группе сегментов заголовка системы защиты, а в сегменте USA группы 1 должен быть задан соответствующий алгоритм. Этот сегмент USA может также содержать данные, необходимые для установления ключевых взаимосвязей между сторонами, выступающими в качестве инициатора и в качестве адресата защиты.

Сторона, действующая как инициатор защиты, должна зашифровать структуру EDIFACT от терминатора сегмента ее заголовка (обмена, группы, сообщения или пакета) и вплоть до первого символа концевика ее сегмента (обмена, группы, сообщения или пакета) и рассматривать результат как шифрованные данные. По получении шифрованных данных сторона, действующая как адресат защиты, должна произвести дешифрование зашифрованных данных и таким образом восстановить исходную структуру EDIFACT, исключив из нее сегменты заголовка и концевика.

5.2.3 Внутренние функции представления и фильтрации

Результатом процесса шифрования оказывается случайная битовая последовательность. Это может вызвать определенные проблемы, связанные с довольно ограниченной пропускной способностью телекоммуникационных сетей. Во избежание этих проблем зашифрованная битовая последовательность может быть отображена на конкретный набор знаков с помощью функции фильтрации.

Цель применения функции фильтрации состоит в расширении объема шифрованных данных. Используемые функции фильтрации могут иметь слегка разнящиеся коэффициенты расширения. Некоторые из них допускают присутствие в отфильтрованном тексте любого символа из целевого набора знаков, в том числе служебных — таких, как терминаторы сегментов, тогда как другие могут эти служебные символы отфильтровывать.

Объем данных, пересылаемых в элемент «длина данных в октетах» сегментов USD и USU, должен отображать длину (возможно, сжатых) зашифрованных (и, возможно, отфильтрованных) данных. Это отображение должно использоваться для определения конца шифрованных данных. Используемая фильтрующая функция должна указываться в элементе 0505 (код фильтрующей функции) сегмента USH из группы сегментов заголовка системы обеспечения конфиденциальности.

5.2.4 Использование метода сжатия перед шифрованием

Поскольку стоимость вычислений, связанных с шифрованием данных, напрямую зависит от размера данных, подлежащих шифрованию, может оказаться полезным их предварительное сжатие перед шифрованием.

Большинство методов сжатия данных не может работать эффективно на шифрованной текстовой информации, даже если она отфильтрована, и поэтому при необходимости сжатия данных они должны осуществляться перед шифрованием.

В дальнейшем, при использовании службы обеспечения конфиденциальности, в группе сегментов заголовка системы безопасности может появиться индикация того факта, что данные были сжаты перед шифрованием, а также могут быть указаны использованный алгоритм сжатия и опциональные параметры. В этом случае для восстановления первоначальной структуры EDIFACT сжатые данные после дешифрования должны быть развернуты.

5.2.5 Последовательность выполнения операций

5.2.5.1 Шифрование и сопутствующие ему операции

Для обработки структуры EDIFACT с целью обеспечения конфиденциальности данных необходимо выполнить следующие операции:

1. Произвести сжатие структуры EDIFACT (опционально) и вычислить контрольное значение параметра целостности для сжатых данных (опционально).
2. Зашифровать структуру EDIFACT (сжатую и защищенную контрольным параметром целостности).
3. Произвести фильтрацию сжатых и защищенных контрольным параметром целостности данных (возможно, зашифрованных).

5.2.5.2 Дешифрование и сопутствующие ему операции

Для обработки зашифрованной структуры EDIFACT с целью восстановления ее первоначального вида необходимо выполнить следующие операции:

1. Восстановить нефильтрованный вид зашифрованных данных (если они были отфильтрованы).
2. Произвести дешифрование зашифрованных данных.
3. Проверить контрольное значение параметра целостности зашифрованных данных (если таковое имеется) и развернуть (осуществить декомпрессию) зашифрованных данных для восстановления первоначального вида структуры EDIFACT (если она была сжата).

Приложение А
(справочное)

Примеры защиты сообщения

А.1 Введение

Приведенный ниже пример иллюстрирует применение сегментов службы безопасности.

Этот пример обеспечения конфиденциальности сообщения основан на использовании вымышленных платежных поручений в сеансе EDIFACT. Описанные здесь механизмы защиты совершенно не зависят от типа сообщений и применимы к любому сообщению EDIFACT.

Пример показывает, каким образом сегменты службы безопасности могут использоваться для обеспечения конфиденциальности информационного наполнения сообщения в случае применения метода, основанного на **симметричном алгоритме** защиты. Предварительно взаимодействующие партнеры обменялись симметричным ключом, и группа сегментов заголовка системы безопасности содержит только два довольно простых сегмента.

А.2 Описание примера

Компания А заказывает Банку А (код типа 603000) услугу по списанию с ее счета 00387806 суммы 54345 фунтов и 10 пенсов 9 апреля 1995 года. Эта сумма должна быть переведена в Банк В (код типа 201827) на счет 00663151 Компании В, находящейся по адресу West Dock, Milford Haven. Платеж производится на основании выставленного счета № 62345. Контактное лицо получателя платежа — м-р Джонс, отдел продаж.

Банк А требует, чтобы платежное поручение было защищено службой безопасности "Конфиденциальность сообщения".

Такая защита осуществляется путем шифрования тела сообщения с помощью симметричного стандартного кода (DES) на стороне отправителя сообщения. При этом предполагается, что предварительно состоялся обмен секретным ключом DES между Компанией А и Банком А. В целях уменьшения объема передаваемой информации тело сообщения сжимается перед выполнением процедуры шифрования. Для этого используется алгоритм сжатия, представленный в стандарте ISO/IEC 12042:1993. *Информационные технологии. Уплотнение данных для обмена информацией. Алгоритм двоичного арифметического кодирования.*

А.3 Характеристики безопасности

В дальнейшем будет осуществляться обращение только к группам сегментов заголовка и сегментов концевика службы конфиденциальности.

ЗАГОЛОВОК СИСТЕМЫ БЕЗОПАСНОСТИ	
СЛУЖБА ЗАЩИТЫ	Конфиденциальность сообщения
ССЫЛОЧНЫЙ НОМЕР ЗАЩИТЫ	Этот заголовок имеет ссылочный номер 1.
ФУНКЦИЯ ФИЛЬТРАЦИИ	Все двоичные значения отфильтровываются 16-ричным фильтром.
КОДИРОВАНИЕ ИСХОДНОГО НАБОРА СИМВОЛОВ	При шифровании сообщение было представлено в 8-битовом АСКИ-коде.
УТОЧНЕНИЕ ИДЕНТИФИКАТОРА ЗАЩИТЫ Отправитель сообщения (сторона, шифрующая сообщение).	М-р СМИТ из Компании А
УТОЧНЕНИЕ ИДЕНТИФИКАТОРА ЗАЩИТЫ Адресат сообщения (сторона, дешифрующая сообщение).	Банк А
ПОРЯДКОВЫЙ НОМЕР В СЛУЖБЕ ЗАЩИТЫ	Порядковый номер этого сообщения в службе защиты 001.
SECURITY DATE AND TIME	Отметка времени: дата 1995 04 09, время 13:59:50.
АЛГОРИТМ ЗАЩИТЫ	
АЛГОРИТМ ЗАЩИТЫ Используемый алгоритм Криптографический режим работы Алгоритм Механизм дополнения незначащей информацией	 Используется симметричный алгоритм обеспечения конфиденциальности сообщения Используется режим поблочной передачи зашифрованного текста. Используется алгоритм DES. Используется схема дополнения двоичными нулями.

ПАРАМЕТР АЛГОРИТМА Спецификатор параметра алгоритма Значение параметра алгоритма	 Идентифицирует значение параметра этого алгоритма как имя симметричного ключа, переданное в предварительном сеансе обмена. Используется ключ с именем ENC-KEY1.
АЛГОРИТМ ЗАЩИТЫ	
АЛГОРИТМ ЗАЩИТЫ Способ использования алгоритма Алгоритм	 Алгоритм уплотнения используется для сокращения размера сообщения перед его шифрованием. Используется алгоритм сжатия ИСО 12042.
ЗАГОЛОВОК ШИФРОГРАММЫ	
ДЛИНА ДАННЫХ В ОКТЕТАХ ССЫЛОЧНЫЙ НОМЕР ШИФРОГРАММЫ ЧИСЛО БАЙТОВ ДОПОЛНЕНИЯ	Размер сжатого, зашифрованного и отфильтрованного тела сообщения. Ссылочный номер: 1. Число байтов дополнения: 4.
Зашифрованные данные	
Зашифрованные данные	Сжатое, зашифрованное и отфильтрованное тело сообщения
КОНЦЕВИК ШИФРОГРАММЫ	
ДЛИНА ДАННЫХ В ОКТЕТАХ ССЫЛОЧНЫЙ НОМЕР ШИФРОГРАММЫ	Размер сжатого, зашифрованного и отфильтрованного тела сообщения. Ссылочный номер: 1.
КОНЦЕВИК ЗАЩИТЫ	
ЧИСЛО ЗАЩИТНЫХ СЕГМЕНТОВ	Число сегментов: 6. (USH, USA, USA, USD, USU, UST)
ССЫЛОЧНЫЙ НОМЕР ЗАЩИТЫ	Ссылочный номер данного концевика защиты: 1.

Приложение В
(справочное)

Пример процесса обработки

В.1 Пример шифрования

Диаграмма, представленная на рисунке В.1, иллюстрирует процесс обработки. Конкретные его реализации могут содержать разные последовательности операций и разные конкретные компоненты.

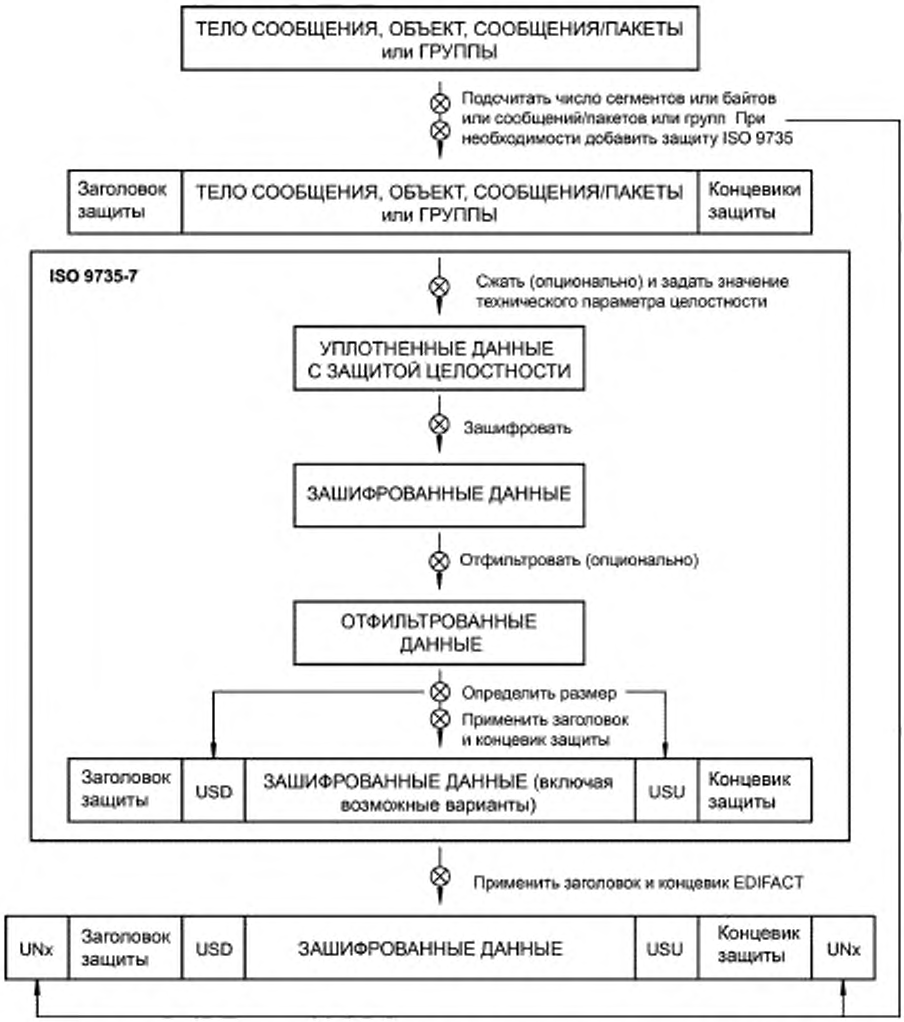


Рисунок В.1 — Процессы, задействованные в шифровании структуры EDIFACT

В.2 Пример дешифрования

Диаграмма, представленная на рисунке В.2, иллюстрирует процесс обработки. Конкретные его реализации могут содержать разные последовательности операций и разные конкретные компоненты.

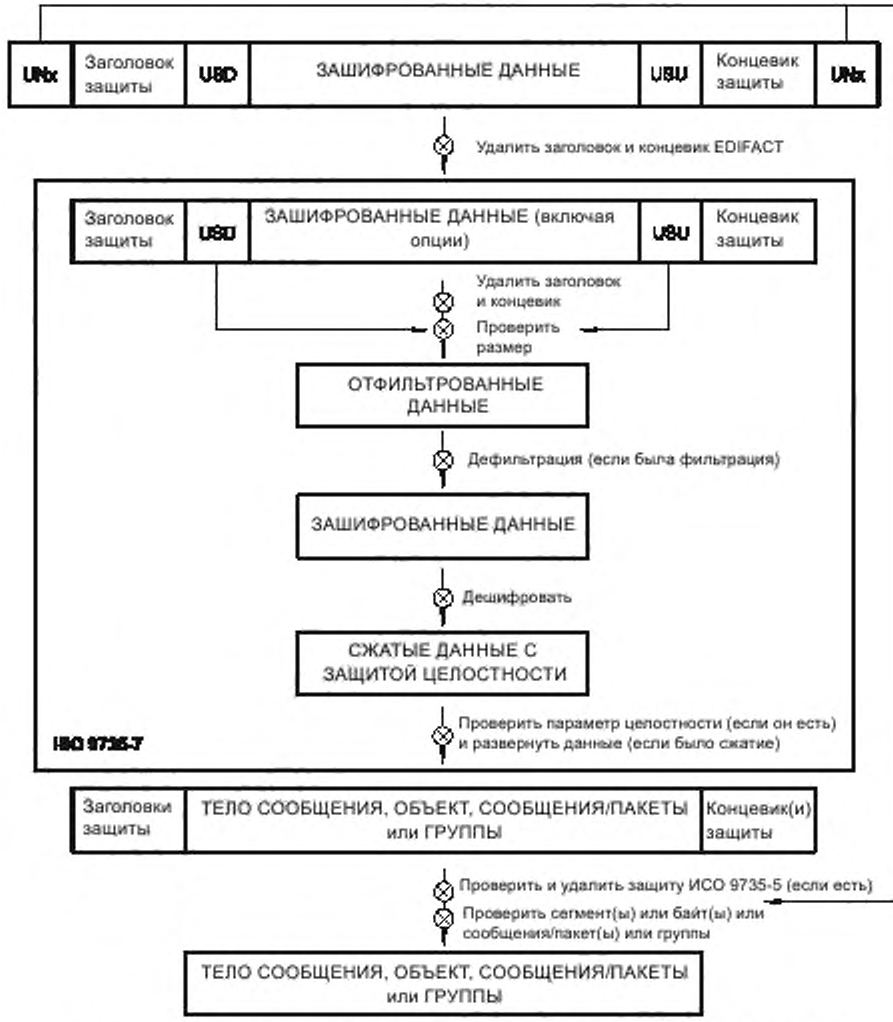


Рисунок В.2 — Процессы, задействованные в дешифровании структуры EDIFACT

Приложение С
(справочное)

Служба и алгоритмы обеспечения конфиденциальности

С.1 Цель и область применения

В данном приложении приводятся примеры возможных комбинаций элементов данных и кодовых значений из групп защитных сегментов. Эти примеры подобраны специально для иллюстрации некоторых широко используемых методов защиты данных на основе требований международных стандартов.

Полный набор возможных комбинаций слишком широк, чтобы его можно было представить в этом приложении. Поэтому отобранные здесь примеры не должны рассматриваться как рекомендованные алгоритмы или режимы функционирования. Пользователям стандарта предлагается самостоятельно выбирать подходящие методы для защиты от предполагаемых ими угроз безопасности.

Цель данного приложения состоит в том, чтобы предоставить пользователю, который уже выбрал подходящие методы защиты, достаточно широкие возможности для реализации надлежащих технических решений в своей конкретной прикладной системе.

Перечень кодов, используемых в приведенных матрицах (выборка из полного списка кодов)

0501	***Код службы безопасности (защиты)***
4	Конфиденциальность

0523	***Код используемого алгоритма***
3	Подпись запрашивающей стороны
4	Хеширование на стороне запроса
5	Патентованный метод шифрования
8	Патентованный метод сжатия
9	Патентованный метод обеспечения целостности при сжатии

0525	***Код криптографического режима***
2	CBC (режим DES)
16	DSMR (схема цифровой подписи для дешифрования сообщения)
36	CTS (режим RC5)

0527	***Код алгоритма шифрования***
1	DES (Data Encryption Standard) — стандарт шифрования данных
4	IDEA (International Data Encryption Algorithm) — международный алгоритм шифрования данных
10	RSA — RSA-кодирование
14	RIPEMD-160 (специальная хеш-функция №1)
18	ZLIB (алгоритм сжатия данных)
25	CRC-32 (Cyclic Redundancy Check) — циклический избыточный код
27	ISO12042 (стандарт сжатия данных)
29	RC5 (симметричный блочный код с переменной длиной ключа)

0531	***Спецификатор параметра алгоритма***
5	Симметричный ключ, зашифрованный симметричным ключом
6	Симметричный ключ, зашифрованный открытым ключом
9	Имя симметричного ключа
10	Имя секретного ключа
12	Абсолютная величина
13	Экспонента
14	Длина модуля

0563	***Спецификатор контрольного значения***
1	Уникальное контрольное значение

0577	*Спецификатор стороны защиты*
1	Отправитель сообщения
2	Получатель сообщения
3	Владелец сертификата
4	Проверяющая сторона

0591	*Код механизма дополнения незначащей информацией*
1	Дополнение нулями
2	Дополнение по стандарту PKCS #1
4	Дополнение по стандарту TBSS

Используемые сокращения

a123, 1, ABC99	=	представления ссылочного номера защиты
CA	=	Certification Authority (сертификационный орган)
CA-Sig	=	CA-Signature (подпись сертификационного органа)
Enc-Key	=	Encrypted Key (секретный ключ)
Exp	=	открытая экспонента
Key-N	=	Key Name (имя ключа)
Len	=	Длина (сжатых) зашифрованных (и отфильтрованных) данных, выраженная числом октетов
Mod	=	Public modulus (открытый модуль)
Mod-L	=	длина модуля
PK/CA	=	Public Key of Certification Authority (открытый ключ сертификационного органа)

С.2 Комбинации, в которых используются симметричные алгоритмы и интегрированные сегменты защиты для обеспечения конфиденциальности структуры EDIFACT

Матрица, приведенная в табл. С1, устанавливает взаимосвязи для следующих случаев:

- защита на уровне интегрированной структуры сообщение/пакет/группа/обмен (ISO 9735-7);
- использование симметричных алгоритмов шифрования;
- использование симметричных и несимметричных алгоритмов для обмена ключами;
- службы защиты, обеспечивающие конфиденциальность;
- обеспечение конфиденциальности с помощью алгоритмов DES, IDEA и RC5 — с тремя примерами применения.

1. Алгоритм DES в режиме CBC с секретным ключом, известным получателю. В этом случае необходимый секретный ключ шифруется с помощью ключа шифрования ключей, который совместно используется отправителем и получателем и вызывается по имени. Сжатие данных при этом не применяется. Схема дополнения незначащей информацией — дополнение нулями; она требует дополнительных сведений о числе дополняющих байтов.

2. Алгоритм RC5 в режиме CTS с секретным ключом, известным получателю. В этом случае необходимый секретный ключ шифруется с помощью ключа шифрования ключей, который совместно используется отправителем и получателем и вызывается по имени. Перед шифрованием применяется процедура сжатия ISO 12042.

3. Алгоритм IDEA в режиме CBC с секретным ключом шифрования, обмен которым осуществляется с использованием открытого ключа получателя. Открытый ключ вложен в сертификат. Перед шифрованием применяются процедура сжатия Z-lib и защита целостности с помощью алгоритма CRC-32.

- Хотя отправитель и получатель совместно используют общие ключи, сами криптографические механизмы заранее не согласовываются. Поэтому все применяемые алгоритмы и режим работы имеют явные имена.
- В таблице показаны только те поля защиты, которые имеют отношение к реально используемым методам обеспечения безопасности, алгоритмам и режимам функционирования.
- Сегмент USC содержит в явном виде индикатор хеш-функции и функции цифровой подписи, используемой сертификационным органом для подписания сертификата. Открытый ключ сертификационного органа, требующийся для проверки подписи в сертификате, уже известен получателю. Этот ключ вызывается по имени, указанному в сегменте USC.

Таблица С.1 — Матрица связей

МЕТКА	Наименование	S	R	Конфиденциальность — пример 1	Конфиденциальность — пример 2	Конфиденциальность — пример 3	Примеч.
SG 1		C	99	один на службу защиты			1
USH	ЗАГОЛОВОК СИСТЕМЫ БЕЗОПАСНОСТИ	M	1				
0501	КОД СЛУЖБЫ ЗАЩИТЫ	M	1	4	4	4	

Продолжение таблицы С.1

МЕТКА	Наименование	S	R	Конфиденциальность — пример 1	Конфиденциальность — пример 2	Конфиденциальность — пример 3	Примеч.
0534	ССЫЛОЧНЫЙ НОМЕР ЗАЩИТЫ	M	1	a123	1	ABC99	
S500	УТОЧНЕНИЕ ИДЕНТИФИКАТОРА ЗАЩИТЫ	C	2	(отправитель)			
0577	Спецификатор стороны защиты	M		1	1	1	
0511	Спецификатор стороны защиты	C		идентификатор отправителя	идентификатор отправителя	идентификатор отправителя	
S500	УТОЧНЕНИЕ ИДЕНТИФИКАТОРА ЗАЩИТЫ	C	2	(получатель)			
0577	Спецификатор стороны защиты	M		2	2	2	
0511	Идентификатор стороны защиты	C		идентификатор получателя	идентификатор получателя	идентификатор получателя	
USA	АЛГОРИТМ ЗАЩИТЫ	C	3	(алгоритм шифрования)			
S502	АЛГОРИТМ ЗАЩИТЫ	M	1				
0523	Код области применения алгоритма	M		5	5	5	
0525	Код секретного режима работы	C		2	36	2	
0527	Код алгоритма	C		1	29	4	
0591	Код механизма дополнения незначащей информацией	C		1	2	4	2
S503	ПАРАМЕТР АЛГОРИТМА	C	9	один на секретный ключ			
0531	Спецификатор параметра алгоритма	M		5	5	6	
0554	Значение параметра алгоритма	M		ключ	ключ	ключ	
S503	ПАРАМЕТР АЛГОРИТМА	C	9	один для конкретного имени ключа шифрования ключей			
0531	Спецификатор параметра алгоритма	M		10	10	—	
0554	Значение параметра алгоритма	M		номер ключа	номер ключа	—	
USA	АЛГОРИТМ ЗАЩИТЫ	C	3	(алгоритм сжатия)			
S502	АЛГОРИТМ ЗАЩИТЫ	M	1				
0523	Код области применения алгоритма	M		—	8	8	
0525	Код секретного режима работы	C		—	—	—	

Продолжение таблицы С.1

МЕТКА	Наименование	S	R	Конфиденциальность — пример 1	Конфиденциальность — пример 2	Конфиденциальность — пример 3	Примеч.
0527	Код алгоритма	C		—	27	18	
USA	АЛГОРИТМ ЗАЩИТЫ	C	3	(алгоритм обеспечения целостности сжатых данных)			
S502	АЛГОРИТМ ЗАЩИТЫ	M	1				
0523	Код области применения алгоритма	M		—	—	9	
0525	Код секретного режима работы	C		—	—	—	
0527	Код алгоритма	C		—	—	25	
SG 2		C	2	только один: сертификат получателя			
USC	СЕРТИФИКАТ	M	1				
S500	УТОЧНЕНИЕ ИДЕНТИФИКАТОРА ЗАЩИТЫ	C	2	(владелец сертификата)			
0577	Спецификатор стороны защиты	M		—	—	3	
0511	Идентификатор стороны защиты	C		—	—	идентификатор владельца	
S500	УТОЧНЕНИЕ ИДЕНТИФИКАТОРА ЗАЩИТЫ	C	2	(сторона аутентификации)			
0577	Спецификатор стороны защиты	M		—	—	4	
0538	Наименование ключа	C		—	—	(имя PK/CA)	
0511	Идентификатор стороны защиты	C		—	—	идентификатор CA	
USA	АЛГОРИТМ ЗАЩИТЫ	C	3	(хеш-функция CA для подписи в сертификате)			
S502	АЛГОРИТМ ЗАЩИТЫ	M	1				
0523	Код области применения алгоритма	M		—	—	4	
0525	Код секретного режима работы	C		—	—	—	
0527	Код алгоритма	C		—	—	14	
USA	АЛГОРИТМ ЗАЩИТЫ	C	3	(функция цифровой подписи CA для подписания сертификата)			
S502	АЛГОРИТМ ЗАЩИТЫ	M	1				
0523	Код области применения алгоритма	M		—	—	3	
0525	Код секретного режима работы	C		—	—	16	
0527	Код алгоритма	C		—	—	10	
S503	ПАРАМЕТР АЛГОРИТМА	C	9	(модуль открытого ключа CA)			

Продолжение таблицы С.1

МЕТКА	Наименование	S	R	Конфиденциальность — пример 1	Конфиденциальность — пример 2	Конфиденциальность — пример 3	Примеч.
0531	Спецификатор параметра алгоритма	M		—	—	12	
0554	Значение параметра алгоритма	M		—	—	Mod	
S503	ПАРАМЕТР АЛГОРИТМА	C	9	(экспонента открытого ключа CA)			
0531	Спецификатор параметра алгоритма	M		—	—	13	
0554	Значение параметра алгоритма	M		—	—	Exp	
S503	ПАРАМЕТР АЛГОРИТМА	C	9	(длина модуля открытого ключа CA)			
0531	Спецификатор параметра алгоритма	M		—	—	14	
0554	Значение параметра алгоритма	M		—	—	Mod-L	
USA	АЛГОРИТМ ЗАЩИТЫ	C	3	(функция шифрования для владельца сертификата)			
S502	АЛГОРИТМ ЗАЩИТЫ	M	1				
0523	Код области применения алгоритма	M		—	—	5	
0525	Код области применения алгоритма	C		—	—	—	
0527	Код алгоритма	C		—	—	10	
S503	ПАРАМЕТР АЛГОРИТМА	C	9	(модуль открытого ключа владельца)			
0531	Спецификатор параметра алгоритма	M		—	—	12	
0554	Значение параметра алгоритма	M		—	—	Mod	
S503	ПАРАМЕТР АЛГОРИТМА	C	9	(экспонента открытого ключа владельца)			
0531	Спецификатор параметра алгоритма	M		—	—	13	
0554	Значение параметра алгоритма	M		—	—	Exp	
S503	ПАРАМЕТР АЛГОРИТМА	C	9	(длина модуля открытого ключа владельца)			
0531	Спецификатор параметра алгоритма	M		—	—	14	
0554	Значение параметра алгоритма	M		—	—	Mod-L	
USR	РЕЗУЛЬТАТ ЗАЩИТЫ	C	1				
S508	РЕЗУЛЬТАТ КОНТРОЛЯ	M	2				

Окончание таблицы С.1

МЕТКА	Наименование	S	R	Конфиденциальность — пример 1	Конфиденциальность — пример 2	Конфиденциальность — пример 3	Примеч.
0563	Спецификатор контроля значения	M		—	—	1	
0560	Контрольное значение	C		—	—	CA-Sig	
USD	ЗАГОЛОВОК ШИФРОГРАММЫ	M	1				
0556	ДЛИНА ДАННЫХ, ИЗМЕРЯЕМАЯ ЧИСЛОМ ОКТЕТОВ	M	1	Len	Len	Len	
0518	ССЫЛОЧНЫЙ НОМЕР ШИФРОГРАММЫ	C	1	—	A	—	
0582	ЧИСЛО ДОПОЛНЯЮЩИХ БАЙТОВ	C	1	3	—	—	3
Защищаемые структуры данных (тело сообщения, объект, группы сообщений/пакетов)							
USU	КОНЦЕВИК ШИФРОГРАММЫ	M	1				
0556	ДЛИНА ДАННЫХ, ИЗМЕРЯЕМАЯ ЧИСЛОМ ОКТЕТОВ	M	1				
0518	ССЫЛОЧНЫЙ НОМЕР ШИФРОГРАММЫ	C	1	—	A	—	
SG n		C	99	один для одной службы защиты			1
UST	КОНЦЕВИК ЗАЩИТЫ	M	1				
0534	ССЫЛОЧНЫЙ НОМЕР ЗАЩИТЫ	M		a123	1	ABC99	
0588	ЧИСЛО ЗАЩИТНЫХ СЕГМЕНТОВ	M	1	5	6	12	

Примечания:
1 — Обе структуры должны иметь одинаковое число вхождений.
2 — Дополнение незначащей информацией применимо только к сегменту USA, определяющему алгоритм шифрования.
3 — Число дополняющих байтов приведено для примера.

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов национальным стандартам Российской Федерации

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
ISO 9735-1	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»
ISO 9735-2	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»
ISO 9735-5	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 безопасности для пакетного EDI (подлинность, целостность и невозможность отказа отправителя от авторства сообщения)»
ISO 9735-10	IDT	*
ISO/IEC 10181-5	-	*

* Соответствующий национальный стандарт отсутствует. До его принятия рекомендуется использовать перевод на русский язык данного международного стандарта.

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

- IDT — идентичные стандарты.

Библиография

[1] ISO 639 (all parts), Code for the representation of names of langua (Коды для представления названий языков (все части ISO 639)

[2] ISO/IEC 646, Information technology; ISO 7-bit coded character set for information interchange (Информационные технологии. 7-битный набор кодированных символов ISO для обмена информацией)

[3] ISO/IEC 2022, Information technology — Character code structure and extension techniques (Информационные технологии. Структура кода символов и методы расширения)

[4] ISO/IEC 2375, Information technology — Procedure for registration of escape sequences and coded character sets (Информационные технологии. Процедура регистрации управляющей последовательности и наборов кодированных знаков)

[5] ISO/IEC 6523 (all parts), Information technology — Structure for the identification of organizations and organization parts (Информационные технологии. Структура идентификации организаций и их подразделений (все части ISO/IEC 6523)

[6] ISO 8372[1)], Information processing; Modes of operation for a 64-bit block cipher algorithm (Обработка информации. Режимы работы алгоритма 64-битового блочного шифрования)

[7] ISO 8601, Data elements and interchange formats; information interchange; representation of dates and times (Элементы данных и форматы информационного обмена. Обмен информацией. Представление дат и времени)

[8] ISO 8731-1[2)], Banking; Approved algorithms for message authentication; Part 1: DEA (Банковское дело. Утвержденные алгоритмы для аутентификации сообщений. Часть 1. Алгоритмы кодирования данных (DEA)

[9] ISO 8731-2[3)], Banking; approved algorithms for message authentication; Part 2: message authenticator algorithm (Банковское дело. Утвержденные алгоритмы для аутентификации сообщений. Часть 2. Алгоритм аутентификации сообщений)

[10] ISO/IEC 8859 (all parts), Information technology — 8-bit single-byte coded graphic character sets (Информационные технологии. 8-битные однобайтовые наборы кодированных графических знаков (все части ISO/IEC 8859)

[11] ISO/IEC 9594-8, Information technology. Open Systems Interconnection. The Directory. Part 8: Public-key and attribute certificate frameworks (Информационные технологии. Взаимосвязь открытых систем. Директория. Часть 8. Системы сертификатов открытого ключа и атрибутов)

[12] ISO 9735:1988, Electronic data interchange for administration, commerce and transport (EDIFACT); application level syntax rules (Электронный обмен данными в управлении, торговле и на транспорте (EDIFACT). Синтаксические правила для прикладного уровня)

[13] ISO 9735:1988/Amd 1:1992, Electronic data interchange for administration, commerce and transport (EDIFACT); application level syntax rules; amendment 1 (Электронный обмен данными в управлении, торговле и на транспорте (EDIFACT). Синтаксические правила для прикладного уровня. Изменение 1)

[14] ISO 9735 (all parts):1998[1)], Electronic data interchange for administration, commerce and transport (EDIFACT); application level syntax rules (Электронный обмен данными в управлении, торговле и на транспорте (EDIFACT). Синтаксические правила для прикладного уровня (версия 4) (все части ISO 9735)

[15] ISO/IEC 9796 (all parts), Information technology — Security techniques — Digital signature schemes giving message recovery (Информационные технологии. Методы защиты. Схемы цифровой подписи, обеспечивающие восстановление сообщений (все части ISO/IEC 9796)

[16] ISO/IEC 9797, Information technology; security techniques; data integrity mechanism using a cryptographic check function employing a block cipher algorithm (Информационные технологии. Методы защиты. Коды аутентификации сообщений (MAC)

[17] ISO/IEC 10116, Information technology; modes of operation for an n-bit block cipher algorithm (Информационные технологии. Методы защиты. Режимы работы для n-битовых блочных шифров)

[18] ISO/IEC 10118-1, Information technology — Security techniques — Hash-functions — Part 1. General (Информационные технологии. Методы защиты. Хэш-функции. Часть 1. Общие положения)

[19] ISO/IEC 10118-3, Information technology — Security techniques — Hash-functions — Part 3: Dedicated hash-functions (Информационные технологии. Методы защиты. Хэш-функции. Часть 3: Специализированные хэш-функции)

[20] ISO 10126-1[2)], Banking; procedures for message encipherment (wholesale); Part 1. general principles (Банковское дело. Процедуры кодирования сообщений (оптовая торговля). Часть 1. Общие принципы)

[1)] Изъят из обращения.

[2)] Изъят из обращения.

[3)] Изъят из обращения.

[21] ISO/IEC 10646, Information technology — Universal Coded Character Set (UCS) (Информационные технологии. Универсальный набор кодированных знаков (UCS)

[22] ISO 11166-2[1)], Banking — Key management by means of asymmetric algorithms — Part 2: Approved algorithms using RSA cryptosystem (Банковское дело. Управление ключами с помощью асимметричных алгоритмов. Часть 2. Утвержденные алгоритмы с использованием криптосистемы RSA)

[23] ISO/IEC 12042, Information technology; data compression for information interchange; binary arithmetic coding algorithm (Информационные технологии. Уплотнение данных для обмена информацией. Алгоритм двоичного арифметического кодирования)

[1)] Изъят из обращения.

УДК 658:562.014:006.354 ОКС 35.240.60

Ключевые слова: атрибут, сертификат, кодовый список, справочник составных элементов, управляющий знак, криптография, дешифрация

Редактор *Я.В. Кожаринова*
Технический редактор *В.Н. Прусакова*
Корректор *Л.С. Лысенко*
Компьютерная верстка *А.А. Ворониной*

Сдано в набор 14.12.2016. Подписано в печать 23.12.2016. Формат 60×84 1/8. Гарнитура Ариал.
Усл. печ. л. 3,26. Уч.-изд. л. 3,03. Тираж 25 экз. Зак. 3278

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Издано и отпечатано во ФГУП «СТАНДАРТИНФОРМ», 123995 Москва, Гранатный пер., 4.
gost.e-ecolog.ru stinfo.ru

gost.e-ecolog.ru