ГОСТ Р ИСО/МЭК МФС 10611-1—95

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ

ФУНКЦИОНАЛЬНЫЙ СТАНДАРТ

ПРОФИЛИ АМН1n. СИСТЕМЫ ОБРАБОТКИ СООБЩЕНИЙ. УНИФИЦИРОВАННЫЙ ОБМЕН СООБЩЕНИЯМИ

ЧАСТЬ 1. ОБЕСПЕЧЕНИЕ УСЛУГ СИСТЕМ ОБРАБОТКИ СООБЩЕНИЙ

Издание официальное

БЗ 7—94/318

ГОССТАНДАРТ РОССИИ
Москва

gost.e-ecolog.ru

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ

ФУНКЦИОНАЛЬНЫЙ СТАНДАРТ

ПРОФИЛИ AMH1n. СИСТЕМЫ ОБРАБОТКИ СООБЩЕНИЙ. УНИФИЦИРОВАННЫЙ ОБМЕН СООБЩЕНИЯМИ

ЧАСТЬ 1. ОБЕСПЕЧЕНИЕ УСЛУГ СИСТЕМ ОБРАБОТКИ СООБЩЕНИЙ

Издание официальное

ГОССТАНДАРТ РОССИИ
Москва

Предисловие

1 РАЗРАБОТАН Комитетом при Президенте Российской Федерации по политике информатизации и ВНЕСЕН НА УТВЕРЖДЕНИЕ Техническим комитетом по стандартизации ТК 22 «Информационная технология»

2 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Постановлением Госстандарта России от 24.10.95 № 549

Настоящий стандарт содержит полный аутентичный текст международного стандарта ИСО/МЭК МФС 10611-1—94 «Информационная технология. Международный функциональный стандарт. Профили AMH1n. Системы обработки сообщений. Унифицированный обмен сообщениями. Часть 1. Обеспечение услуг систем обработки сообщений»

3 ВВЕДЕН ВПЕРВЫЕ

© ИПК Издательство стандартов, 1996

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Госстандарта России

Содержание

Введение IV
1 Область применения 1
2 Нормативные ссылки 2
3 Определения 4
4 Сокращения 6
5 Соответствие 7
6 Базовые требования 8
7 Функциональные группы 9
8 Присвоение имен и адресация 22
9 Обработка ошибок и особых случаев 24
Приложение A Элементы услуг 25
Приложение B Изменения и технические поправки 34
Приложение C Защита обмена сообщениями — реализация и логическое обоснование 35
Приложение D Дополнительные рекомендации по обеспечению межсетевого обмена 1984 45
Приложение E Общие сведения о назначении и применимости профилей AMH1 48

Введение

Настоящий стандарт определен как функциональный стандарт в соответствии с принципами, установленными ГОСТ Р ИСО/МЭК ТО 10000-1. Функциональная стандартизация — это одна из частей общей сферы деятельности в области информационной технологии (ИТ), охватывающей базовые стандарты, профили и механизмы регистрации. Профиль представляет собой комбинацию базовых стандартов, которые в совокупности выполняют конкретную функцию ИТ. Профили стандартизуют использование факультативных возможностей и других вариантов в базовых стандартах и создают основу для разработки унифицированных международно признанных системных тестов.

Одна из наиболее важных задач международного функционального стандарта (МФС) заключается в том, чтобы быть основой разработки (организациями, кроме ИСО и МЭК) международно признанных тестов и центров тестирования. МФС разрабатывают не просто для «узаконивания» конкретного набора базовых стандартов и факультативных возможностей, но и для того, чтобы способствовать взаимодействию открытых систем. Разработка широко приемлемых тестов, основанных на настоящем и других МФС, очень важна для успешного достижения этой цели.

ГОСТ Р ИСО/МЭК МФС 10611 состоит из нескольких частей. Настоящий стандарт является первой частью. В ней определено обеспечение услуг системы обработки сообщений. Во второй части определены требования к сервисным элементам удаленных операций, надежной передачи, управления ассоциацией (СЭУО, СЭНП, СЭУА) и протоколам уровня представления и сеансового уровня для использования системами обработки сообщений. В третьей части определен профиль АМН11(Р1), в четвертой части — профиль АМН12(Р3) и в пятой части — профиль АМН13(Р7).

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационная технология
Функциональный стандарт

ПРОФИЛИ AMH1n. СИСТЕМЫ ОБРАБОТКИ СООБЩЕНИЙ. УНИФИЦИРОВАННЫЙ ОБМЕН СООБЩЕНИЯМИ

Часть 1. Обеспечение услуг систем обработки сообщений

Information technology. International standardized profiles AMH1n. Message handling systems.
Common messaging.
Part 1. MHS service support

Дата введения 1996—07—01

1 ОБЛАСТЬ ПРИМЕНЕНИЯ

1.1 Общие положения

Настоящий стандарт содержит общие требования к обеспечению элементов услуг системы обработки сообщений (СОС) и устанавливает соответствующие функциональные возможности, которые обычно несвойственно обсуждать исключительно из-за простого вида протокола СОС. Эти требования составляют часть прикладных функций унифицированного обмена сообщениями, как определено в настоящем функциональном стандарте (ФС), который формирует общую основу для содержимого типозависимых ФС на СОС, планируемых к разработке. Такие требования во многих случаях применимы более чем к одному протоколу СОС или могут быть отнесены к функциональным возможностям компонента, который, несмотря на то, что может быть проверен через протокол, как раз не относится к обеспечению протокола. На них, следовательно, должны быть даны ссылки в прикладных профилях унифицированного обмена сообщениями СОС, стандартизованных в частях 3—5 настоящего ФС, которые устанавливают конкретные протоколы СОС и соответствующие функциональные возможности.

Издание официальное

Требования в настоящем стандарте охватывают положения о функциональных возможностях, относящихся к услугам передачи сообщений (как определено в разделе 8 ИСО/МЭК 10021-1), и об использовании этих возможностей наряду с возможностями, относящимися к взаимодействию с услугами физической доставки (УФД) (как определено в разделе 10 ИСО/МЭК 10021-1). Рассмотрены также функциональные возможности, относящиеся к хранилищам сообщений (ХС) и агенту пользователя (АП), которые охватывают типонезависимое содержимое. Функциональные возможности, специфичные для конкретного типа содержимого (включая обеспечение услуг агентом пользователя, для пользователя СОС), предусматриваются в отдельных ФС по профилям типозависимого содержимого.

Требования в настоящем стандарте делятся на базовые требования, которые должны обеспечиваться всеми реализациями СОС, и на множество факультативных функциональных групп, которые охватывают существенные области дискретных значений соответствующих функциональных возможностей, которые не обязательно должны обеспечиваться всеми реализациями.

В приложении Е приведены общие сведения о назначении и применимости набора профилей AMH1n, а также сведения о структуре ГОСТ Р ИСО/МЭК МФС 10611.

1.2 Место в таксономии

Настоящая часть ГОСТ Р ИСО/МЭК МФС 10611 является первой частью ФС, идентифицированного в ГОСТ Р ИСО/МЭК ТО 10000-2 как «AMH1. Системы обработки сообщений. Унифицированный обмен данными» (см. также ГОСТ Р ИСО/МЭК ТО 10000-1, подраздел 8.2, в котором определены многочастевые ФС).

Настоящая часть ГОСТ Р ИСО/МЭК МФС 10611 сама по себе не определяет каких-либо профилей.

2 НОРМАТИВНЫЕ ССЫЛКИ

Изменения и технические поправки в базовых стандартах, на которые сделаны ссылки, перечислены в приложении В.

Примечание — Ссылки в основной части настоящего стандарта на конкретные разделы стандартов ИСО/МЭК следует рассматривать как ссылки на соответствующие разделы эквивалентных рекомендаций МККТТ (указанных ниже), если не оговорено иное.

В настоящем стандарте использованы ссылки на следующие стандарты:

ГОСТ Р ИСО/МЭК 8824—93 Системы обработки информации. Взаимосвязь открытых систем. Спецификация абстрактной синтаксической нотации один (АСН.1)

ГОСТ Р ИСО/МЭК ТО 10000-1—93 Информационная технология. Основы и таксономия функциональных профилей. Часть 1. Основы

ГОСТ Р ИСО/МЭК ТО 10000-2—93 Информационная технология. Основы и таксономия функциональных профилей. Часть 2. Таксономия профилей

ГОСТ Р ИСО/МЭК МФС 10611-3—95 Информационная технология. Функциональный стандарт. Профили АМН1п. Системы обработки сообщений. Унифицированный обмен сообщениями. Часть 3. Профиль АМН11. Передача сообщений (с использованием протокола Р1)

ИСО 7498-2—90[1] Системы обработки информации. Взаимосвязь открытых систем. Часть 2. Архитектура защиты информации

ИСО/МЭК 9594-8—90[1] Информационная технология. Справочник. Часть 8. Основы аутентификации [См. также Рекомендацию X.509 МККТТ (1988)]

ИСО/МЭК 10021-1—90[1] Информационная технология. Передача текста. Системы обмена текстами, ориентированные на сообщения. Часть 1. Общее описание услуг [См. также Рекомендацию X.400 МККТТ (1988)]

ИСО/МЭК 10021-2—90[1] Информационная технология. Передача текста. Системы обмена текстами, ориентированные на сообщения. Часть 2. Общая архитектура [См. также Рекомендацию X.402 МККТТ (1988)]

ИСО/МЭК 10021-4—90[1] Информационная технология. Передача текста. Системы передачи текста, ориентированные на сообщения. Часть 4. Система передачи сообщений. Определение абстрактных услуг и процедуры [См. также Рекомендацию X.411 МККТТ (1988)]

---

[1] До прямого применения данного документа в качестве государственного стандарта распространение его осуществляет секретариат ТК 22 «Информационная технология».

ИСО/МЭК 10021-5—90[1] Информационная технология. Передача текста. Системы передачи текста, ориентированные на сообщения. Часть 5. Хранилище сообщений. Определение абстрактных услуг [См. также Рекомендацию X.413 МККТТ (1988)]

ИСО/МЭК 10021-6—90[1] Информационная технология. Передача текста. Системы передачи текста, ориентированные на сообщения. Часть 6. Спецификации протокола [См. также Рекомендацию X 419 МККТТ (1988)]

Рекомендация X.400 МККТТ (1988) Общее описание системы и службы обработки сообщений

Рекомендация X.402 МККТТ (1988) Системы обработки сообщений. Общая архитектура

Рекомендация X.411 МККТТ (1988) Системы обработки сообщений. Система передачи данных. Определение абстрактных услуг и процедуры

Рекомендация X.413 МККТТ (1988) Системы обработки сообщений. Хранилище сообщений. Определение абстрактных услуг

Рекомендация X.509 МККТТ (1988) Справочник. Основы аутентификации

Руководство для разработчика СОС, версия 8, март 1992 (Специальная согласительная группа МККТТ по системам обработки сообщений и СРГ по обмену сообщениями ИСО/МЭК СТК1/ПК18/РГ4)

3 ОПРЕДЕЛЕНИЯ

В настоящем стандарте использованы приведенные ниже определения.

В настоящем стандарте использованы термины, определенные в базовых стандартах, на которые сделаны ссылки. Дополнительно определены термины, приведенные ниже.

3.1 Общие понятия

Базовое требование — элемент услуг, элемент протокола, элемент процедуры или любая другая идентифицируемая характеристика, определенная в базовых стандартах, которые должны обеспечиваться всеми реализациями СОС.

---

[1] До прямого применения данного документа в качестве государственного стандарта распространение его осуществляет секретариат ТК 22 «Информационная технология».

Функциональная группа — один или несколько элементов услуг, элементов протокола, элементов процедуры или других идентифицируемых характеристик, определенных в базовых стандартах, которые в совокупности определяют важную область факультативных возможностей СОС.

Примечание — Функциональная группа может охватывать любую комбинацию характеристик СОС, определенных в базовых стандартах, для которой результат реализации может быть определен как стандартизованный внешний интерфейс, т.е. через стандартный протокол обмена данными ВОС (другие виды упомянутого интерфейса, такие как стандартный программный интерфейс, не входят в предмет рассмотрения данной версии настоящего ФС).

3.2 Классификация видов обеспечения

Степень обеспечения элементов услуг в настоящем стандарте определяют приведенные ниже термины.

Обязательное обеспечение (О):

при отправке: поставщик услуг должен быть способен обеспечить элемент услуг доступным для пользователя услуг в роли отправителя: пользователь услуг должен быть способен использовать элемент услуг в роли отправителя;

при обработке: поставщик услуг должен реализовать все процедуры, определенные в базовых стандартах, которые относятся к обеспечению элемента услуг (т.е. способны обеспечить полные возможности элемента услуг);

при получении: поставщик услуг должен быть способен обеспечить элемент услуг доступным для пользователя услуг в роли получателя; пользователь услуг должен быть способен использовать элемент услуг в роли получателя;

факультативное обеспечение (Ф): реализация не обязательно должна обеспечивать данный элемент услуг. Если обеспечение заявлено, данный элемент услуг должен рассматриваться так, как если бы для него было определено обязательное обеспечение;

условное обеспечение (У): элемент услуг должен быть обеспечен при некоторых условиях, определенных в настоящем стандарте. Если эти условия удовлетворяются, то элемент услуг должен рассматриваться так, как если бы для него было определено обязательное обеспечение. Если условия не удовлетворяются, то элемент услуг должен рассматриваться так, как если бы для него было определено факультативное обеспечение (если не указано иное).

не входит в предмет рассмотрения (Н/Р): элемент услуг не входит в предмет рассмотрения настоящего стандарта, т.е. он не может быть объектом тестирования на соответствие международному функциональному стандарту. Тем не менее, обработка соответствующих элементов протокола может быть определена в последующих частях настоящего ФС;

не используется (—): элемент услуг не применяется в конкретном контексте, в котором используется эта классификация.

3.3 Объектные идентификаторы профилей

В таблице 1 приведены объектные идентификаторы профилей, которые определены в ГОСТ Р ИСО/МЭК МФС 10611.

Примечание — Данные объектные идентификаторы введены для формальных целей и любое их использование не определяется. Они не имеют отношений к каким-либо реализациям систем обработки сообщений и не встречаются в протоколах, определенных в настоящем ФС.

Таблица 1 — Объектные идентификаторы профилей

Профиль	Объектный идентификатор
AMH111	{iso(1)standard(0)common-messaging(10611)message-transfer(3)normal-mode(1)}
AMH112	{iso(1)standard(0)common-messaging(10611)message-transfer(3)×410-mode(2)}
AMH12	{iso(1)standard(0)common-messaging(10611)mts-access(4)}
AMH13	{iso(1)standard(0)common-messaging(10611)mts-access(4)}

4 СОКРАЩЕНИЯ

ОМО84 — обеспечение межсетевого обмена 84;
ОСПУ — обработка сообщений прикладного уровня;
АСН.1 — абстрактная синтаксическая нотация один;
ЗК — защита компьютера;
ЗС — защита связи;
ЗСРП — заявка о соответствии реализации протоколу;
ПР — преобразование;
ИС — использование справочника;
СР — список распределения;
АССк — агент систем справочника;
АПСк — агент пользователя справочника;
ЭУ — элемент услуг;
ФГ — функциональная группа;

ФС — функциональный стандарт;
СПД — самая последняя доставка;
СОС — системы обработки сообщений;
МУЗ — многоуровневая защита;
ХС — хранилище сообщений;
ПС — передача сообщений;
АПС — агент передачи сообщений;
СПС — система передачи сообщений;
ВОС — взаимосвязь открытых систем;
ФД — физическая доставка;
МДФД — модуль доступа физической доставки;
ПА — переадресация;
ВС — возврат содержимого;
ЗЩ — защита;
АП — агент пользователя.

Уровень обеспечения элементов услуг (см. 3.2):

О — обязательное обеспечение;
Ф — факультативное обеспечение;
У — условное обеспечение;
Н/Р — не входит в предмет рассмотрения;
— — не используется.

5 СООТВЕТСТВИЕ

Требования соответствия не определены в этой части настоящего ФС.

Примечание — Настоящая часть ФС представляет собой ссылки на базовые требования и функциональные группы, охватываемые набором профилей AMH1n, и дополнительные специфичные для протоколов требования, определяемые в последующих частях настоящего ФС. Хотя настоящая часть ФС содержит обязательные требования, однако требований к соответствию настоящей части нет (т.е. они не идентифицированы в таксономии СОС в ГОСТ Р ИСО/МЭК ТО 10000-2), поскольку такие требования существенны только тогда, когда на них ссылаются в контексте конкретного протокола.

Требования соответствия определяются протоколом для каждого компонента СОС в последующих частях настоящего ФС со ссылкой на требования настоящей части ФС. Обеспечение функциональных возможностей, как определено в настоящем стандарте, может быть верифицировано только в том случае, когда действия реализации могут быть определены на стандартном внешнем интерфейсе, т.е. через стандартный протокол обмена данными ВОС. Кроме того,

обеспечение элементов услуг и других функциональных возможностей на интерфейсе услуг не обязательно должно быть верифицируемо, если только такой интерфейс не реализован в форме стандартного протокола обмена данными ВОС. Могут быть обеспечены и другие формы упомянутого интерфейса (такие, как пользовательский интерфейс человека-оператора или стандартный программный интерфейс), однако они не требуются для оценки соответствия этой версии настоящего ФС.

6 БАЗОВЫЕ ТРЕБОВАНИЯ

В приложении А определены базовые требования к обеспечению элементов услуг (ЭУ) для соответствия настоящему стандарту. Базовые требования определяют уровень обеспечения, требуемый всеми реализациями СОС, как свойственно каждому типу компонента СОС, т.е. АПС, ХС или АП (выполняющим роль пользователя АПС или пользователя ХС в зависимости от ситуации).

Примечание — Настоящий стандарт определяет только обеспечение услуг агентом передачи сообщения и хранилищем сообщения и использование таких услуг пользователем СПС и пользователем ХС. Стандарт не определяет обеспечение таких услуг агентами пользователей СОС, которые определяются в профилях, специфичных для типа содержимого.

6.1 Содержимое и типы кодированной информации

В заявке о соответствии реализации протоколу (ЗСРП) должно быть указано, какой тип содержимого и какие значения типа кодированной информации обеспечиваются.

6.2 Длина сообщения

Если реализация налагает любые ограничения на размер содержимого сообщения или конверта, то все такие ограничения должны быть указаны в ЗСРП.

Примечание — Реализаторы советуют избегать ограничений размера сообщений, поскольку это возможно. Например, любое ограничение, которое предотвращает передачу сообщения размером 2 мегаоктета, может быть причиной проблем при взаимодействии с системами 1984. Требования должны меняться с учетом приложения и функциональной среды и могут быть гораздо выше 2 мегаоктетов.

6.3 Количество получателей

В ЗСРП должно быть установлено количество получателей, если имеется ограничение на количество получателей, которое может быть определено в конверте сообщения.

7 ФУНКЦИОНАЛЬНЫЕ ГРУППЫ

В приложении А определены также любые дополнительные требования к обеспечению элементов услуг СОС, если заявлено обеспечение факультативной функциональной группы (ФГ), что свойственно каждому типу компонента СОС. В последующих разделах обобщены функциональные возможности, обеспечиваемые каждой из факультативных ФГ, и идентифицированы все конкретные требования и те положения, относящиеся к реализации, которые не входят в предмет рассмотрения формального соответствия ГОСТ Р ИСО/МЭК МФС 10611. Сводка функциональных групп, идентификация которых может обеспечена (Д), и тех, которые не относятся (Н) к каждому типу компонента СОС (т.е. АПС, ХС или АП независимо от того, выступают ли они в роли пользователя СПС или пользователя ХС), приведена в таблице 2.

Таблица 2 — Сводный перечень факультативных функциональных групп АМН1п

Функциональная группа	АПС	ХС	АП
Преобразование (ПР)	Д	Н	Н[1)]
Список распределения (СР)	Д	Н	Н
Физическая доставка (ФД)	Д	Н	Д
Переадресация (ПА)	Д	Н	Н[1)]
Последняя доставка (ПД)	Д	Н	Д
Возврат содержимого (ВС)	Д	Н	Д
Защита (ЗП)	Д	Д	Д
Использование справочника (ИС)	Д	Н	Д
Обеспечение межсетевого обмена 84 (ОМО84)	Д	Н	Н[1)]

[1)] Функциональные возможности АП могут быть определены дополнительно в профилях типозависимого содержимого

Требования соответствия к обеспечению различных функциональных групп охватывают обеспечение дополнительных элементов протокола и(или) процедур и определены в 3, 4, 5-й частях настоящего ФС соответственно в протоколе(ах), относящихся к каждой функциональной группе.

7.1 Преобразование (ПР)

ФГ «преобразование» охватывает обеспечение тех элементов услуг, которые поддерживают функциональные возможности, необходимые

для выполнения функции преобразования типа кодированной информации. Обеспечение ФГ ПР используется только в АПС.

Примечание — Обеспечение ЭУ, связанное с запрещением преобразования, является базовым требованием, но это не предполагает способности к выполнению преобразования.

Должно обеспечиваться либо явное преобразование, либо неявное преобразование, либо то и другое. Аттестуемая реализация должна удовлетворять правилам, определенным в 14.3.5 и 14.3.9 ИСО/МЭК 10021-4.

Соответствие ГОСТ Р ИСО/МЭК МФС 10611 не требует функциональной возможности выполнения каких-либо конкретных преобразований. В дальнейшем специфические требования могут быть включены в функциональные стандарты типозависимого содержимого для СОС, которые запланированы к разработке или могут быть определены отдельно иным образом.

В ЗСРП должно констатироваться, какой из типов преобразований может выполнить реализация из тех типов преобразования (т.е. явного или неявного), для которых заявлено обеспечение. ЗСРП должна также устанавливать условия, при которых определяется потеря информации (если таковая имеется) для каждого преобразования типа кодированной информации, обеспечение которого заявлено.

Примечание — Не всегда можно проверить обеспечение преобразования при отсутствии дополнительной спецификации, которая связана с одним или несколькими идентифицируемыми типами содержимого.

7.2 Список распределения (СР)

ФГ «список распределения» охватывает все вопросы, относящиеся к расширению списка распределения (СР). Обеспечение ФГ СР относится только к АПС.

Примечание — Другие аспекты, имеющие отношение к использованию СР (например, способность предоставлять сообщение, определяющее получателя, которым является СР), рассматриваются как базовое требование. Точно так же базовым требованием является способность АПС принимать и правильно обрабатывать сообщение, которое отражает расширение предшествующего СР.

Для соответствия ГОСТ Р ИСО/МЭК МФС 10611 не требуется никаких функциональных возможностей административного управления СР, кроме тех, которые определены в 14.3.10 ИСО/МЭК 10021-4. Любые последующие требования могут зависеть от реализации.

7.3 Физическая доставка (ФД)

ФГ «физическая доставка» касается доступа к услугам физической доставки (т.е. почтовая, курьерская связь и т.п.). ФГ ФД охватывает две отдельные и различные части:

- обеспечение ЭУ ФД при предоставлении;
- обеспечение соразмещенного модуля доступа физической доставки (МДФД).

Обеспечение ЭУ ФД при предоставлении используется в АПС и в АП. Если АПС обеспечивает МДФД и также обеспечивает предоставление сообщения, он должен обеспечивать и ЭУ ФД при предоставлении.

Обеспечение ФГ ФД также требует обеспечения соответствующих атрибутов расширения адресов отправителя/получателя (О/П).

Если МДФД генерирует какую-либо ошибку в экспорте, АПС должен генерировать отчет о недоставке или реагировать другим соответствующим действием (например, обработкой альтернативного получателя). Все другие виды обработки, касающиеся фактического физического изображения и доставки сообщения, не входят в предмет рассмотрения ГОСТ Р ИСО/МЭК МФС 10611.

7.4 Переадресация (ПА)

ФГ «переадресация» охватывает обеспечение тех ЭУ, которые обеспечивают функциональные возможности, необходимые для выполнения действий, связанных с доставкой сообщения к получателю, отличных от действий, первоначально определенных отправителем. Обеспечение ФГ ПА относится только к АПС.

Примечание — Обеспечение ЭУ, связанного с запретом переадресации, является базовым требованием, но это не предполагает возможности выполнения переадресации. Точно так же обеспечение ЭУ «разрешается альтернативный получатель» является базовым требованием, но это не означает возможности назначения альтернативного получателя.

Аттестуемая реализация должна удовлетворять правилам, определенным в 14.3 ИСО/МЭК 10021-4.

Средства, которыми достигается ЭУ «назначение альтернативного получателя», не входят в предмет рассмотрения ГОСТ Р ИСО/МЭК МФС 10611.

7.5 Последняя доставка (ПД)

ФГ «последняя доставка» охватывает обеспечение ЭУ «последняя доставка», т.е. функциональные возможности, необходимые по причине случившейся недоставки, если время последней доставки,

определенное отправителем, истекло. Обеспечение ФГ ПД относится к АПС или АП. Если АПС обеспечивает ФГ ПД и также обеспечивает предоставление сообщения, он должен обеспечивать и предоставление ЭУ ПД.

Примечание — Указание последней доставки гарантируется только в том случае, если она обеспечивается, по крайней мере, доставляющим АПС.

7.6 Возврат содержимого (ВС)

ФГ «возврат содержимого» охватывает обеспечение ЭУ «возврат содержимого», т.е. функциональные возможности, необходимые по причине возвращения содержимого предоставленного сообщения с любым уведомлением о недоставке, если так требует отправитель. Обеспечение ФГ ВС относится к АПС или АП. Если АПС обеспечивает ФГ ВС и также обеспечивает предоставление сообщения, он должен обеспечивать и предоставление ЭУ ВС.

Примечание — Возврат содержимого гарантируется только в том случае, если он обеспечивается всеми АПС, через которые могло проходить сообщение.

7.7 Защита (ЗЩ)

7.7.1 *Общие понятия*

ФГ «защита» охватывает обеспечение защиты обмена сообщениями и определяет три класса защиты, которые являются нарастающими подмножествами характеристик защиты, установленных в базовых стандартах СОС:

S0. Этот класс защиты требует только те функции защиты, которые используются между пользователями СПС. Следовательно, механизмы защиты реализуются в пределах пользователя СПС. АПС должен обеспечить только синтаксис услуг защиты при предоставлении и доставке (обеспечение синтаксиса при ретрансляции является базовым требованием). Не предполагается, что АПС должен понимать семантику услуг защиты.

S1. Этот класс защиты требует обеспечения функциональных возможностей защиты как пользователем СПС, так и СПС. Функциональные возможности СПС требуются только для обеспечения административного управления защищенным доступом. Как и в случае S0, большинство механизмов защиты реализуется пользователем АПС. S1 обеспечивает в основном целостность информации и аутентификацию пользователей АПС. Однако предполагается, что АПС должен обеспечивать цифровые сигнатуры аутентификации равноправных партнеров, метки защиты и контексты защиты.

S2. Этот класс защиты дополняет функции защиты, выполняемые АПС и СПС. *Основная функция защиты, дополняемая* в этом классе, представляет собой аутентификацию СПС и, следовательно, может быть обеспечена также функция «безотказность».

Помимо этого, каждый из трех классов защиты имеет свой вариант (поименованные соответственно как S0C, S1C и S2C), которые требуют обеспечения сквозной конфиденциальности содержимого.

С каждым классом защиты может быть использован двойной конверт как факультативное расширение, однако эта возможность выходит за рамки соответствия ГОСТ Р ИСО/МЭК МФС 10611 и должна быть предметом двустороннего соглашения.

Обеспечение ФГ ЗЩ относится к АПС, ХС или АП (выполняющим роль либо пользователя СПС, либо пользователя ХС) и требует, как минимум, обеспечения класса защиты S0.

Если не указано иное, могут быть использованы симметричные или асимметричные методы (либо их комбинация) в пределах каждого класса защиты, идентифицированные идентификатором зарегистрированного алгоритма.

С каждым классом защиты могут быть использованы различные степени гарантии в доверительной функциональной возможности ЗК, но этот вопрос не входит в предмет рассмотрения настоящего ФС.

В пределах каждого класса защиты могут быть использованы различные уровни гарантии, возложенные на функциональные возможности, но этот вопрос не входит в предмет рассмотрения настоящего ФС.

Полные логические обоснования для каждого из классов защиты и более подробные сведения о защите приведены в приложении С.

В таблице 3 обобщены требования классов защиты у пользователя СПС и у АПС.

Таблица 3 — Сводное описание классов защиты ЗЩ

Класс защиты	Пользователь СПС	АПС
Базовый		Обеспечение ретрансляции элемента услуг «защита»

Окончание таблицы 3

Класс защиты	Пользователь СПС	АПС
S0	Целостность содержимого Проверка доставки Аутентификация отправителя (сквозная)	Обеспечение предоставления и доставка элемента услуг «защита»
S1	Дополнительно к S0: Присвоение метки защиты сообщения Контекст защиты Административное управление защитой	Дополнительно к S0: Аутентификация равноправных логических объектов Разметка защиты сообщения Контекст защиты Управление защитой
S2	Дополнительно к S1: Проверка подлинности отправителя Проверка предоставления	Дополнительно к S1: Проверка подлинности отправителя Проверка предоставления
SnC	Дополнительно к Sn: Конфиденциальность содержимого	Как Sn

Нарастающие функциональные возможности классов защиты могут быть представлены в виде диаграммы, как показано на рисунке 1.

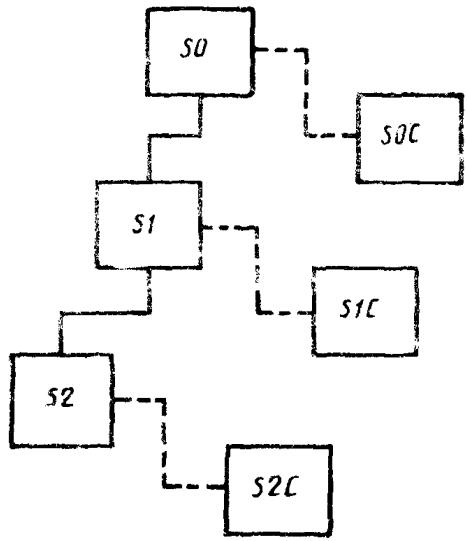

Рисунок 1 — Нарастающие функциональные возможности классов защиты ЗШ

7.7.2 *Защита обеспечения межсетевого обмена*

Обеспечение межсетевого обмена между реализациями, поддерживающими различные классы защиты, может достигаться с точки зрения любого общего используемого класса или классов защиты. Как установлено в базовых стандартах, реализация, которая обеспечивает административное управление защитой доступа, должна проверять метку сообщения, зонд или отчет относительно контекста защиты. При установлении соединения согласование класса защиты не производится.

Действующий класс защиты идентифицируется с использованием идентификатора стратегии защиты, как определено в таблице 4. Такие родовые идентификаторы стратегии защиты подразумевают только обеспечение услуг защиты СОС, как определено для этих классов защиты в настоящем стандарте. При использовании таких идентификаторов стратегии защиты не предполагается никаких других функциональных возможностей ЗК или ЗС. Более конкретные стратегии защиты могут быть основаны на одном или нескольких классах защиты, как определено в данном разделе, но для этого может потребоваться использование зарегистрированных идентификаторов стратегий защиты для частной защиты обеспечения межсетевого обмена.

Таблица 4 — Идентификаторы меток защиты

Идентификатор	Значение
ид-защита СОС	{ИСО(1) идентифицированная организация(3) ewos(16) eg(2) coc(4) защита (4)}
ид-идентификатор-стратегии	{ид-защита coc 1}
Идентификаторы-стратегии защиты:	
Класс-защиты S0	{ид-идентификатор-стратегии 00}
Класс-защиты S0C	{ид-идентификатор-стратегии 01}
Класс-защиты S1	{ид-идентификатор-стратегии 10}
Класс-защиты S1C	{ид-идентификатор-стратегии 11}
Класс-защиты S2	{ид-идентификатор-стратегии 20}
Класс-защиты S2C	{ид-идентификатор-стратегии 21}
ид-идентификатор-категории	{ид-защита coc 2}
Категория защиты:	
Частная	{ид-идентификатор-категории 0}
Конфиденциальная	{ид-идентификатор-категории 1}
Коммерческая-конфиденциальность	{ид-идентификатор-категории 2}
Конфиденциальность административного-управления	{ид-идентификатор-категории 3}
Личная-конфиденциальность	{ид-идентификатор-категории 4}

Метка защиты может дополнительно содержать одну или несколько классификаций защиты, категорий защиты и метку собственности. В таблице 3 определен минимальный набор значений для категорий защиты. Опять-таки, дополнительные значения могут быть зарегистрированы для частной защиты обеспечения межсетевого обмена. Тем не менее, во всех случаях точная семантика категорий защиты не входит в предмет рассмотрения настоящего ФС и может потребовать двустороннего соглашения.

Услуга защиты «контекст защиты» гарантирует, что метка защиты соответствует, по крайней мере, одной из набора меток, определенных в контексте защиты, установленной между взаимодействующими объектами. Реализация, которая обеспечивает эту услугу, должна, как минимум, обеспечивать точное соответствие в отношении равенства идентификатора стратегии защиты, классификации защиты и элементов категорий защиты метки.

Примечание — Требования базового обеспечения состоят в том, что отсутствие элемента не должно трактоваться как «любое значение», т.е. все допустимые комбинации событий и значения элементов разметки защиты сообщений должны быть детально проработаны в контексте защиты (см. также приложение С).

7.7.3 *Описание классов защиты*

В последующих таблицах идентифицированы услуги защиты, охватываемые каждым из классов защиты в пределах ФГ ЗЩ. Там, где классификация услуг защиты не меняется для более высоких классов защиты, услуга защиты не повторяется в таблицах для этих старших классов защиты. На рисунке 2 пояснены заголовки колонок, используемые в таблицах 5, 6, 7, 8, которые идентифицируют те компоненты СОС, которые привлечены для обеспечения и использования каждой услуги защиты.

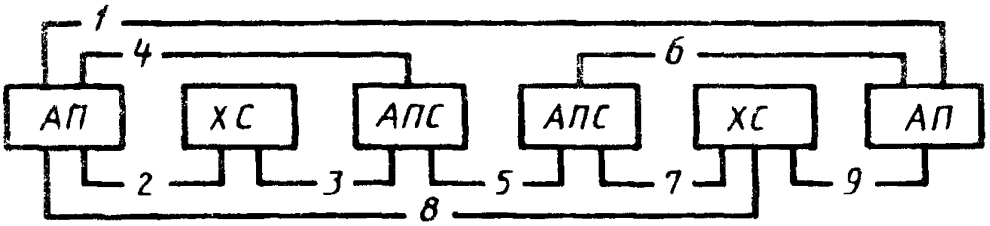

Рисунок 2 — Использование условных обозначений в таблицах классов защиты

7.7.3.1 *Класс защиты S0*

Таблица 5 — Класс защиты S0

Услуга защиты	1	2	3	4	5	6	7	8	9
	АП/АП	АП/ХС	ХС/АПС	АП/АПС	АПС/АПС	АПС/АП	АПС/ХС	АП/ХС	ХС/АП
АУТЕНТИФИКАЦИЯ ОТПРАВИТЕЛЯ									
Аутентификация отправителя сообщения[1)]	О	Н/Р	—	Н/Р	—	—	—	—	—
Аутентификация отправителя зонда	—	Н/Р	—	Н/Р	—	—	—	—	—
Аутентификация отправителя отчета	—	—	—	—	Н/Р	Н/Р	Н/Р	—	—
Подтверждение предоставления	—	—	—	—	—	Н/Р	—	—	—
Подтверждение доставки	О	—	—	—	—	—	—	О[8)]	—
АДМИНИСТРАТИВНОЕ УПРАВЛЕНИЕ ЗАЩИТОЙ ДОСТУПА									
Аутентификация равноправных логических объектов[2), 6)]	—	Ф	Ф	Ф	Ф	Ф	Ф	—	Ф
Контекст защиты	—	Ф	Ф	Ф	Ф	Ф	Ф	—	Ф
КОНФИДЕНЦИАЛЬНОСТЬ ДАННЫХ									
Конфиденциальность соединения	—	Н/Р	Н/Р	Н/Р	Н/Р	Н/Р	Н/Р	—	Н/Р
Конфиденциальность содержимого	Ф	—	—	—	—	—	—	—	—
Конфиденциальность потока сообщений	Н/Р	—	—	—	—	—	—	—	—
ЦЕЛОСТНОСТЬ ДАННЫХ									
Целостность соединения	—	Н/Р	Н/Р	Н/Р	Н/Р	Н/Р	Н/Р	—	Н/Р
Целостность содержимого	О	—	—	—	—	—	—	—	—
Целостность последовательности сообщения[4)]	Ф	—	—	—	—	—	—	—	—

Окончание таблицы 5

Услуга защиты	1	2	3	4	5	6	7	8	9
	АП/ АП	АП/ ХС	ХС/ АПС	АП/ АПС	АПС/ АПС	АПС/ АП	АПС/ ХС	АП/ ХС	ХС/ АП
БЕЗОТКАЗНОСТЬ									
Безотказность отправителя[1), 5)]	Ф	—	—	Н/Р	—	—	—	—	—
Безотказность предоставления	—	—	—	—	—	Н/Р	—	—	—
Безотказность доставки[5)]	Ф	—	—	—	—	—	—	Ф[8)]	—
Разметка защиты сообщения[2), 3)]	Ф	Ф	Ф	Ф	Ф	Ф	Ф	Ф	Ф
АДМИНИСТРАТИВНОЕ УПРАВЛЕНИЕ ЗАЩИТОЙ									
Изменение удостоверения	—	Ф	—	Ф	Н/Р[7)]	Ф	Ф	—	—
Регистр	—	Ф	—	Ф	Н/Р[7)]	—	—	—	—
Регистр ХС	—	Ф	—	—	—	—	—	—	—

[1)] Обеспечивается только для получателя сообщений (с использованием элемента защиты «целостность аргумента сообщения»)

[2)] При использовании либо асимметричного, либо симметричного алгоритма так, как определено идентификатором алгоритма

[3)] При использовании разметки защиты должен быть установлен указатель стратегии защиты

[4)] Расположение и управление порядковыми номерами не входит в предмет рассмотрения настоящего ФС; этот вопрос является предметом двустороннего соглашения

[5)] При использовании или нотариально заверенного сертификата (симметричный алгоритм), или безотказных сертификатов и полномочий (асимметричный алгоритм)

[6)] Аутентификация между соразмещенными объектами является локальным вопросом

[7)] Эти услуги рассчитаны на обеспечение услугами нестандартного административного управления и, следовательно, не входят в предмет рассмотрения настоящего ФС

[8)] «Безотказность доставки» может быть обеспечена только при использовании услуги «подтверждение доставки». Однако, если совместно используются услуги «подтверждение доставки» и «конфиденциальность содержимого», доставка осуществляется в ХС, и подтверждение доставки может быть осуществлено только вычислительными средствами на основании зашифрованного содержимого. Следует отметить, что это не обеспечивает безотказной доставки

7.7.3.2 *Класс защиты S1*

Таблица 6 — Класс защиты S1

Услуга защиты	1	2	3	4	5	6	7	8	9
Как и для S0, плюс:	АП/ АП	АП/ ХС	ХС/ АПС	АП/ АПС	АПС/ АПС	АПС/ АП	АПС/ ХС	АП/ ХС	ХС/ АП
АУТЕНТИФИКАЦИЯ ОТПРАВИТЕЛЯ									
Аутентификация отправителя сообщения[2]	O[1]	Н/Р	—	Н/Р	—	—	—	—	—
АДМИНИСТРАТИВНОЕ УПРАВЛЕНИЕ ЗАЩИТОЙ ДОСТУПА									
Аутентификация равноправных логических объектов[3], [4]	—	O[1]	O[1]	O[1]	O[1]	O[1]	O[1]	—	O[1]
Контекст защиты	—	O[1]	O[1]	O[1]	O[1]	O[1]	O[1]	—	O[1]
КОНФИДЕНЦИАЛЬНОСТЬ ДАННЫХ									
Конфиденциальность соединения[6]	—	Н/Р	Н/Р	Н/Р	Н/Р	Н/Р	Н/Р	—	Н/Р
ЦЕЛОСТНОСТЬ ДАННЫХ									
Целостность соединения[6]	—	Н/Р	Н/Р	Н/Р	Н/Р	Н/Р	Н/Р	—	Н/Р
Целостность содержимого	O[1]	—	—	—	—	—	—	—	—
Разметка защиты сообщения[3]	O[1]	O[1]	O[1]	O[1]	O[1]	O[1]	O[1]	O[1]	O[1]
АДМИНИСТРАТИВНОЕ УПРАВЛЕНИЕ ЗАЩИТОЙ									
Изменение удостоверения	—	O	—	O	Н/Р[5]	O	O	—	—
Регистр	—	O	—	O	Н/Р[5]	—	—	—	—
Регистр ХС	—	O	—	—	—	—	—	—	—

[1] Должна использоваться всегда

[2] Обеспечивается только для получателя сообщений (при использовании элемента защиты «целостность аргумента сообщения»)

[3] При использовании либо асимметричного, либо симметричного алгоритма так, как определено идентификатором алгоритма

[4] Аутентификация между соразмещенными объектами является локальным вопросом

[5] Эти услуги рассчитаны на обеспечение услугами нестандартного управления и, следовательно, не входят в предмет рассмотрения настоящего ФС

[6] Должны быть обеспечены, как определено в разделе 10 ИСО/МЭК 10021-2 и в ИСО 7498-2

7.7.3.3 *Класс защиты S2*

Таблица 7 — Класс защиты S2

Услуга защиты	1	2	3	4	5	6	7	8	9
Как и для S1, плюс:	АП/ АП	АП/ ХС	ХС/ АПС	АП/ АПС	АПС/ АПС	АПС/ АП	АПС/ ХС	АП/ ХС	ХС/ АП
АУТЕНТИФИКАЦИЯ ОТПРАВИТЕЛЯ									
Аутентификация отправителя сообщения[3]	О[1]	О[1]	—	О[1]	—	—	—	—	—
Аутентификация отправителя зонда	—	О[1]	—	О[1]	—	—	—	—	—
Аутентификация отправителя отчета	—	—	—	—	О[1]	О[1]	О[1]	—	—
Подтверждение предоставления	—	—	—	—	—	О	—	—	—
БЕЗОТКАЗНОСТЬ									
Безотказность отправителя[1]	О[4]	—	—	О[2]	—	—	—	—	—
Безотказность предоставления	—	—	—	—	—	О[2]	—	—	—
Безотказность доставки	О[4]	—	—	—	—	—	—	О[2]	—

[1] Должна использоваться всегда

[2] Используется асимметричный механизм (т.е. безотказные сертификаты и полномочия) для аутентификации в пределах АПС и СОС

[3] При использовании элемента защиты «контроль аутентификации отправителя сообщения»

[4] При использовании нотариально заверенного сертификата (симметричный алгоритм) или безотказных сертификатов и полномочий (асимметричный алгоритм)

7.7.3.4 *Варианты классов защиты конфиденциальности SnC*

Таблица 8 — Варианты классов защиты конфиденциальности SnC

Услуга защиты	1	2	3	4	5	6	7	8	9
Как и для Sn, плюс:	АП/ АП	АП/ ХС	ХС/ АПС	АП/ АПС	АПС/ АПС	АПС/ АП	АПС/ ХС	АП/ ХС	ХС/ АП
КОНФИДЕНЦИАЛЬНОСТЬ ДАННЫХ									
Конфиденциальность содержимого	О	—	—	—	—	—	—	—	—

7.8 Использование справочника (ИС)

ФГ «использование справочника» охватывает обеспечение элемента услуг «назначение получателя по имени справочника» следующим образом:

- обеспечение спецификации получателя посредством имени справочника пользователем СПС или АПС при предоставлении;

- обеспечение доступа к услугам справочника агентом передачи сообщения (АПС), чтобы получить один или несколько адресов О/П (или при предоставлении, или впоследствии, если отсутствует адрес О/П или он определен недействительным и присутствует имя справочника).

Примечание — Справочник может также применяться непосредственно пользователями СОС для получения информации, чтобы содействовать в предоставлении сообщений. Однако такое использование не требует особой СОС и это, следовательно, не входит в предмет рассмотрения настоящего стандарта.

Для АП обеспечение ФГ ИС требует только способности предоставления сообщений с одним или несколькими именами О/П, определенными с использованием имени справочника в соответствии с 8.5.5 ИСО/МЭК 10021-4. Так или иначе АП также должен обладать способностью непосредственного доступа к справочнику, что не входит в предмет рассмотрения настоящего ФС.

АПС может обращаться к услугам справочника, используя «агента пользователя справочника» (АПСПР). Вопрос об интерфейсе между АПС и АПСПР является локальным вопросом и не входит в предмет рассмотрения ГОСТ Р ИСО/МЭК МФС 10611. Точно так же взаимосвязь между АПСПР и одним или несколькими агентами системы справочника, предусматривающая услугу справочника, не входит в предмет рассмотрения ГОСТ Р ИСО/МЭК МФС 10611. Единственной информацией, которая, предположительно, может быть предоставлена справочной службой по данной версии ГОСТ Р ИСО/МЭК МФС 10611, является атрибут, содержащий один или несколько адресов О/П.

Примечание — СПС может использовать также службу справочника для получения информации, которая может быть использована, например в маршрутизации сообщений. Однако такое использование службы справочника не определяется базовыми стандартами СОС и, следовательно, не входит в предмет рассмотрения ГОСТ Р ИСО/МЭК МФС 10611.

7.9 Обеспечение межсетевого обмена 84 (ОМО84)

ФГ «обеспечение межсетевого обмена 84» охватывает обеспечение взаимодействия между реализациями, соответствующими ГОСТ Р

ИСО/МЭК МФС 10611 (называемыми «системами 1988»), и реализациями, соответствующими Рекомендации X.400 МККТТ (1984) (называемыми «системами 1984»). Обеспечение ФГ ОМО84 относится только к АПС и не используется, если только АПС не обеспечивает прикладной контекст протокола передачи СОС Р1 1984 (см. ГОСТ Р ИСО/МЭК МФС 10611-3).

Обеспечение ФГ ОМО84 требует соблюдения правил межсетевого обмена, определенных в приложении 8 ИСО/МЭК 10021-6. Дополнительные практические рекомендации по обеспечению межсетевого обмена с системами 1984 описаны в приложении D.

8 ПРИСВОЕНИЕ ИМЕН И АДРЕСАЦИЯ

8.1 Кодирование атрибутов адресов О/П

Основные правила, регулирующие различные способы кодирования (в допустимых случаях) атрибутов адресов О/П, определены в 18.2 ИСО/МЭК 10021-2.

Примечание — Рекомендуется использовать форму альфа-2 атрибута имя-страны. Для атрибутов имя-административного-региона и имя-частного-региона рекомендуется использовать форму распечатываемой строки.

АПС должен быть способен воспринимать предоставляемые сообщения, содержащие атрибуты адресов О/П в любом действительном коде, в целях их передачи и доставки (согласно обеспечиваемым портам). Никаких ограничений на репертуар символов не налагается, т.е. должны обеспечиваться все репертуары, определенные в ГОСТ Р ИСО/МЭК 8824 для телетексной строки.

АП должен быть способен предоставлять и воспринимать доставленные сообщения, содержащие атрибуты адресов О/П с любыми допустимыми кодами в пределах мнемонической формы. Однако обеспечение конкретного репертуара символов, а также методы включения таких значений на передающей стороне и методы обеспечения к ним доступа со стороны пользователя СОС на принимающей стороне не входят в предмет рассмотрения настоящего ФС.

8.2 Эквивалентность атрибута адреса О/П

В операциях сравнения предоставленного адреса О/П с набором известных адресов О/П применяются следующие правила эквивалентности для определения доставки, которые дополняют правила, определенные в 18.4 ИСО/МЭК 10021-2:

Если предоставленный адрес О/П может быть определен как недвусмысленный «подспецифицированный» известный адрес О/П, то адреса О/П эквивалентны.

Примечание 1 — «Подспецифицированный» означает, что некоторые атрибуты (или компоненты структурированных атрибутов) присутствуют в известном адресе О/П, но отсутствуют в предоставленном адресе О/П. «Подспецификация» не означает эквивалентности частичного значения (например, подстроки), когда одни и те же атрибуты присутствуют в обоих адресах О/П.

- «Надспецифицированные» адреса О/П не являются эквивалентными.

Примечание 2 — «Надспецификация» означает, что в предоставленном адресе О/П имеется больше атрибутов (или компонентов структурированных атрибутов), чем в известном адресе О/П. Тем не менее, в зависимости от локальной стратегии региона получателя неопознанные определяемые регионом атрибуты могут быть проигнорированы, если определена «надспецификация».

- Атрибуты, которые присутствуют в закодированных строках телетекса и в распечатываемых строках в том же самом адресе О/П, могут рассматриваться эквивалентными с точки зрения их регистрации для того же АП. Агенты ПС не несут ответственности за верификацию эквивалентности различных кодировок одного и того же атрибута. Каждая кодировка атрибута может быть использована для целей маршрутизации и доставки.

Дополнительные требования к правилам согласования конкретных репертуаров не входят в предмет рассмотрения ГОСТ Р ИСО/МЭК МФС 10611.

8.3 Способность маршрутизации

Способность АПС определять маршрут к другому АПС или место назначения пользователя СПС описана в разделе 19 ИСО/МЭК 10021-2. ГОСТ Р ИСО/МЭК МФС 10611 не устанавливают каких-либо требований относительно атрибутов адреса О/П, которые можно использовать в целях определения маршрута.

Для любого АПС, который обеспечивает передачу сообщений, в ЗСРП должно быть указано, какой из атрибутов адреса О/П можно использовать для определения дальнейшего маршрута, и должны быть перечислены любые ограничения (например, может ли маршрутизация основываться на конкретных значениях атрибута или только на наличии атрибута, любые ограничения на диапазоны значений, репертуары символов и т.д.).

Для любого АПС, который обеспечивает передачу сообщения, в ЗСРП должно быть указано: обеспечена ли перемаршрутизация.

8.4 Проверка адресов О/П

Как установлено в 14.6.1.4 ИСО/МЭК 10021-4, АПС должен проверять при предоставлении соответствие адресов О/П форматам, определенным в ИСО/МЭК 10021-2.

9 ОБРАБОТКА ОШИБОК И ОСОБЫХ СЛУЧАЕВ

Верхние границы, определенные в приложении В ИСО/МЭК 10021-4 и в приложении Е ИСО/МЭК 10021-5, являются обязательными для настоящего ФС.

Реализация не должна порождать элементов, которые превышают такие границы.

Реализация, обнаруживающая нарушение этих границ, может генерировать «нарушение предельных размеров», но это не является обязательным требованием.

От реализации не требуется способность принимать элементы вплоть до таких границ в тех случаях, когда в базовых стандартах определена индикация соответствующей ошибки (например, слишком длинное содержимое, слишком много получателей).

Обработка других нарушений протокола должна быть вопросом локальной политики. Реализации не требуют подтверждения правильности выполнения протокола, за исключением тех случаев, когда требуется выполнить действие, основанное на элементах такого протокола.

ПРИЛОЖЕНИЕ А
(обязательное)

ЭЛЕМЕНТЫ УСЛУГ

В случае выявления противоречий между текстом основной части настоящего стандарта и таблицами данного приложения предпочтение следует отдать таблицам приложения.

А.1 Элементы услуг ПС

В таблицах А.1—А.4 колонка «Базовое требование» отражает базовые требования к соответствию ГОСТ Р ИСО/МЭК МФС 10611, т.е. минимальный уровень обеспечения, требуемый от всех реализаций СОС (см. раздел 6). Колонка «Функциональная группа» (приведено ее сокращенное наименование — ФГ) определяет любые требования, обеспечиваемые дополнительно, если заявлено обеспечение факультативной функциональной группы (см. раздел 7). Каждая из указанных колонок разделена на несколько других колонок, отражающих обеспечение при отправке («Отправ.»), при обработке («Обраб.») и при получении («Получ.»), как определено в 3.2. Колонки отправителя и получателя, в свою очередь, разделены, чтобы отличить обеспечение, требуемое для АПС, от обеспечения, требуемого для пользователя СПС (последнее отражает только использование услуг ПС, а не их доступность пользователям СОС и может быть классифицировано далее в профиле типозависимого содержимого).

Таблица А.1 — Элементы услуг, относящиеся к базовым услугам ПС

Элемент услуг	Базовое требование					Функциональная группа					
	Отправ.		Обраб.	Получ.		ФГ	Отправ.		Обраб.	Получ.	
	Пользователь СПС	АПС		АПС	Пользователь СПС		Пользователь СПС	АПС		АПС	Пользователь СПС
Административное управление доступом[1)]	О	О	О	О	О						
Индикация типа содержимого	О	О	О	О	О						
Преобразованная индикация	—	—	О	О	О						
Указание времени доставки	—	—	О	О	О						
Идентификация сообщения	О	О	О	О	О						
Уведомление о недоставке	О	О	О	—	—						

Окончание таблицы А.1

Элемент услуг	Базовое требование					Функциональная группа					
	Отправ.		Обраб	Получ.		ФГ	Отправ.		Обраб.	Получ.	
	Пользователь СПС	АПС		АПС	Пользователь СПС		Пользователь СПС	АПС		АПС	Пользователь СПС
Индикация типов исходной кодированной информации	О	О	О	О	О						
Индикация времени предоставления	О	О	О	О	О						
Регистрация характеристик пользователь/АП[1)]	—	—	О	О	О						

[1)] Реализация этого ЭУ является локальным вопросом и должна выполняться с использованием доверительных функциональных возможностей, когда она реализуется в сочетании с ФГ ЗЩ

Таблица А 2 — Факультативные средства пользователя службы ПС

Элемент услуг	Базовое требование					Функциональная группа					
	Отправ.		Обраб.	Получ.		ФГ	Отправ.		Обраб.	Получ.	
	Пользователь СПС	АПС		АПС	Пользователь СПС		Пользователь СПС	АПС		АПС	Пользователь СПС
Разрешен альтернативный получатель	Ф	О	У[2)]	У[2)]	—	ПА			О	О	
Назначение альтернативного получателя[3)]	—	—	Ф	—	—	ПА			О		
Конфиденциальность содержимого	Ф	Ф	—	Ф	Ф	ЗЩ[1)]					
Целостность содержимого	Ф	Ф	—	Ф	Ф	ЗЩ[1)]					
Запрет преобразования	О	О	У[4)]	О	О	ПР			О		

Продолжение таблицы А.2

Элемент услуг	Базовое требование					Функциональная группа					
	Отправ.		Обраб.	Получ.		ФГ	Отправ.		Обраб.	Получ.	
	Пользователь СПС	АПС		АПС	Пользователь СПС		Пользователь СПС	АПС		АПС	Пользователь СПС
Запрет преобразования из-за потери информации	Ф	О	У[5]	О	Ф	ПР			О		
Задержанная доставка	Ф	О	О	—	—						
Аннулирование задержанной доставки[6]	Ф	О	О	—	—						
Уведомление о доставке	О	О	О	—	—						
Обеспечение получателя справочным именем	Ф	Ф	Ф	—	—	ИС	О	О	О		
Раскрытие других получателей	Ф	О	О	О	О						
Указание предыстории расширения СР	—	—	У[7]	О	Ф	СР			О		
Запрет расширения СР	О[8]	О	У[7]	—	—	СР			О		
Явное преобразование	Ф	О	Ф	—	—	ПР			У[10]		
Степень выбора доставки	О	О	О	О	О						
Удержание для доставки	—	—	У[9]	У[9]	Ф						
Неявное преобразование	—	—	Ф	—	—	ПР			У[10]		
Обозначение последней доставки	Ф	Ф	Ф	—	—	ПД	О	О	О		
Конфиденциальность потока сообщений	Н/Р	Н/Р	Н/Р	Н/Р	Н/Р						

Продолжение таблицы А.2

Элемент услуг	Базовое требование					Функциональная группа					
	Отправ.		Обраб.	Получ.		ФГ	Отправ.		Обраб.	Получ.	
	Пользователь СПС	АПС		АПС	Пользователь СПС		Пользователь СПС	АПС		АПС	Пользователь СПС
Аутентификация отправителя сообщения	Ф	Ф	Н/Р	Ф	Ф	ЗЩ[1)]					
Разметка защиты сообщения	Ф	Ф	Ф	Ф	Ф	ЗЩ[1)]					
Целостность последовательности сообщений	Ф	Ф	—	Ф	Ф	ЗЩ[1)]					
Многоадресная доставка	О	О	О	—	—						
Безотказность доставки	Ф	Ф	Ф	Ф	Ф	ЗЩ[1)]					
Безотказность отправителя	Ф	Ф	Ф	Ф	Ф	ЗЩ					
Безотказность предоставления	Н/Р	Н/Р	Н/Р	—	—	ЗЩ					
Альтернативный получатель, запрошенный отправителем	Ф	Ф	Ф	—	—	ПА		О	О		
Запрет уведомления о недоставке	Ф	О	О	—	—						
Зонд[11)]	Ф	О	О	—	—						
Аутентификация отправителя зонда	Н/Р	Н/Р	Н/Р	—	—	ЗЩ[1)]					
Подтверждение доставки	Ф	Ф	—	Ф	Ф	ЗЩ[1)]					
Подтверждение предоставления	Н/Р	Н/Р	Н/Р	—	—	ЗЩ[1)]					
Переадресация запрещена отправителем	О[8)]	О	У[12)]	—	—	ПА			О		
Переадресация поступающих сообщений	—	—	Ф	Ф	Ф	ПА			О	О	

Окончание таблицы А.2

Элемент услуг	Базовое требование					Функциональная группа					
	Отправ.		Обраб.	Получ.		ФГ	Отправ.		Обраб	Получ.	
	Пользователь СПС	АПС		АПС	Пользователь СПС		Пользователь СПС	АПС		АПС	Пользователь СПС
Аутентификация отправителя отчета	Н/Р	Н/Р	Н/Р	Н/Р	Н/Р	ЗЩ[1)]					
Запрошенный метод доставки	Ф	Ф	Ф	Ф	—						
Ограниченная доставка	—	—	Н/Р	Н/Р	Н/Р						
Возврат содержимого	Ф	Ф	Ф	—	—	ВС	О	О	О		
Управление защитой доступа	Ф	Ф	Ф	Ф	Ф	ЗЩ[1)]					
Использование списка распределения	О[13)]	О[13)]	Ф	—	—	СР			О		

[1)] См. таблицу А.5

[2)] Обеспечение этого ЭУ обязательно, если обеспечивается назначение альтернативного получателя

[3)] Метод, которым АПС определяет альтернативного получателя, не входит в предмет рассмотрения настоящего ФС

[4)] Обеспечение этого ЭУ обязательно, если обеспечивается неявное преобразование

[5)] Обеспечение этого ЭУ обязательно, если обеспечивается любой вид преобразования. Однако, если потерянная информация не полностью определена в базовых стандартах, то определить, была ли потеря информации, является локальным вопросом. Если реализация не может определить потерю информации, то она должна трактовать это требование как запрещенное преобразование

[6)] Сообщение следует хранить у АПС-отправителя в целях обеспечения для этого ЭУ

[7)] Обеспечение этого ЭУ обязательно, если обеспечивается расширение СР

[8)] Обеспечение этого ЭУ обязательно, так как значением по умолчанию является «разрешено». Для соответствия этому ФС требуется только способность выработки значения «запрещено»

[9)] Обеспечение этого ЭУ обязательно, когда использование реализации протокола РЗ является локальным вопросом в случае соразмещенного пользователя СПС

[10)] ФГ ПР требует обеспечения, по крайней мере, одного явного преобразования и неявного преобразования

[11)] Хотя обеспечение этого ЭУ агентом ПС требуется для соответствия базовым стандартам, рекомендуется, чтобы это обеспечение не требовали пользователи СПС

[12)] Обеспечение этого ЭУ обязательно, если поддерживается переадресация поступающих сообщений

[13)] Использование списка распределения в предоставлении возможно всегда, так как СР нельзя отличить от других адресов О/П

Таблица А.3 — Элементы услуг, относящиеся к взаимосвязи базовой услуги ОС/ФД

Элемент услуг	Базовое требование					Функциональная группа					
	Отправ.		Обраб.	Получ.		ФГ	Отправ.		Обраб.	Получ.	
	Пользователь СПС	АПС		АПС	Пользователь СПС		Пользователь СПС	АПС		АПС	Пользователь СПС
Базовое физическое изображение	Ф	Ф	—	Ф	Ф	ФД	О	О		О	О
Обычная почта	Ф	Ф	—	Ф	Ф	ФД	О	О		О	О
Физическое продвижение разрешено	Ф	Ф	—	Ф	Ф	ФД	О	О		О	О
Недоставляемая почта с возвратом физического сообщения	Ф	Ф	—	Ф	Ф	ФД	О	О		О	О

Таблица А.4 — Факультативные средства пользователя для взаимосвязи услуг ОС/ФД

Элемент услуг	Базовое требование					Функциональная группа					
	Отправ.		Обраб.	Получ.		ФГ	Отправ.		Обраб.	Получ.	
	Пользователь СПС	АПС		АПС	Пользователь СПС		Пользователь СПС	АПС		АПС	Пользователь СПС
Дополнительное физическое преобразование	Ф	Ф	—	Ф	Ф	ФД		О			
Доставка через почтовое окошко	Ф	Ф	—	Ф	Ф	ФД	О	О		О	О
Доставка через почтовое окошко с извещением	Ф	Ф	—	Ф	Ф	ФД		О			
Доставка через бюрофаксную службу	Ф	Ф	—	Ф	Ф	ФД		О			

Окончание таблицы А.4

Элемент услуг	Базовое требование					Функциональная группа					
	Отправ.		Обраб	Получ.		ФI	Отправ.		Обраб.	Получ.	
	Пользователь СПС	АПС		АПС	Пользователь СПС		Пользователь СПС	АПС		АПС	Пользователь СПС
Служба экспресс-почты	Ф	Ф	—	Ф	Ф	ФД	У[1]	О		У[1]	У[2]
Уведомление СОС о физической доставке	Ф	Ф	—	Ф	Ф	ФД		О			
Уведомление СФД о физической доставке	Ф	Ф	—	Ф	Ф	ФД		О			
Физическое продвижение запрещено	Ф	Ф	—	Ф	Ф	ФД	О	О		О	О
Регистрируемая почта	Ф	Ф	—	Ф	Ф	ФД		О			
Регистрируемая почта «лично — адресату»	Ф	Ф	—	Ф	Ф	ФД		О			
Запрос адреса продвижения	Ф	Ф	—	Ф		ФД		О			
Специальная доставка	Ф	Ф	—	Ф	Ф	ФД	У[1]	О		У[1]	У[2]

[1] По крайней мере, должен обеспечиваться один из этих ЭУ

[2] ЭУ должен обеспечиваться МДФД, если он обеспечивается АПС

Таблица А.5 — Услуги защиты

Элемент услуг	Класс защиты					
	S0		S1		S2	
	Пользователь СПС	АПС	Пользователь СПС	АПС	Пользователь СПС	АПС
Конфиденциальность содержимого[3]	У[1]	О	У[1]	О	У[1]	О
Целостность содержимого	О[3]	О[3]	О[2]	О[2]	О[2]	О[2]

Окончание таблицы А.5

Элемент услуг	Класс защиты					
	S0		S1		S2	
	Пользователь СПС	АПС	Пользователь СПС	АПС	Пользователь СПС	АПС
Аутентификация отправителя сообщения	О[4]	О[3]	О[2),4]	О[2]	О[2]	О[2]
Разметка защиты сообщения	Ф	О[3]	О[2]	О[2]	О[2]	О[2]
Целостность последовательности сообщений[3]	Ф	О	Ф	О	Ф	О
Безотказность доставки	Ф	О[3]	Ф	О[3]	О	О
Безотказность отправителя	Ф	О[3]	Ф	О[3]	О	О
Безотказность предоставления	Н/Р	Н/Р	Н/Р	Н/Р	О	О
Аутентификация отправителя зонда	Н/Р	Н/Р	Н/Р	Н/Р	О[2]	О[2]
Подтверждение доставки	О	О	О	О	О	О
Подтверждение предоставления	Н/Р	Н/Р	Н/Р	Н/Р	О	О
Аутентификация отправителя отчета	Н/Р	Н/Р	Н/Р	Н/Р	О	О
Административное управление защитой доступа	Ф	Ф	О[2]	О[2]	О[2]	О[2]

[1] Обеспечение становится обязательным, если заявлено обеспечение варианта класса конфиденциальности SnC

[2] Этот ЭУ должен использоваться всегда, и АПС должен проверить, всегда ли присутствует(ют) соответствующий(е) элемент(ы)

[3] Не предполагается, что АПС будет выполнять какие-либо действия, кроме обеспечения синтаксиса соответствующего элемента(ов) (исключая случай применения примечания 2)

[4] Только пользователь СПС с пользователем СПС

А.2 Элементы услуг ХС

В таблицах А.6 и А.7 колонка «Базовое требование» отражает базовые требования к соответствию ГОСТ Р ИСО/МЭК МФС 10611, т.е. минимальный уровень обеспечения, требуемый от всех реализаций СОС (см. раздел 6). Колонка «Функциональная группа» (приведено ее сокращенное наименование — ФГ) определяет любые требования, обеспечиваемые дополнительно, если заявлено обеспе-

чение факультативной функциональной группы (см. раздел 7). Каждая из указанных колонок, в свою очередь, разделена на несколько других колонок, чтобы отличить обеспечение, требуемое для ХС, от обеспечения, требуемого для пользователя ХС, т е АП (последнее отражает только использование услуг ХС, а не их доступность пользователю СОС и может быть классифицировано далее в профиле типозависимого содержимого).

Таблица А.6 — Хранилище базовых сообщений

Элемент услуг	Базовое требование		Функциональная группа		
	АП	ХС	ФГ	АП	ХС
Регистр ХС	Ф	О			
Аннулирование хранимого сообщения	О	О			
Извлечение хранимого сообщения	О	О			
Листинг хранимого сообщения	Ф	О			
Сводный перечень хранимых сообщений	Ф	О			

Таблица А.7 — Факультативные средства пользователя ХС

Элемент услуг	Базовое требование		Функциональная группа		
	АП	ХС	ФГ	АП	ХС
Состояние готовности хранимого сообщения	Ф	Ф			
Автопродвижение хранимого сообщения	Ф	Ф			

ПРИЛОЖЕНИЕ В
(обязательное)

ИЗМЕНЕНИЯ И ТЕХНИЧЕСКИЕ ПОПРАВКИ

Международные стандарты постоянно подвергаются пересмотрам и изменениям со стороны заинтересованных технических комитетов ИСО/МЭК. Приведенные ниже изменения и технические поправки одобрены СТК1 ИСО/МЭК и рассматриваются в настоящем ФС как нормативные ссылки.

Примечание – Соответствующие технические поправки эквивалентных рекомендаций МККТТ содержатся в совместном документе МККТТ/ИСО «Руководство для разработчика СОС» (версия 11).

ИСО/МЭК 10021-1/Тп.1:1991
ИСО/МЭК 10021-1/Тп.2:1991
ИСО/МЭК 10021-1/Тп.3:1992
ИСО/МЭК 10021-1/Тп.4:1992
ИСО/МЭК 10021-1/Тп.5:1992
ИСО/МЭК 10021-1/Тп.6:1994
ИСО/МЭК 10021-2/Тп.1:1991
ИСО/МЭК 10021-2/Тп.2:1991
ИСО/МЭК 10021-2/Тп.3:1992
ИСО/МЭК 10021-2/Тп.4:1992
ИСО/МЭК 10021-2/Тп.5:1993
ИСО/МЭК 10021-2/Тп.6:1994
ИСО/МЭК 10021-2/Тп.7:1994
ИСО/МЭК 10021-4/Тп.1:1991
ИСО/МЭК 10021-4/Тп.2:1991
ИСО/МЭК 10021-4/Тп.3:1992
ИСО/МЭК 10021-4/Тп.4:1992
ИСО/МЭК 10021-4/Тп.5:1992
ИСО/МЭК 10021-4/Тп.6:1993
ИСО/МЭК 10021-4/Тп.7:1994
ИСО/МЭК 10021-4/Тп.8:1994
ИСО/МЭК 10021-5/Тп.1:1991
ИСО/МЭК 10021-5/Тп.2:1991
ИСО/МЭК 10021-5/Тп.3:1992
ИСО/МЭК 10021-5/Тп.4:1992
ИСО/МЭК 10021-5/Тп.5:1992
ИСО/МЭК 10021-5/Тп.6:1993
ИСО/МЭК 10021-5/Тп.7:1994
ИСО/МЭК 10021-6/Тп.1:1991
ИСО/МЭК 10021-6/Тп.2:1991
ИСО/МЭК 10021-6/Тп.3:1992
ИСО/МЭК 10021-6/Тп.4:1992
ИСО/МЭК 10021-6/Тп.5:1992
ИСО/МЭК 10021-6/Тп.6:1993
ИСО/МЭК 10021-6/Тп.7:1994

ИСО/МЭК 10021-1/Изм.2:1994
ИСО/МЭК 10021-2/Изм.1:1993
ИСО/МЭК 10021-2/Изм.2:1994
ИСО/МЭК 10021-4/Изм.1:1994

ПРИЛОЖЕНИЕ С
(информационное)

ЗАЩИТА ОБМЕНА СООБЩЕНИЯМИ — РЕАЛИЗАЦИЯ И ЛОГИЧЕСКОЕ ОБОСНОВАНИЕ

С.1 Введение

Цель функциональной группы «защита» (ЗЩ) состоит в том, чтобы определить принципы обеспечения защиты обмена сообщениями в системах обработки сообщений (СОС) в рамках общей структуры функциональных профилей в области СОС

С.2 Уязвимость обработки сообщений

Уязвимость обработки сообщений (угрозы), которая может быть предупреждена с использованием ЗК и ЗС, определена в приложении D ИСО/МЭК 10021-2

- маскирование,
- нарушение последовательности сообщении,
- модификация информации,
- отклонение услуги,
- отказ,
- утечка информации.

Существуют другие специфические угрозы, если имеются ошибки в обеспечении разделения информации, в том числе

- манипулирование,
- неправильный маршрут,
- внутренние угрозы,

внешние угрозы

Некоторые из этих угроз определены в ИСО 7498-2, в котором определены также другие угрозы, не относящиеся к СОС

Приложение D ИСО/МЭК 10021-2 также содержит рекомендуемые услуги защиты СОС, которые могут быть использованы для защиты от таких угроз Некоторые угрозы СОС не могут быть легко предотвращены одни просто обнаруживаются другие не подходят для стандартизации

С.3 Общие принципы

С.3.1 Стратегия защиты

Общая стратегия защиты организации должна быть обусловлена рассмотрением уязвимости со стороны угроз и способов отражения угроз (т е процедурно, физически персоналом, документацией и мероприятиями по защите информационной технологии) Такая стратегия защиты может быть выражена в виде набора законов, правил и накопленного опыта, определяющих способы, с помощью которых организация управляет защищает и распределяет чувствительную информацию Эта стратегия защиты определяет общие принципы организации защиты и должна учитывать все аспекты защиты

Защита в пределах организации касается не только СОС и должна рассматриваться в более глобальном и общем смысле. Обширные аспекты стратегии защиты должны поэтому включать в себя вопросы, связанные с кадровым составом (такие, как проверка и состояние конфиденциальности среди персонала), управлением доступом конечного

пользователя, физической, процедурной и документальной защитой. В этом приложении, тем не менее, рассматривается только защита в информационной технологии, особенно в области связи (ЗС) и вычислительных машин (ЗК), как относящаяся к стандартизации защиты СОС, работающей в функциональной среде запоминания с последующей передачей.

С.3.2 Классы защиты

В базовых стандартах СОС некоторые угрозы отражаются мерами защиты с использованием средств информационной технологии. Эти меры реализуются предоставлением услуг защиты и выполняются с использованием элементов защиты.

Эта группа ФС СОС вместе с возможностями защиты (услуги и элементы), определенными в базовых стандартах, составляют нарастающий набор классов защиты. Класс защиты обычно не должен полностью реализовать стратегию защиты, он лишь рассматривается как общий компонент, который может содействовать реализации такой стратегии защиты.

Класс защиты S0 требует только обеспечение услуг сквозной защиты между АП (целостность содержимого, аутентификация отправителя сообщения, подтверждение доставки) и, следовательно, может быть использован для обеспечения некоторых видов защиты даже в случае транзита через промежуточную СПС, которая может оказаться без должного уровня доверия.

Класс защиты S1 дополнительно требует обеспечение и использование административного управления защитой доступа в пределах СПС, с тем чтобы позволить реализовать стратегию защиты, основанную на разметке, и доверительный межсетевой обмен между регионами защиты.

Класс защиты S2 дополнительно требует обеспечение и использование контроля аутентификации отправителя в пределах СПС для подтверждения подлинности отправителя сообщений, зондов и отчетов и, тем самым, для подтверждения бесспорности услуги в пределах СПС.

Каждый из классов защиты имеет также вариант (SnC), требующий обеспечить сквозную конфиденциальность содержимого (логическим обоснованием таких вариантов является исключение затрат на реализацию и накладных расходов, вызванных шифрованием всего содержимого сообщения, если только это не является определяющим требованием).

Каждый класс защиты содержит набор обязательных и факультативных услуг защиты. В пределах класса защиты обязательные услуги защиты могут быть выбраны абонентом или пользователем как на основе сообщения, так и на согласованный договорный период времени. Хотя возможности и механизмы выполнения обязательных услуг защиты должны быть обеспечены всегда, однако вопрос о том, предлагается ли такая услуга защиты по выбору пользователя или она вызывается постоянно, является локальным вопросом. В то же время, использование некоторых услуг защиты требуется всегда для отдельных классов защиты. Это проявляется в настоящем стандарте введением динамических требований дополнительно к определенным в базовых стандартах СОС при гарантии того, что соответствующие элементы протокола всегда присутствуют. Точно так же использование некоторых услуг защиты запрещено для отдельных классов защиты. Это проявляется в настоящем стандарте введением динамических требований дополнительно к определенным в базовых стандартах СОС при гарантии того, что данный элемент протокола всегда отсутствует.

С.3.4 Методы шифрования

Возможности защиты обмена сообщениями, определенные в базовых стандартах СОС, должны быть обеспечены путем использования трех базовых методов защиты, а именно:

- симметричного шифрования;
- асимметричного шифрования,
- функций доверительности (т.е. мер ЗК).

Стандарты СОС позволяют использовать эти методы на индивидуальной основе для обеспечения услуг защиты или в комбинации в соответствии со стратегией защиты. Настоящий стандарт объединяет методы с целью установить исчерпывающий набор возможностей защиты, которые предназначены для отражения угроз службе обмена сообщениями. В некоторых случаях услуги защиты, определенные в стандартах СОС, могут быть реализованы только путем использования одного из упомянутых методов, а именно асимметричного шифрования. Однако фактически реализуемый метод должен зависеть от алгоритмов, которые должны быть зарегистрированы полномочным органом защиты данного региона.

Цель настоящего стандарта состоит в том, чтобы не ограничивать реализации одними асимметричными методами. Там, где возможно, услуги защиты могут быть реализованы с использованием доверительных функциональных возможностей в сочетании с симметричным, асимметричным методами или одновременным использованием этих методов шифрования. В частности, настоящий стандарт допускает использование либо асимметричного, либо симметричного методов как для обозначаемых, так и для зашифрованных данных в пределах полномочий сообщения.

Фактически реализуемый метод зависит от используемого алгоритма. Предполагается, что алгоритмы согласованы на двусторонней основе и зарегистрированы полномочным органом регистрации. Тем не менее, идентификатор алгоритма должен быть уникальным и однозначно идентифицировать алгоритм.

Рекомендуется, чтобы соответствующая СТРОКА БИТОВ АСН.1 обычно использовалась для размещения шифрованных данных (генерируемых путем использования макрокоманды ENCRYPTED) и, тем самым, для вставки нулевых битов заполнителей, которые могут потребоваться для правильного функционирования некоторых алгоритмов. Как вариант реализация должна явно использовать такое действие.

Рекомендуется, чтобы при отсутствии какого-либо требования к обеспечению других специфических алгоритмов реализации поддерживали алгоритмы, идентифицированные в ИСО/МЭК 9594-8. Также настоятельно рекомендуется, чтобы реализации были способны использовать любые методы шифрования путем «разъемных соединений» или на модульной основе.

В случае верификации SIGNATURE (например, подтверждение доставки, проверка аутентификации отправителя) реализации должны предусматривать, чтобы все данные, относящиеся к таким объектам, как сообщение, зонд или отчет, были включены в подпись.

С.3.5 Вопросы реализации

С.3.5.1 *Аутентификация равноправных объектов*

Аутентификация равноправных объектов достигается с помощью определенных механизмов аутентификации в различных операциях Bind (Связка), основанных на асимметричном или симметричном методе. Информация управления ключом, необхо-

димая при симметричной «аутентификации равноправных объектов», не входит в предмет рассмотрения настоящего стандарта.

С.3.5.2 *Конфиденциальность*

Конфиденциальность соединения, которая основана на использовании нижерасположенных уровней ВОС не входит в предмет рассмотрения настоящего ФС. Механизмы достижения конфиденциальности соединения являются предметом двустороннего соглашения между равноправными партнерами (т.е. конфиденциальность соединения может быть достигнута созданием доверительного соединения ВОС между равноправными партнерами).

Конфиденциальность соединения может быть достигнута симметричным или асимметричным методом шифрования.

Примечание – Шифрование асимметричным методом предотвращает предоставление сообщений многочисленным получателям, но не позволяет использовать тот же самый секретный шифр.

С.3.5.3 *Целостность*

Целостность соединения, которая основана на использовании нижерасположенных уровней ВОС, не входит в предмет рассмотрения настоящего ФС. Механизмы достижения целостности соединения являются предметом двустороннего соглашения между равноправными партнерами. Следует отметить, что целостность «соединения» может быть повышена с использованием СЭНП.

«Целостность содержимого» достигается вычислительными методами проверки целостности содержимого в качестве функции целостности содержимого сообщения. В том случае, когда для вычисления проверки целостности содержимого используется симметричный метод, требуется секретный шифр. Этот шифр целостности содержимого может быть конфиденциально переслан получателю сообщения с использованием элемента защиты «конфиденциальность аргумента сообщения», т.е. средствами шифрования данных в полномочии сообщения (здесь могут быть другие шифры или части шифра, не посланные отправителем с сообщением, но управление такими внешними шифрами не входит в предмет рассмотрения настоящего стандарта). Следует отметить, что включение проверки целостности содержимого в шифрованные данные полномочного сообщения должно быть снабжено дополнительно защитой против угроз маскирования.

Примечание – Функция целостности содержимого может также включать в себя целостность уведомлений получения-неполучения и может способствовать «бесспорности получения», поскольку бесспорность доставки может оказаться недостаточной в случае доставки в хранилище сообщений.

С.3.5.4 *Аутентификация отправителя сообщения*

Сквозная (т.е. от АП до АП) аутентификация отправителя сообщения (с использованием элемента защиты «целостность аргумента сообщения») обеспечивается автоматически целостностью содержимого. Класс защиты S2 гарантирует дополнительную защиту (т.е. целостность разметки) благодаря требованию к обеспечению проверки подлинности отправителя в пределах СПС.

С.3.5.5 *Доказательство/Безотказность*

Если для «целостности содержимого» используется асимметричный метод, он может также обеспечить «безотказность» отправителя (АП к АП) в зависимости от уровня доверия, помещенного в сертификат. При использовании симметричного метода целостность содержимого может также обеспечивать безотказность отправителя, но

только при нотариально заверенном подтверждении целостности содержимого, и обеспечивать функциональные возможности управления заверенным шифром. Степень безотказности может быть достигнута путем использования услуг заверенной отчетности.

Примечание — Предполагается, что передающий АП должен гарантировать, что уведомление доставки будет запрошено, если запрошено подтверждение доставки.

С.3.5.6 *Административное управление защитой доступа*

«Административное управление защитой доступа» может быть реализовано сочетанием функциональных возможностей многоуровневой защиты (МУЗ) и гарантией наличия различных компонентов СОС для обеспечения такой функциональности. Функциональные возможности МУЗ, которые реализуются (согласно стандартам СОС) благодаря использованию меток защиты, контекста защиты и полномочий защиты, могут быть применены иерархическим или функциональным образом в зависимости от требований стратегии данного региона.

Гарантия МУЗ в целом также требует других средств (ЗК), а это не входит в предмет рассмотрения базовых стандартов СОС и настоящего стандарта. Должны быть даны ссылки на соответствующие полномочные органы защиты и на любые применимые критерии оценки защиты (например, Европейский критерий оценки защиты информационной технологии).

Услуга «контекст защиты» гарантирует, что разметка защиты сообщения соответствует, по меньшей мере, одному из набора меток, определенных в контексте защиты, установленной между взаимодействующими объектами. Реализация, которая обеспечивает эту услугу, должна, как минимум, поддерживать точное соответствие равенства идентификатора стратегии защиты, классификации защиты и элементов категорий защиты метки. Какие-либо другие правила согласования (например, охватывающие элемент частной метки или основывающиеся на альтернативных методах сравнения) могут быть использованы в отдельных прикладных сценариях, но такое требование, которое должно быть предметом двустороннего соглашения, должно вводиться в зависимости от стратегии защиты.

Примечание — Требование базового обеспечения состоит в том, что отсутствие элемента не должно трактоваться как «любое значение», т.е. все допустимые сочетания вхождения и значения элементов разметки защиты сообщения должны быть детально проработаны в контексте защиты. Таким образом, если необходимо передать сообщение с меньшими требованиями защиты, чем возможности связанных объектов, оно должно быть помечено соответствующим идентификатором класса защиты и контекст защиты должен включать в себя этот класс в пределах набора допустимых идентификаторов стратегии защиты. При использовании такого механизма межсетевой обмен может быть ограничен сообщениями только одного класса защиты.

Разметка защиты сообщения может быть реализована в расширениях на каждое сообщение либо в данных со знаком, либо зашифрованных данных маркера сообщения на каждого получателя. Рекомендуется, чтобы целостность разметки защиты защищалась введением ее в маркер данных со знаком или (если метка вводится в расширения на каждое сообщение) путем расчетной проверки подлинности отправителя сообщений. Какие из этих меток контролируются относительно контекста защиты, зависит от действующей стратегии защиты. Стратегия защиты должна также определять любые требования к допустимым значениям меток (на каждого получателя) в том случае, когда сообщение адресуется многим получателям (и, тем самым, имеет много

полномочий). Если метка также включается в зашифрованные данные, она должна иметь то же значение, что и в данных со знаком полномочий или в расширениях на каждое сообщение (и может, таким образом, иметь семантики сквозной конфиденциальности). Такая метка может быть использована для административного управления защитой доступа АП получателя.

С.3.5.7 *Участие при использовании списков распределения*

АПС, выполняющий расширение списка распределения (СР), должен создавать все поля на каждого получателя для членов СР. Он может создавать либо новые полномочия для каждого члена СР (т.е. используя имя получателя, который является членом этого СР), либо как вариант он может копировать те же полномочия (т.е. содержащие имя получателя из своего СР) в поля на каждого получателя для каждого члена СР. В первом случае проверка целостности содержимого не должна изменяться, если она используется для аутентификации отправителя сообщения. В этом случае также пункт расширения СР должен обеспечивать, по крайней мере, тот же самый класс защиты, что и отправитель, и иметь заверенные функциональные возможности. Выбор варианта должен, следовательно, осуществляться в соответствии со стратегией защиты, которая может совсем запретить использование списков распределения.

Примечание – Если стратегия защиты разрешает использование списков распределения, она должна устанавливать также стратегию обработки СР для уведомлений.

С.3.5.8 *Участие в переадресации*

Реализация функциональной группы «защита» может, кроме того, либо потребовать, чтобы любые функциональные возможности переадресации были заверены, либо, наоборот, запретить использование переадресации.

Если функциональные возможности переадресации должны быть заверены, то они должны быть объектами стратегии защиты и должны подчиняться разметке защиты, как это определено в базовых стандартах СОС. Рекомендуется, чтобы маркер не изменялся при переадресации (т.е. он должен содержать имя получателя, первоначально определенное отправителем).

С.3.5.9 *Участие при обеспечении межсетевого обмена 84*

Защита межсетевого обмена между реализациями, соответствующими функциональной группе «защита», и системами 1984 не обеспечивается. Метод двойного конверта, однако, может быть использован при прохождении через системы 1984.

С.3.5.10 *Участие при использовании справочника*

Реализация функциональной группы «защита» может, кроме того, либо потребовать, чтобы любая услуга справочника была заверена, либо, наоборот, запретить использование услуг справочника.

С.3.5.11 *Участие при преобразовании*

Реализация функциональной группы «защита» может, кроме того, потребовать, чтобы любые возможности преобразования были заверены для регенерации соответствующих элементов защиты (особый контроль целостности содержимого), либо, наоборот, запретить использование преобразования в пределах СПС. В частности, следует отметить, что использование функциональных возможностей преобразования сделает недействительной любую аутентификацию отправителя, основанную на содержимом отправителя. В связи с этим рекомендуется, чтобы всегда устанавливался запрет преобразования, когда АПС используется без защиты для целей ретрансляции.

С.3.5.12 *Учетная информация*

Учетная информация зависит от идентификации и аутентификации пользователей, и вся информация о действиях пользователей должна надлежащим образом записываться и храниться.

Учетные функции, обеспечиваемые регионами (или АПС), являются предметом двусторонних соглашений между регионами (или АПС) и могут факультативно обеспечивать услуги бесспорности. К учетным функциям относятся механизмы подробного анализа, такие как журнал защиты, результат ревизий и архивы, либо механизмы, основанные на протоколе. Механизмы, основанные на протоколе, предназначенные для обеспечения учетных функций, должны быть предметом двусторонних соглашений.

С.3.5.13 *Двойной конверт*

Двойной конверт может быть использован с каждым классом защиты в качестве факультативного расширения возможностей защиты, которые могут быть использованы для подсчета конкретных уязвимостей. Двойной конверт следует применять на границе региона и подчинять правилам АПС на границах административного региона. На рисунке С.1 приведена иллюстрация этого метода.

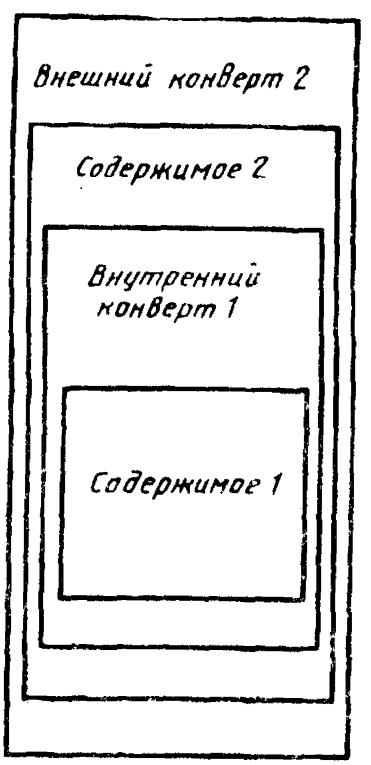

Рисунок С.1 — Двойной конверт

Адресация и трассовая информация не обязательно одинаковы в конвертах 1 и 2. Трассовая информация не передается между внутренним и внешним конвертами. При использовании способа двух конвертов рекомендуется, чтобы трассовая информация внешнего конверта всегда архивировалась в пункте, где внутренний конверт становится субъектным сообщением.

Метод двойного конверта может быть использован в функциональных средах СПС 1984 и 1988 и может, в принципе, быть применен при предоставлении, доставке и пересылке конвертов. При использовании функциональной среды 1988 для внешнего конверта 2 могут быть применены любые классы защиты. Рекомендуется, чтобы содержимое 2 (внутренний конверт 1 плюс содержимое 1) было зашифровано. Если метод двойного конверта используется в качестве защиты пути ретрансляции через регион 1984, то любое шифрование содержимого 2 должно быть предметом двустороннего и(или) многостороннего соглашения.

С.4 Класс защиты S0

С.4.1 Обоснование

Класс защиты S0 ограничивается функциональными возможностями защиты, действующими между пользователями СПС на сквозной основе, для того чтобы позволить передачу через СПС, которая может оказаться негарантированной. Он предназначен для того, чтобы минимизировать объем функциональных возможностей в СПС для обеспечения предоставления элементов, связанных с этими услугами. Услуги защиты, которые должны быть обеспечены (т.е. должны быть доступными), — это те услуги, которые считают существенно важными в любой функциональной среде защиты обмена сообщениями:

- целостность содержимого;
- аутентификация отправителя сообщения (сквозная);
- подтверждение доставки.

Иные услуги защиты, такие как конфиденциальность содержимого, могут быть обеспечены факультативно.

С.4.2 Техническое участие

Техническое участие класса защиты S0 осуществляется следующим образом:

- при предоставлении сообщения пользователю СПС потребуются механизмы для генерации макрокоманд SIGNED, SIGNATURE и ENCRYPTED;
- при доставке сообщения пользователю СПС потребуются механизмы для обработки макрокоманд SIGNED, SIGNATURE и ENCRYPTED.

С.5 Класс защиты S1

С.5.1 Обоснование

Класс защиты S1 представляет собой супернабор классов защиты S0, которые устанавливают базовые требования к функциональным возможностям защиты не только в пределах пользователя СПС, но также и в пределах СПС. Функциональные возможности в пределах СПС предназначены для активизации стратегии защиты в пределах региона защиты. Как следствие S1 позволяет реализовать маршрут доверия.

Примечание - Уровень доверия в маршруте должен зависеть от уровня доверия в разметке защиты и от контекста защиты.

С.5.2 Техническое участие

Техническое участие класса защиты S1 такое же, как и класса защиты S0, со следующими дополнениями:

- АПС потребуются механизмы для регистрации, изменения удостоверения личности и операций абстрактной связки (т.е. макрокоманды SIGNED для связки);

- ХС потребуются механизмы для регистрации ХС и операции связки ХС (т.е. макрокоманды SIGNED для связки ХС);

- потребуется обеспечение разметки защиты сообщения (уровень гарантии является предметом требований защиты отдельного региона);

- может потребоваться обеспечение надежного доступа;

- АПС может потребовать контроль наличия элементов защиты, которое в настоящем ФС определено как обязательное;

-необходимо обеспечить доверительное соединение ВОС между равноправными партнерами для адекватной конфиденциальности, целостности и аутентификации равноправных логических объектов.

С.6 Класс защиты S2

С.6.1 Обоснование

Класс защиты S2 представляет собой супернабор классов защиты S1. Он требует, чтобы АПС проверял отправку сообщений, зондов и отчетов в пределах СПС и осуществлял расширенные проверки целостности по меткам в пределах СПС. Дополнительные услуги защиты, предоставляемые этим классом защиты, могут содействовать в обеспечении доверительной маршрутизации в пределах СПС. Дополнительно предоставляется возможность поддержки услуги бесспорности в пределах СПС.

С.6.2 Техническое участие

Определяемые классом защиты S2 дополнительные услуги защиты используют исключительно асимметричные методы.

Техническое участие класса защиты S2 такое же, как участие класса защиты S1, со следующими дополнениями:

- АПС или пользователю СПС могут потребоваться механизмы макрокоманды SIGNED для обработки сертификатов, если сертификаты используются;

- факультативно обеспечиваемая конфиденциальность содержимого не разрешается в том случае, когда проверка подлинности отправителя сообщений используется для обеспечения услуг безотказности;

- АПС могут потребоваться механизмы для генерации и обработки макрокоманды SIGNATURE, позволяющие проверять подлинности сообщения, зонда и отчета (MOAC, POAC и ROAC);

- АПС или пользователю СПС могут потребоваться сопряжения со службой справочника, поддерживающей «основы аутентификации» в соответствии с ИСО/МЭК 9594-8, либо как вариант он может распределить ключи общего пользования некоторыми другими доверительными способами, которые соответствуют ИСО/МЭК 9594-8;

- при использовании сертификатов необходимо обеспечить заверенные средства генерации сертификатов;

- АПС потребуются механизмы, позволяющие выработать подтверждение предоставления макрокоманды SIGNATURE;

- AHC потребуются механизмы выработки макрокоманды ROAC SIGNATURE с отчетами.

С.7 Варианты классов защиты «конфиденциальность» (SnC)

С.7.1 Обоснования

Эти варианты классов защиты представляют собой супернабор классов S0, S1 и S2, дополняющих требования к обеспечению сквозной «конфиденциальности содержимого». Цель введения указанных вариантов состоит в том, чтобы исключить накладные расходы на реализацию и обработку, обусловленные шифрованием всего содержимого сообщения, если только не существует определяющего требования. Также возможна защита методов и механизмов шифрования (т.е. алгоритмов, длин ключей, версий ключей и т.п.) с использованием административного управления защитой доступа.

С.7.2 Техническое участие

Техническое участие вариантов класса защиты «конфиденциальность» такое же, как и участие соответствующих основных классов со следующим дополнением:

- пользователю CHC могут потребоваться механизмы, которые могут использовать макрокоманды ENCRYPTED для шифрования и дешифрования содержимого.

ПРИЛОЖЕНИЕ D
(информационное)

ДОПОЛНИТЕЛЬНЫЕ РЕКОМЕНДАЦИИ ПО ОБЕСПЕЧЕНИЮ МЕЖСЕТЕВОГО ОБМЕНА 1984

D.1 Введение

Это приложение содержит некоторые дополнительные рекомендации, касающиеся обеспечения межсетевого обмена между реализациями, соответствующими ГОСТ Р ИСО/МЭК МФС 10611 (в дальнейшем называемыми «системами 1988») и реализациями, соответствующими ранним версиям базовых стандартов СОС (в дальнейшем называемыми «системами 1984»).

Такие рекомендации дополняют требования функциональной группы «обеспечение межсетевого обмена 84» либо потому, что вопросы обеспечения межсетевого обмена не входят в предмет рассмотрения базовых стандартов СОС (и, следовательно, не входят в предмет рассмотрения формального соответствия настоящему стандарту), либо потому, что решение этих вопросов предложено в рамках базовых стандартов СОС.

D.2 Внутренняя трассовая информация

Правила обеспечения межсетевого обмена, приведенные в приложении В ИСО/МЭК 10021-6, имеют дело со многими аспектами понижения уровня протокола P1, но не охватывают АПС, который или генерирует, или рассчитывает на получение внутренней трассовой информации, как определено в раннем проекте MOTIS 1985/6. Поскольку последний в настоящее время заменен, ниже приведено для справки первоначальное требование:

```
InternalTraceInfo  ::= [APPLICATION 30] IMPLICIT SEQUENCE
                         OF SEQUENCE {
                           MTAName,
                           MTASuppliedInfo }
MTAName            ::= PrintableString
MTASuppliedInfo    ::= SET {
        arrival             [0] IMPLICIT Time,
        deferred            [1] IMPLICIT Time OPTIONAL
        action              [2] IMPLICIT INTEGER {
                                relayed              (0),
                                rerouted             (1),
                                recipientReassignment (2)}
        previous            MTAName OPTIONAL }
```

Приводимые ниже процедуры представляют «отображение» или преобразование между стандартной внутренней трассовой информацией, обеспечиваемой системами 1988, и внутренней трассовой информацией, определенной выше. Они рекомендуются для использования в тех случаях, когда требуется одновременное применение систем 1988 и систем 1984, которые обеспечивают внутреннюю трассовую информацию приведенной спецификации в одном и том же регионе.

Процедуры описаны с точки зрения требуемых изменений семантики. Следует, однако, отметить, что синтаксис АСН.1 также отличается от рассмотренного, что может потребовать сложной трансляции.

D.2.1 Правила пересылки внутренней трассовой информации в системы 1984

Если глобальный индентификатор региона какого-либо элемента внутренней трассовой информации не идентифицирует текущий регион, тогда этот элемент и все предшествующие элементы внутренней трассовой информации аннулируются. Глобальный идентификатор региона удаляется из всех оставшихся элементов внутренней трассовой информации.

Если преобразованные типы кодированной информации присутствуют в каком-либо элементе внутренней трассовой информации, тогда этот и все предшествующие элементы внутренней трассовой информации удаляются.

Если какой-либо элемент внутренней трассовой информации имеет установленные раздельно или одновременно биты переадресации и обработки списка распределения, тогда дополнительный элемент внутренней трассовой информации порождается путем копирования имени АПС и принятых элементов и установкой действующего элемента в ПереназначениеПолучателя (новый элемент вставляется непосредственно за первоначальным элементом).

Если какой-либо элемент внутренней трассовой информации имеет пробный элемент, содержащий регион, то этот пробный элемент удаляется.

Следует также отметить, что базовые стандарты СОС 1988 определяют имя АПС как строку МК5, тогда как в приведенной выше спецификации внутренней трассовой информации 1984 используется распечатываемая строка.

Во избежание возможных зацикливаний в пределах региона рекомендуется, чтобы имена АПС включали в себя только те символы, которые входят в репертуар символов «распечатываемая строка».

D.2.2 Правила пересылки внутренней трассовой информации из системы 1984

Глобальный идентификатор региона всех элементов внутренней трассовой информации является набором, идентифицирующим текущий регион.

Если элемент внутренней трассовой информации получен из системы 1984 с действующим значением ПереназначениеПолучателя, то другой действующий элемент порождается с установленным битом переадресации. Если непосредственно предшествующий элемент внутренней трассовой информации имел идентичное имя АПС, к нему добавляется генерируемый элемент «другие действия», а текущий элемент внутренней трассовой информации удаляется. В противном случае текущий элемент внутренней трассовой информации имеет добавленный к нему элемент «другие действия», а элемент «действие маршрутизации» устанавливается в состояние ретрансляции.

D.3 Атрибут общее-имя адреса О/П

В ИСО/МЭК 10021-6/Тп.6 определено преобразование атрибута общее-имя адреса О/П в атрибут типа «общий», определяемый регионом, и обратное преобразование из атрибута типа «общий», также определяемого регионом.

D.4 Дополнительные нестандартные расширения 1984

При выдаче ответа на выходящий из системы 1984 запрос установления ассоциации значение идентификатора протокола воспринимается либо как «1», либо как «8883». Если инициируется установление ассоциации с системой 1984, для идентификатора протокола следует использовать только значение «1».

Реализации могут дополнительно обеспечивать преобразования других нестандартных расширений 1984, где они имеют эквивалентные функции в стандартах 1988 (например, обозначение последней доставки), но в противном случае следует принимать и аннулировать такие элементы.

ПРИЛОЖЕНИЕ Е
(информационное)

ОБЩИЕ СВЕДЕНИЯ О НАЗНАЧЕНИИ И ПРИМЕНИМОСТИ ПРОФИЛЕЙ АМН1

Е.1 Введение

Настоящее приложение содержит некоторые сведения общего характера о назначении и применимости профилей АМН1, которые определены в настоящем многочастевом ФС.

Е.2 Профили обработки сообщений

Профили АМН применяются в оконечных системах, работающих в функциональной среде открытых систем взаимодействия (ОСВ) с форматом части распределенной СОС, функциональная среда которой базируется на ИСО/МЭК 10021 и эквивалентных рекомендациях Х.400 МККТТ.

Набор профилей АМН1 охватывает только унифицированный обмен сообщениями, т.е. те аспекты базовых стандартов в области СОС, которые не зависят от контекста особенностей обмена сообщениями (типа содержимого). Такие требования рассматриваются как «общие», и предполагается, что им удовлетворяют все реализации СОС.

В дальнейшем наборы профилей для специфических типов содержимого установят дополнительные требования, которые применимы к определенным сценариям использования СОС, представленным определенными классами агентов пользователей и содержимым протокола. В настоящее время определены следующие наборы профилей специфических типов содержимого:

- профили межперсонального обмена сообщениями АМН2, которые в первую очередь предназначены для обмена сообщениями между людьми;
- профили обмена сообщениями в рамках электронного обмена данными, которые разработаны для обеспечения электронного обмена данными между прикладными процессами.

Наборы профилей специфических типов содержимого (АМН2, АМН3 и те типы содержимого, которые будут определены в дальнейшем) охватывают как сквозную связь АП с АП (содержимое протокола и связанные функциональные возможности АП), так и использование услуг обработки сообщений (на основе требуемого соответствия надлежащим профилям АМН1 с дополнительным обеспечением любых требований специфических типов содержимого).

Также могут быть рекомендованы один или несколько профилей из набора АМН1 в целях установления соответствия без ссылок на любые типы содержимого, которые могут быть обеспечены.

Е.3 Профили АМН1

Каждый профиль АМН1 устанавливает определенную совокупность стандартов ВОС, предусматривающую одну из услуг СОС, реализуемых протоколами СОС:

а) АМН11 — протокол передачи сообщений (протокол Р1) между АПС;

б) АМН12 — протокол доступа СОС (протокол Р3) между удаленным АП и АПС, а также между удаленным ХС и АПС;

в) АМН13 — протокол доступа ХС (протокол Р7) между удаленным АП и ХС.

Е.4 Определение сценария АМН1

На рисунке Е.1 показано, как применяются профили АМН1 в наиболее используемых различных конфигурациях СОС, которые могут быть выполнены в виде раздельной или комбинированной реализации различных функциональных объектов СОС (т.е. АПС, АП, ХС).

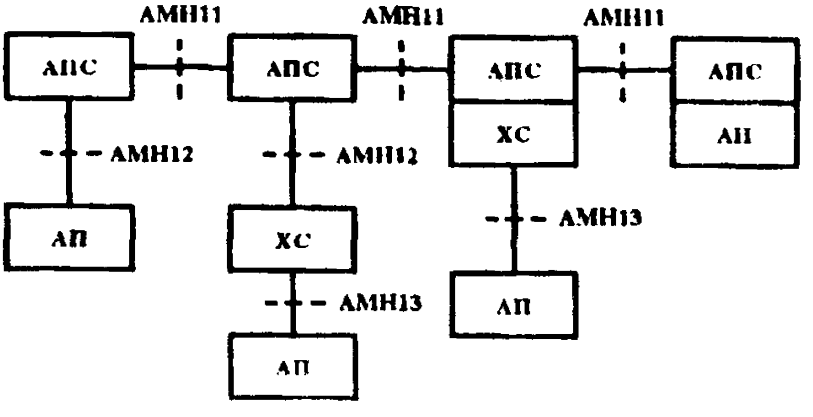

Рисунок Е.1 — Сценарий АМН1

Следует особо подчеркнуть, что профили АМН занимают в настоящее время в рамках таксономии профилей ВОС позицию согласно ГОСТ Р ИСО/МЭК ТО 10000. Следовательно, профили АМН1 только устанавливают взаимосвязь между функциональными объектами СОС в том случае, когда реализуется использование стандартного протокола передачи данных СОС. Другие формы представленного интерфейса, такие как стандартизованный программный интерфейс, не входят в предмет рассмотрения настоящего издания ГОСТ Р ИСО/МЭК МФС 10611. Таким образом, если «соразмещены» два или более функциональных объекта СОС (т.е. отсутствует связь через стандартный протокол передачи данных СОС), то определение интерфейса между функциональными объектами связано с необходимостью дополнительной спецификации.

Примечание — Следует отметить, что термин «соразмещенный» не раскрывает необходимого смысла, который обеспечивал бы функциональные объекты СОС на одной и той же физической платформе, но подчеркивает только то, что они не осуществляют связь через стандартные протоколы СОС. Таким образом, например, количество функциональных объектов СОС, распределенное по всей локальной области сети, может логически соразмещаться в рамках этого обсуждения. Рассмотренные выше различные конфигурации СОС, следовательно, не дают необходимого представления дискретных физических систем.

Спецификация конфигурации СОС, охватывающая соразмещенные функциональные объекты СОС, может быть достигнута обычной ссылкой только на один или несколько профилей, которые описывают внешнее поведение этой конфигурации. Таким образом, в случае соразмещенных АПС и АП может быть потребовано соответствие реализации профилю АМН11 (предусматривающему протокол передачи сообщений Р1) вместе с любым профилем специфического типа содержимого, предусматривающего функциональные возможности АП и протокол содержимого (такие

как АМН21). Подобным же образом в случае соразмещенных АПС и ХС может быть потребовано соответствие реализации профилю АМН1 вместе с профилем АМН13 (предусматривающим протокол доступа к ХС Р7).

Спецификация интерфейса между соразмещенными объектами СОС предполагается типичной и может быть нештатной только в том случае, если источником таких компонентов были затребованы различные поставщики. Такое требование может быть иногда в случае соразмещенных АПС и АП. Однако оно отличается от рассмотренного выше в случае соразмещенных АПС и ХС, которые типичным образом могут быть обеспечены одним и тем же поставщиком.

Спецификация интерфейса между соразмещенными АПС и АП может быть идеально определена ссылкой на специфический прикладной программный интерфейс. Однако, вполне возможно все же устанавливать соответствующие функциональные характеристики такого интерфейса, по крайней мере отчасти, ссылкой на профиль АМН12, который предусматривает протокол доступа АПС Р3. Такая ссылка может быть необходима для включения явной заявки, которая является требованием обеспечения абстрактной услуги АПС, и не требуется при реализации с использованием протокола Р3. Ссылка также может быть необходима при рассмотрении обеспечиваемых требований к отдельным элементам абстрактной услуги АПС.

Е.5 Модель профиля АМН1

На рисунке Е.2 приведены протоколы и услуги верхних уровней ВОС, предусмотренные профилями АМН1 для обеспечения функций СОС.

Прикладной уровень	СОС	ИСО/МЭК 10021—90 (части 1—6)
	СЭУО	ИСО/МЭК 9072—89
	СЭНП	ИСО/МЭК 9066—89
	СЭУА	ИСО 8650—88
Уровень представления		ИСО 8823—88, ИСО 8824—90, ИСО 8825—90
Сеансовый уровень		ИСО 8327—87

Рисунок Е.2 — Модель профиля АМН1

Е.6 Структура функционального стандарта

Набор профилей АМН1 установлен в функциональном стандарте (ГОСТ Р ИСО/МЭК МФС 10611), состоящем из следующих частей:

Часть 1. Обеспечение услуг систем обработки сообщений.

В этой части содержатся общие требования к обеспечению элементов услуг системы обработки сообщений (СОС) и устанавливаются соответствующие функциональные возможности, предусматриваемые набором профилей АМН1. Эти требования составляют часть прикладных функций унифицированного обмена сообщениями, как определено в частях настоящего функционального стандарта (ФС), который формирует общую основу для содержимого типозависимых ФС на СОС, планируемых к разработке. Такие требования во многих случаях применимы более чем к одному протоколу СОС

или могут быть отнесены к функциональным возможностям компонента, который, несмотря на то, что может быть проверен через протокол, как раз не относится к обеспечению протокола.

Часть 2. Спецификация сервисных элементов удаленных операций, надежной передачи, управления ассоциацией и протоколов уровня представления и сеансового уровня для использования в системах обработки сообщений.

В этой части устанавливается способ использования сервисного элемента удаленных операций (СЭУО), сервисного элемента надежной передачи (СЭНП), сервисного элемента управления ассоциацией (СЭУА), уровня представления и сеансового уровня для обеспечения требуемых функций верхних уровней ВОС для систем обработки сообщений (СОС).

Часть 3. Профиль АМН11. Передача сообщений (с использованием протокола Р1).

Эта часть охватывает вопросы передачи сообщений между агентами передачи сообщений (АПС), использующими протокол передачи сообщений Р1.

Часть 4. Профиль АМН12. Доступ к системе передачи сообщений (с использованием протокола Р3).

В этой части определяется доступ к системе передачи сообщений (СПС) с использованием протокола доступа к СПС Р3.

Часть 5. Профиль АМН13. Доступ к хранилищу сообщений (с использованием протокола Р7).

В этой части определяется доступ к хранилищу сообщений (ХС) с использованием протокола доступа к ХС Р7.

УДК 681.324:006.354 ОКС 35.100 П85 ОКСТУ 4002

Ключевые слова: обработка данных, обмен информацией, манипулирование данными, сообщения, процедуры передачи данных, процедуры управления, услуги

Редактор *Л.В. Афанасенко*
Технический редактор *О.Н. Власова*
Корректор *А.В. Прокофьева*
Компьютерная верстка *В.И. Грищенко*

Сдано в набор 16.11.95. Подписано в печать 16.02.96. Усл. печ. л. 3,23.
Усл. кр.-отт. 3,35 Уч.-изд. л. 3,45. Тираж 285 экз. С 3214. Зак. 64.

ИПК Издательство стандартов
107076, Москва, Колодезный пер., 14.
ЛР № 021007 от 10.08.95.
Набрано в Издательстве на ПЭВМ
Филиал ИПК Издательство стандартов — тип. "Московский печатник"
Москва, Лялин пер., 6

gost.e-ecolog.ru