ГОСУДАРСТВЕННЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

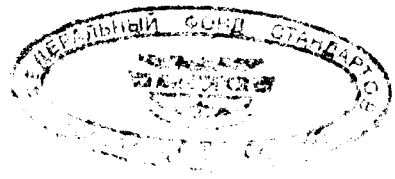
Информационная технология

ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ БАЗОВАЯ ЭТАЛОННАЯ МОДЕЛЬ

Часть 2.

Архитектура защиты информации

Издание официальное



БЗ 3—98/418

ГОССТАНДАРТ РОССИИ
Москва

Предисловие

1 РАЗРАБОТАН Московским научно-исследовательским центром (МНИЦ) Государственного комитета Российской Федерации по связи и информатизации

ВНЕСЕН Техническим комитетом ТК 22 «Информационные технологии»

2 ПРИНЯТ И ВВЕДЕН В ДЕЙСТВИЕ Постановлением Госстандарта России от 18 марта 1999 г. № 77

Настоящий стандарт содержит полный аутентичный текст международного стандарта ИСО 7498-2—89 «Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации»

3 ВВЕДЕН ВПЕРВЫЕ

Содержание

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационная технология

ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ БАЗОВАЯ ЭТАЛОННАЯ МОДЕЛЬ

Часть 2. Архитектура защиты информации

Information technology. Open Systems Interconnection. Basic Reference Model.
Part 2. Security Architecture

Дата введения 2000—01—01

Введение

ГОСТ Р ИСО/МЭК 7498 определяет базовую эталонную модель взаимосвязи открытых систем (ВОС). Настоящий стандарт устанавливает основы для обеспечения скоординированных разработок действующих и будущих стандартов по ВОС.

Назначение ВОС состоит в обеспечении такой взаимосвязи неоднородных вычислительных систем, которая позволила бы достичь эффективного обмена данными между прикладными процессами. В различных ситуациях необходимо обеспечение управляющих функций защиты информации, которой обмениваются прикладные процессы. Эти управляющие функции могут довести стоимость получения или модификации данных выше возможной ценности самих данных, либо привести к такому большому времени получения данных, по истечении которого ценность этих данных теряется.

Настоящий стандарт определяет общие архитектурные элементы, относящиеся к защите, которые могут соответствующим образом использоваться в тех случаях, когда необходима защита данных, передаваемых между открытыми системами. Настоящий стандарт устанавливает в рамках эталонной модели основные направления и ограничения по совершенствованию действующих стандартов или по разработке новых стандартов в области ВОС для обеспечения защиты обмениваемых данных и, тем самым, обеспечивает согласованный подход к защите информации в рамках ВОС.

Для понимания настоящего стандарта необходимо знать основные сведения по защите информации. Поэтому читателю, недостаточно подготовленному в этой области, рекомендуется сначала ознакомиться с приложением А.

Настоящий стандарт является расширением базовой эталонной модели в части аспектов защиты информации, которые являются общими архитектурными элементами для протоколов обмена данными, но не рассмотрены в базовой эталонной модели.

1 Область применения

Настоящий стандарт:

a) содержит общее описание тех услуг и соответствующих механизмов защиты, которые могут быть обеспечены эталонной моделью;

b) определяет те позиции в рамках эталонной модели, в которых могут обеспечиваться эти услуги и механизмы.

Настоящий стандарт расширяет область применения ГОСТ Р ИСО/МЭК 7498-1, охватывая вопросы защиты обмена данными между открытыми системами.

Основные услуги и механизмы защиты и их соответствующее размещение определено для всех уровней базовой эталонной модели. Кроме того, определены также архитектурные взаимоотношения услуг и механизмов защиты с базовой эталонной моделью. В оконечных системах, установках и организациях могут потребоваться дополнительные средства защиты. Эти средства используются в различных прикладных контекстах. Определение услуг защиты, необходимых для обеспечения этих дополнительных средств, не входит в предмет рассмотрения настоящего стандарта.

Издание официальное

Функции защиты в рамках ВОС рассмотрены с учетом только тех наблюдаемых аспектов маршрутов обмена данными, которые позволяют оконечным системам обеспечивать защищенную передачу информации между ними. Защита в рамках ВОС не касается средств защиты, необходимых в оконечных системах, установках и организациях, за исключением тех случаев, когда эти системы оказывают влияние на выбор и позицию услуг защиты, наблюдаемых в ВОС. Эти аспекты защиты могут быть стандартизированы, но вне области распространения стандартов по ВОС.

Настоящий стандарт дополняет концепции и принципы, установленные в ГОСТ Р ИСО/МЭК 7498-1, но не изменяет их. Настоящий стандарт не является ни спецификацией, ни основой для оценки соответствия действующих реализаций.

2 Нормативные ссылки

В настоящем стандарте использованы ссылки на следующие стандарты.

ГОСТ Р ИСО/МЭК 7498-1—99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть.1. Базовая модель

ГОСТ Р ИСО/МЭК 7498-4—99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 4. Основы административного управления

ГОСТ Р ИСО 8648—98 Информационная технология. Взаимосвязь открытых систем. Внутренняя организация сетевого уровня

3 Определения и сокращения

3.1 В настоящем стандарте используют следующие термины, определенные в ГОСТ Р ИСО/МЭК 7498-1:

a) **(N)-соединение;**
b) **(N)-передача данных;**
c) **(N)-логический объект;**
d) **(N)-средство;**
e) **(N)-уровень;**
f) **открытая система;**
g) **равноправные логические объекты;**
h) **(N)-протокол;**
j) **(N)-протокольный блок данных;**
k) **(N)-ретранслятор;**
l) **маршрутизация;**
m) **упорядочение;**
n) **(N)-услуга;**
p) **(N)-сервисный блок данных;**
q) **(N)-данные пользователя;**
r) **подсеть;**
s) **ресурс ВОС;**
t) **синтаксис передачи.**

3.2 Настоящий стандарт использует следующие термины соответствующих стандартов:

передача без установления соединения (ГОСТ Р ИСО/МЭК 7498-1)
оконечная система (ГОСТ Р ИСО/МЭК 7498-1)
блок данных (ГОСТ Р ИСО/МЭК 7498-1)
функции трансляции и маршрутизации (ГОСТ Р ИСО 8648)
информационная база административного управления (ИБАУ) (ГОСТ ИСО 7498-4)

Кроме того, в настоящем стандарте используют следующие сокращения:

ВОС — взаимосвязь открытых систем
СБД — сервисный блок данных
ИБАУ — информационная база административного управления
ИБАУЗ — информационная база административного управления защитой

3.3 В настоящем стандарте используют следующие определения:

3.3.1 **Управление доступом** — предотвращение несанкционированного использования какого-либо ресурса, включая предотвращение использования ресурса неполномочным способом.

3.3.2 **Список управления доступом** — список логических объектов, имеющих разрешение на доступ к ресурсу, вместе с перечнем их прав на доступ.

3.3.3 **Учетность** — свойство, обеспечивающее однозначное отслеживание собственных действий любого логического объекта.

3.3.4 **Активная угроза** — угроза преднамеренного несанкционированного изменения состояния системы.

Примечание — Примерами активных угроз, относящихся к защите информации, могут служить модификация сообщений, дублирование сообщений, вставка ложных сообщений, маскирование какого-либо логического объекта под санкционированный логический объект и отклонение услуги.

3.3.5 **Анализ процедур** — см. анализ процедур защиты.

3.3.6 **Данные трассировки** — см. данные трассировки защиты.

3.3.7 **Аутентификация** — см. аутентификация отправителя данных и равноправного логического объекта.

Примечание — В настоящем стандарте термин «аутентификация» не используется по отношению к целостности данных; вместо него используется термин «целостность данных».

3.3.8 **Информация аутентификации** — информация, используемая для установления подлинности запрашиваемой личности.

3.3.9 **Обмен аутентификацией** — механизм, предназначенный для подтверждения подлинности какого-либо логического объекта путем обмена информацией.

3.3.10 **Полномочие** — предоставление прав, гарантирующих доступ к ресурсам в соответствии с правами на доступ.

3.3.11 **Доступность** — свойство быть доступным и используемым по запросу со стороны уполномоченного логического объекта.

3.3.12 **Функциональная возможность** — маркер, используемый в качестве идентификатора какого-либо ресурса, овладение которым дает право на доступ к данному ресурсу.

3.3.13 **Канал** — маршрут передачи информации.

3.3.14 **Шифротекст** — данные, получаемые в результате использования шифрования. Семантическое содержимое полученных в результате шифрования данных недоступно.

Примечание — Шифротекст может сам по себе служить входом в процесс шифрования, в результате чего вырабатывается суперзашифрованный выход.

3.3.15 **Открытый текст** — смысловые данные, семантическое содержимое которых доступно.

3.3.16 **Конфиденциальность** — свойство, позволяющее не давать права на доступ к информации или не раскрывать ее неполномочным лицам, логическим объектам или процессам.

3.3.17 **Удостоверение личности** — данные, передаваемые для установления заявленной подлинности логического объекта.

3.3.18 **Криптоанализ** — анализ криптографической системы и/или ее входов и выходов с целью получения конфиденциальных переменных и/или чувствительных данных, включая открытый текст.

3.3.19 **Криптографическое контрольное значение** — информация, получаемая в результате выполнения криптографического преобразования (см. криптография) блока данных.

Примечание — Контрольное значение может быть получено путем выполнения одного или нескольких шагов и является результатом математической функции ключа и блока данных. Оно обычно используется для проверки целостности блока данных.

3.3.20 **Криптография** — дисциплина, охватывающая принципы, средства и методы преобразования данных для сокрытия их информационного содержимого, предотвращения их необнаруживаемой модификации и/или их несанкционированного использования.

Примечание — Криптография устанавливает методы, используемые при шифровании и дешифровании. Любое вторжение в криптографические принципы, средства или методы, представляет собой криптоанализ.

3.3.21 **Целостность данных** — способность данных не подвергаться изменению или аннулированию в результате несанкционированного доступа.

3.3.22 **Аутентификация отправителя данных** — подтверждение того, что отправитель полученных данных соответствует заявленному.

3.3.23 **Дешифрование** — процесс, обратный соответствующему обратимому процессу шифрования.

3.3.24 **Дешифрация** — см. дешифрование.

3.3.25 **Отклонение услуги** — предотвращение санкционированного доступа к ресурсам или задержка операций, критичных ко времени.

3.3.26 **Цифровая подпись** — дополнительные данные или криптографическое преобразование (см. криптография) какого-либо блока данных, позволяющие получателю блока данных убедиться в подлинности отправителя и целостности блока данных и защитить его от искажения с помощью, например, средств получателя.

3.3.27 **Шифрование** — криптографическое преобразование данных (см. криптография) для получения шифротекста.

Примечание — Шифрование может быть необратимым процессом, в связи с чем соответствующий процесс дешифрования невозможно реализовать.

3.3.28 **Шифрация** — см. шифрование.

3.3.29 **Межконцевое шифрование** — шифрование данных внутри или на стороне отправителя оконечной системы с соответствующим дешифрованием, выполняемое только внутри или на стороне получателя оконечной системы. (См. также позвенное шифрование.)

3.3.30 **Стратегия защиты, основанная на идентификации** — стратегия защиты информации, основанная на идентификаторах и/или атрибутах пользователей, группы пользователей или логических объектов, действующих от имени пользователей и доступных им ресурсов/логических объектов.

3.3.31 **Целостность** — см. целостность данных.

3.3.32 **Ключ** — последовательность символов, управляющая операциями шифрования и дешифрования.

3.3.33 **Административное управление ключом** — генерация, сохранение, распределение, удаление, каталогизирование и применение ключей в соответствии со стратегией защиты.

3.3.34 **Позвенное шифрование** — индивидуальное прикладное применение шифрования к данным на каждом звене системы обмена данных. (См. также межконцевое шифрование.)

Примечание — Позвенное шифрование подразумевает, что данные, передаваемые через логический объект ретранслятора, должны иметь формат открытого текста.

3.3.35 **Обнаружение манипуляции** — механизм, используемый для обнаружения возможной модификации блока данных (случайной или преднамеренной).

3.3.36. **Маскирование** — стремление какого-либо логического объекта выглядеть в виде другого логического объекта.

3.3.37 **Нотаризация** — регистрация данных доверенным третьим лицом, которое обеспечивает последующее подтверждение правильности их характеристик, таких как содержимое, отправитель, время и получатель.

3.3.38 **Пассивная угроза** — угроза несанкционированного раскрытия информации без изменения состояния системы.

3.3.39 **Пароль** — конфиденциальная информация аутентификации, обычно состоящая из строки знаков.

3.3.40 **Аутентификация равноправного логического объекта** — подтверждение того, что равноправный логический объект в какой-либо ассоциации является заявленным логическим объектом.

3.3.41 **Физическая защита** — средства, используемые для обеспечения физической защиты ресурсов от преднамеренной или случайной угрозы.

3.3.42 **Стратегия** — см. стратегия защиты.

3.3.43 **Собственность** — право отдельных лиц контролировать или влиять на сбор и хранение относящейся к ним информации и на определение тех, кем и для кого может быть раскрыта эта информация.

Примечание — Поскольку данный термин относится к праву отдельных лиц, он не может быть точно определен и его использования следует избегать, за исключением обоснованных случаев для запрашиваемой защиты.

3.3.44 **Самоотказ** — самоотрицание одного из логических объектов, участвующих в обмене данными, полного или частичного своего участия в этом обмене.

3.3.45 **Управление маршрутизацией** — применение правил в процессе маршрутизации по выбору или исключению конкретных сетей, звеньев данных или ретрансляторов.

3.3.46 **Стратегия защиты, основанная на правилах** — стратегия защиты, основанная на общих правилах, предъявляемых ко всем пользователям. Эти правила обычно основываются на сравнении чувствительности доступных ресурсов и обладании отдельными пользователями, группами пользователей или логическими объектами, действующими от имени пользователей, соответствующими атрибутами.

3.3.47 **Анализ процедур защиты** — независимый просмотр и анализ системных записей и активностей с целью проверки их адекватности системным управляющим функциям для обеспечения соответствия с принятой стратегией защиты и операционными процедурами, обнаружения пробелов в защите и выдачи рекомендаций по любым указанным изменениям в управлении, стратегии и процедурах.

3.3.48 **Данные трассировки защиты** — накопленные и готовые к использованию данные, предназначенные для детализации причины анализа процедур защиты.

3.3.49 **Метка защиты** — граничная метка, присваиваемая какому-либо ресурсу (в качестве которого может служить блок данных), которая именует или обозначает атрибуты защиты этого ресурса.

Примечание — Метка и/или присвоенное значение могут быть явными или неявными.

3.3.50 **Стратегия защиты** — набор критериев для обеспечения услуг защиты (см. также «стратегия защиты, основанная на идентификации» и «стратегия защиты, основанная на правилах»).

Примечание — Полная стратегия защиты неизбежно будет связана с решением многих вопросов, не входящих в сферу ВОС.

3.3.51 **Услуга защиты** — услуга, предоставляемая каким-либо уровнем взаимосвязанных открытых систем, которая обеспечивает адекватную защиту систем или процедур передачи данных.

3.3.52 **Избирательная защита поля** — защита конкретных полей внутри сообщения, подлежащего передаче.

3.3.53 **Чувствительность** — характеристика ресурса, которая определяет его ценность или важность и может учитывать его уязвимость.

3.3.54 **Подпись** — см. цифровая подпись.

3.3.55 **Угроза** — потенциальная возможность нарушения защиты.

3.3.56 **Анализ трафика** — заключение о состоянии информации на основе наблюдения за потоками трафика (наличие, отсутствие, объем, направление и частота).

3.3.57 **Конфиденциальность потока трафика** — услуга конфиденциальности, предназначенная для защиты от анализа трафика.

3.3.58 **Заполнение трафика** — генерация фиктивных сеансов обмена данными, фиктивных блоков данных и/или фиктивных данных в составе блоков данных.

3.3.59 **Доверительная функциональность** — функционирование, которое воспринимается правильным с точки зрения некоторого критерия, например, критерия, предъявляемого посредством стратегии защиты.

4 Обозначения

В настоящем стандарте используют ту же систему обозначений по уровням, что и в ГОСТ Р ИСО/МЭК 7498-1.

Термин «услуга», если не оговорено иное, используют в смысле «услуга защиты».

5 Общее описание услуг и механизмов защиты

5.1 Общее описание

В данном разделе рассмотрены услуги защиты, включенные в архитектуру защиты ВОС, и механизмы, реализующие эти услуги. Описанные ниже услуги защиты являются базовыми услугами защиты. На практике они должны вызываться на соответствующих уровнях и в соответствующих комбинациях, обычно совместно с услугами и механизмами, не входящими в область распространения ВОС, для обеспечения стратегии защиты и/или удовлетворения требований пользователя. Конкретные механизмы защиты могут использоваться для реализации комбинаций базовых услуг защиты. Практические реализации систем могут использовать для прямого привлечения конкретные комбинации базовых услуг защиты.

5.2 Услуги защиты

Ниже приведено описание услуг защиты, которые могут факультативно обеспечиваться в рамках базовой эталонной модели ВОС. Услуги аутентификации требуют проверки информации аутентификации, включая локально хранимую информацию и передаваемые данные для обеспечения аутентификации (удостоверения личности).

5.2.1 Аутентификация

Как описано ниже, эти услуги обеспечивают проверку подлинности равноправного логического объекта и отправителя данных.

5.2.1.1 *Аутентификация равноправного логического объекта*

Когда эта услуга предоставляется (N)-уровнем, она обеспечивает для (N+1)-логического объекта подтверждение того, что равноправный логический объект является заявленным (N+1)-логическим объектом.

Эта услуга предоставляется для использования во время установления соединения или в фазе передачи данных по соединению с целью подтверждения идентификаторов одного или нескольких логических объектов, соединенных с одним или несколькими другими логическими объектами. Эта услуга позволяет только в момент ее использования удостовериться в том, что какой-то логический объект не пытался замаскироваться под другой логический объект или несанкционированно воспроизвести предыдущее соединение. Возможно использование вариантов односторонней или взаимной аутентификации равноправного логического объекта с наличием или отсутствием проверки полного отказа и возможностью обеспечения различных степеней защиты.

5.2.1.2 *Аутентификация отправителя данных*

Когда эта услуга предоставляется (N)-уровнем, она обеспечивает для (N+1)-логического объекта подтверждение того, что отправитель данных является заявленным (N+1)-логическим объектом.

Услуга аутентификации отправителя данных обеспечивает подтверждение подлинности отправителя блока данных. Эта услуга не обеспечивает защиту от дублирования или модификации блоков данных.

5.2.2 Управление доступом

Эта услуга обеспечивает защиту от несанкционированного использования ресурсов, доступных через ВОС. Этими ресурсами, доступными через протоколы ВОС, могут быть как ресурсы, используемые в рамках ВОС, так и ресурсы, не входящие в область распространения ВОС. Данная услуга может применяться к различным видам доступа к ресурсам (например, использование ресурсов средств обмена данными, ресурсов чтения, записи или удаления информации, ресурсов выполнения обработки) или ко всем видам доступа к ресурсам.

Управление доступом должно рассматриваться в соответствии с различными стратегиями защиты (см. 6.2.1.1).

5.2.3 Конфиденциальность данных

Как описано выше, эти услуги обеспечивают защиту данных от их неполномочного раскрытия.

5.2.3.1 *Конфиденциальность в режиме с установлением соединения*

Эта услуга обеспечивает конфиденциальность всех данных (N)-пользователя, передаваемых по (N)-соединению.

Примечание — В зависимости от использования и уровня, защита всех данных может быть нецелесообразной, например, защита срочных данных или данных в запросе на установление соединения.

5.2.3.2 *Конфиденциальность в режиме без установления соединения*

Эта услуга обеспечивает конфиденциальность всех данных (N)-пользователя в одном (N)-СБД, передаваемом в режиме без установления соединения.

5.2.3.3 *Конфиденциальность выбранного поля*

Эта услуга обеспечивает конфиденциальность выбранных полей в составе данных (N)-пользователя, передаваемых по (N)-соединению или в одном (N)-СБД, передаваемом в режиме без установления соединения.

5.2.3.4 *Конфиденциальность потока трафика*

Эта услуга обеспечивает защиту информации, которая может быть получена в результате наблюдения потоков трафика.

5.2.4 Целостность данных

Эти услуги предотвращают активные угрозы и могут принимать одну из описанных ниже форм.

Примечание — В режиме с установлением соединения использование услуги аутентификации равноправного логического объекта в момент установления соединения и услуги целостности данных во время функционирования соединения может совместно обеспечивать подтверждение подлинности источника всех блоков данных, передаваемых по этому соединению, целостность этих блоков данных и может дополнительно обеспечить обнаружение дублирования блоков данных, например путем использования порядковых номеров.

5.2.4.1 *Целостность в режиме с установлением соединения с восстановлением*

Эта услуга обеспечивает целостность всех данных (N)-пользователя, передаваемых по (N)-соединению, и обнаруживает любую модификацию, вставку, стирание или воспроизведение любых данных внутри полной последовательности СБД (с попыткой восстановления).

5.2.4.2 *Целостность в режиме с установлением соединения без восстановления*

Эта услуга аналогична услуге, описанной в 5.4.2.1, но без попытки восстановления.

5.2.4.3 *Целостность выбранного поля в режиме с установлением соединения*

Эта услуга обеспечивает целостность выбранных полей внутри данных (N)-пользователя в составе какого-либо (N)-СБД, передаваемого по соединению, в виде определения формы искажения выбранных полей: модификации, вставки, удаления или воспроизведения.

5.2.4.4 *Целостность данных, передаваемых в режиме без установления соединения*

Когда эта услуга предоставляется (N)-уровнем, она обеспечивает целостность данных для запрашивающего (N+1)-логического объекта.

Эта услуга обеспечивает целостность одного СБД, передаваемого в режиме без установления соединения, и может принимать форму, определяющую, был ли смодифицирован принятый СБД. Дополнительно может быть предусмотрена ограниченная форма обнаружения воспроизведения.

5.2.4.5 *Целостность выбранного поля в режиме без установления соединения*

Эта услуга обеспечивает целостность выбранных полей внутри одного СБД, передаваемого в режиме без установления соединения, и определяет, были ли смодифицированы выбранные поля.

5.2.5 Безотказность

Эта услуга может принимать одну или обе следующие формы.

5.2.5.1 *Безотказность с подтверждением отправителя*

Получатель данных обеспечивается проверкой отправителя данных. Эта услуга защищает от любой попытки отправителя ложно отрицать передачу данных или их содержимое.

5.2.5.2 *Безотказность с подтверждением доставки*

Передатчик данных обеспечивается подтверждением доставки данных. Эта услуга защищает от любой последующей попытки получателя ложно отрицать получение данных или их содержимое.

5.3 **Специальные механизмы защиты**

Следующие механизмы могут входить в состав соответствующего (N)-уровня для обеспечения некоторых услуг, описанных в 5.2.

5.3.1 Шифрование

5.3.1.1 Шифрование может обеспечивать конфиденциальность либо данных, либо информации потока трафика, и может принимать участие в дополнении ряда других механизмов защиты, описанных в последующих разделах.

5.3.1.2 Алгоритмы шифрования могут быть обратимыми и необратимыми. Существуют два вида общей классификации обратимых механизмов шифрования:

a) симметричное шифрование (т.е. секретный ключ), при котором знание ключа шифрования предполагает знание ключа дешифрования, и наоборот;

b) асимметричное шифрование (т.е. ключ общего пользования), при котором знание ключа шифрования не предполагает знание ключа дешифрования, и наоборот. Два ключа такой системы называются иногда «ключ общего пользования» и «личный ключ».

Алгоритмы необратимого шифрования могут использовать или не использовать ключ. При использовании ключа он может быть общего пользования либо секретным.

5.3.1.3 Наличие механизма шифрования предполагает использование механизма административного управления ключом, за исключением случаев применения некоторых алгоритмов необратимого шифрования. Некоторые основные положения методов административного управления ключом приведены в 8.4.

5.3.2 Механизмы цифровой подписи

Эти механизмы определяют две процедуры:

a) подпись блока данных;

b) верификация подписанного блока данных.

Первый процесс использует информацию, которая является личной (т.е. единственной и конфиденциальной) по отношению к подписавшему лицу. Второй процесс использует процедуры и информацию, которые являются общественно доступными, но из которых не может быть выделена личная информация подписавшего лица.

5.3.2.1 Процесс подписания включает либо шифрование блока данных, либо выработку криптографического контрольного значения блока данных путем использования в качестве личного ключа личной информации подписавшего лица.

5.3.2.2 Процесс верификации включает использование процедур и информации общего пользования с целью определения образования подписи с помощью личной информации подписавшего лица.

5.3.2.3 Существенной характеристикой механизма подписи является то, что подпись может быть произведена только с использованием личной информации подписавшего лица. Таким образом, при верификации подписи можно впоследствии в любой момент времени доказать третьему лицу (например, судье или арбитру), что только единственный обладатель личной информации мог произвести эту подпись.

5.3.3 Механизмы управления доступом

5.3.3.1 Эти механизмы могут использовать подтвержденную подлинность логического объекта или информации о логическом объекте (например, принадлежность к известному множеству логических объектов) или возможностей логического объекта с целью определения и присвоения права этого логического объекта на доступ. Если логический объект пытается использовать неполномочный ресурс или полномочный ресурс с запрещенным для него типом доступа, то функция управления доступом должна отклонить эту попытку и может дополнительно уведомить об этом инциденте с целью генерации сигнала тревоги и/или ее регистрации в качестве части данных отслеживания защиты. Любое уведомление передатчика об отклонении при передаче данных без установления соединения может обеспечиваться только в результате управления доступом, возлагаемого на отправителя данных.

5.3.3.2 Механизмы управления доступом могут, например, базироваться на использовании одного или нескольких следующих факторов:

a) информационных баз управления доступом, где поддерживаются права доступа равноправных логических объектов. Эта информация может обслуживаться санкционированными центрами или логическими объектами, к которым осуществляется доступ, и может иметь форму списка управления доступом или матрицы с иерархической или распределенной структурой. Этот фактор предполагает, что аутентификация равноправного логического объекта обеспечена;

b) информации аутентификации, например, паролей, обладание и последующее представление которых очевидно из полномочий логического объекта, осуществляющего доступ;

c) возможностей, обладание и последующее представление которых очевидно вытекает из наличия у логического объекта или ресурса права на доступ, определяемого данной возможностью.

Примечание — Возможность не должна быть ложной и должна быть присвоена доверительным образом;

d) меток защиты, которые при присвоении какому-либо логическому объекту должны использоваться для разрешения или отклонения права на доступ обычно в соответствии со стратегией защиты;

e) времени попытки получения доступа;

f) маршрута попытки получения доступа;

g) длительности доступа.

5.3.3.3 Механизмы управления доступом могут использоваться на любом конце ассоциации обмена данными и/или в любом ее промежуточном пункте.

Функции управления доступом, задействованные у отправителя или в любом промежуточном пункте, используются для определения права передатчика на обмен данными с получателем и/или для использования запрашиваемых ресурсов связи.

Требования, предъявляемые к механизмам управления доступом в равноправных уровнях на стороне получателя для передачи данных в режиме без установления соединения, должны быть известны заранее отправителю и должны быть зарегистрированы в информационной базе административного управления защитой (см. 6.2 и 8.1).

5.3.4 Механизмы целостности данных

5.3.4.1 Существует два аспекта целостности данных: целостность единичного блока данных или поля и целостность потока блоков данных или полей. В общем случае для обеспечения этих двух типов услуги целостности используются различные механизмы, хотя обеспечение второго типа этой услуги без первого непрактично.

5.3.4.2 Определение целостности единичного блока данных включает два процесса, один из которых выполняется на передающем логическом объекте, а другой — на принимающем. Передающий логический объект добавляет к блоку данных контрольную величину, которая является функцией самих данных. Эта контрольная величина может быть дополнительной информацией, например, кодом проверки блока или криптографическим контрольным значением, и может быть сама зашифрована. Принимающий логический объект генерирует соответствующую контрольную величину и сравнивает ее с принятой контрольной величиной для определения возможной модификации данных в процессе их передачи. Этот механизм сам по себе не может защитить от

воспроизведения отдельного блока данных. На соответствующих уровнях архитектуры обнаружение манипуляции может привести к действию процедуры восстановления (например, путем повторной передачи или исправления ошибок) на данном или вышерасположенном уровне.

5.3.4.3 Для передачи данных в режиме с установлением соединения защита целостности последовательности блоков данных (т.е. защита от нарушения последовательности, потери, воспроизведения, вставок или модификации данных) дополнительно требует некоторых форм явного упорядочения, таких как порядковая нумерация, отметки времени или организация криптографических цепочек.

5.3.4.4 При передаче данных в режиме без установления соединения могут быть использованы отметки времени с целью обеспечения ограниченной формы защиты против воспроизведения отдельных блоков данных.

5.3.5 Механизм обмена информацией аутентификации

5.3.5.1 Для обеспечения обмена информацией аутентификации могут использоваться некоторые из перечисленных ниже методов:

a) использование информации аутентификации, такой как пароли, которые обеспечиваются передающим и проверяются принимающим логическими объектами;

b) методы криптографии;

c) использование характеристик и/или принадлежностей логического объекта.

5.3.5.2 Указанные механизмы могут содержаться в (N)-уровне для аутентификации равноправного логического объекта. Если механизму не удалось провести аутентификацию логического объекта, это приведет к отклонению или разъединению соединения и может также вызвать появление записи в данных отслеживания защиты и/или к уведомлению центра административного управления защитой.

5.3.5.3 При использовании криптографических методов они могут сочетаться с протоколами «квитирования» с целью защиты от воспроизведения (т.е. для обеспечения жизнеспособности).

5.3.5.4 Выбор методов обмена информацией аутентификации должен зависеть от обстоятельств их использования. В большинстве случаев эти методы следует использовать в сочетании со следующими процедурами:

a) установка отметок времени и синхронизированные часы;

b) двух- и трехнаправленное квитирование (для односторонней и взаимной аутентификации, соответственно);

c) услуги без самоотвода, обеспечиваемые цифровой подписью, и/или механизмами нотаризации.

5.3.6 Механизм заполнения трафика

Механизм заполнения трафика может использоваться для обеспечения различных уровней защиты от анализа трафика. Этот механизм может быть эффективным только в том случае, если заполнение трафика защищается услугой конфиденциальности.

5.3.7 Механизм управления маршрутизацией

5.3.7.1 Маршруты могут выбираться либо динамически, либо путем такого предварительного распределения, которое использует только физически защищенные подсети, ретрансляторы или звенья данных.

5.3.7.2 При обнаружении постоянных попыток манипуляции данными оконечные системы могут передать поставщику сетевой услуги команду на установление соединения через другой маршрут.

5.3.7.3 Прохождение данных с определенными метками защиты через соответствующие подсети, ретрансляторы или звенья может быть запрещено стратегией защиты. Кроме того, инициатор соединения (или передатчик блока данных без установления соединения) может установить запрет на использование маршрутов, что требует исключения из маршрута заданных подсетей, звеньев данных или ретрансляторов.

5.3.8 Механизм нотаризации

Характеристики данных, передаваемых между двумя или несколькими объектами, такие как целостность, отправитель, время и получатель, могут быть гарантированы путем использования механизма нотаризации. Гарантия обеспечивается третьим участником-нотариусом, который получает полномочия от взаимодействующих логических объектов и обладает информацией, необходимой для предоставления запрашиваемой гарантии посредством метода, допускающего проверку. Каждый сеанс обмена данными может использовать механизмы цифровой подписи, шифрования и аутентификации в соответствии с видом услуги, предоставляемой нотариусом. При использовании

такого механизма нотаризации данные передаются между двумя взаимодействующими объектами с помощью защищенных сеансов связи и через нотариуса.

5.4 **Общеархитектурные механизмы защиты**

В данном подразделе описан ряд механизмов, которые не являются специфичными для любой конкретной услуги. Так, в разделе 7 эти механизмы описаны неявно, как принадлежащие любому отдельному уровню. Некоторые из этих общеархитектурных механизмов защиты могут рассматриваться как аспекты административного управления защитой (см. также раздел 8). Назначение этих механизмов в основном прямо зависит от запрашиваемой степени защиты.

5.4.1 Доверительная функциональность

5.4.1.1 Доверительная функциональность должна использоваться для расширения области применения или повышения эффективности других механизмов защиты. Любая функциональность, непосредственно обеспечивающая механизмы защиты или доступ к ним, должна быть заслуживающей доверия.

5.4.1.2 Процедуры, используемые для гарантии включения таких доверительных функциональностей в соответствующие аппаратные и программные средства, не входят в предмет рассмотрения настоящего стандарта и в любом случае зависят от уровня воспринимаемой угрозы и ценности защищаемой информации.

5.4.1.3 Как правило, такие процедуры дорогостоящи и сложны в реализации. Эти проблемы могут быть минимизированы путем выбора архитектуры, позволяющей реализовать функции защиты в модулях, которые могут быть выполнены отдельно от функций, не связанных с защитой, и защищены от них.

5.4.1.4 Любая защита ассоциаций, устанавливаемых выше того уровня, на котором предусматривается эта защита, должна обеспечиваться другими средствами, например, соответствующей доверительной функциональностью.

5.4.2 Метки защиты

Ресурсы, включающие элементы данных, могут иметь связанные с ними метки защиты, например, метки, предназначенные для указания уровня чувствительности. Часто с транзитными данными необходимо передавать соответствующие метки защиты. Метка защиты может представлять собой дополнительные данные, связанные с передаваемыми данными, или может быть неявной, например, она может предполагаться при использовании специального ключа для шифрования данных или контекста данных, включающего описание отправителя или маршрута. Неявные метки защиты должны быть точно идентифицированы для обеспечения их соответствующей проверки. Кроме того, они должны быть надежно связаны с соответствующими данными.

5.4.3 Обнаружение события

5.4.3.1 Обнаружение события, относящегося к защите, состоит в выявлении видимых нарушений защиты и может также представлять собой обнаружение «нормальных» событий, таких как успешное получение права на доступ (или подключение к системе). События, относящиеся к защите, могут распознаваться логическими объектами в рамках ВОС, включающими механизмы защиты. Спецификация параметров, составляющих какое-либо событие, обеспечивается административным управлением обработкой событий (см. 8.3.1). Обнаружение различных событий, относящихся к защите, может вызвать, например, одно или несколько следующих действий:

a) выдача локального сообщения о событии;
b) выдача удаленного сообщения о событии;
c) регистрация события в системном журнале (см. 5.4.3);
d) действие процедуры восстановления (см. 5.4.4).

Примерами событий, относящихся к защите, могут служить следующие ситуации:

a) нарушение специальной защиты;
b) выбранное специфическое событие;
c) переполнение счетчика количества ситуаций.

5.4.3.2 Стандартизация поля обнаружения события должна учитывать передачу информации, связанной с выдачей сообщения о событии и его регистрацией, а также синтаксическое и семантическое определения, используемые для передачи сообщения о событии и его регистрации.

5.4.4 Данные отслеживания защиты

5.4.4.1 Данные отслеживания защиты обеспечивают надежный механизм защиты, поскольку они предоставляют потенциальную возможность обнаружения и исследования пробелов защиты путем выдачи последующего анализа процедур защиты. Анализ процедур защиты предусматривает независимый просмотр и анализ системных записей и активностей для проверки адекватности

системным функциям управления, обеспечения соответствия с принятой стратегией защиты и операционными процедурами, оценки нарушения защиты и выдачи рекомендаций о любых задаваемых изменениях в функциях управления, стратегии и процедурах защиты. Анализ процедур защиты требует регистрации информации, относящейся к защите, в виде данных отслеживания защиты, а также анализа информации, извлекаемой из данных отслеживания защиты, и уведомления о его результатах. Документирование или регистрация в системном журнале рассматриваются в качестве механизма защиты и описаны в настоящем разделе. Анализ и генерацию сообщений рассматривают в качестве функции административного управления защитой (см. 8.3.2).

5.4.4.2 Сбор информации о данных отслеживания защиты может удовлетворять различным требованиям путем определения типов событий, относящихся к защите и подлежащих регистрации (например, видимые нарушения защиты или завершение успешных операций).

Сведения о наличии данных отслеживания защиты могут служить в качестве сдерживающего фактора для некоторых потенциальных источников нарушения защиты.

5.4.4.3 Организация данных отслеживания защиты ВОС должна рассматриваться с учетом того, какая информация должна дополнительно записываться в системный журнал, при каких обстоятельствах эта информация должна документироваться, а также какие синтаксические и семантические определения должны использоваться для обмена информацией о данных отслеживания защиты.

5.4.5 Процедура восстановления защиты

5.4.5.1 Процедура восстановления защиты связана с запросами от таких механизмов, как функции обработки событий и административного управления, и выполняет действия по восстановлению в соответствии с используемым набором правил. Эти действия по восстановлению могут относиться к одному из следующих трех типов:

a) немедленные;
b) временные;
c) долгосрочные.

Например

Немедленные действия могут привести к немедленному прерыванию операций, подобному разъединению соединения.

Временные действия могут привести к временной неработоспособности какого-либо логического объекта.

Долгосрочные действия могут привести к занесению логического объекта в «черный список» или к изменению ключа.

5.4.5.2 Объектами стандартизации являются протоколы действий процедуры восстановления и административного управления восстановлением защиты (см. 8.3.3).

5.5 Иллюстрация взаимоотношений услуг и механизмов защиты

В таблице 1 перечислены механизмы, которые по отдельности или в сочетании с другими механизмами рассматриваются в качестве возможных в некоторых случаях для обеспечения каждой услуги. Эта таблица представляет собой обзор таких взаимоотношений и не является исчерпывающей. Услуги и механизмы, приведенные в этой таблице, описаны в 5.2 и 5.3. Более подробное описание взаимоотношений приведено в разделе 6.

Таблица 1 — Механизмы обеспечения услуг

Механизмы / Услуги	Шифрование	Цифровая подпись	Управление доступом	Целостность данных	Обмен аутентификацией	Заполнение трафика	Управление маршрутизацией	Нотаризация
Аутентификация равноправного логического объекта	Да	Да	*	*	Да	*	*	*
Аутентификация отправителя данных	Да	Да	*	*	*	*	*	*
Услуга управления доступом	*	*	Да	*	*	*	*	*
Конфиденциальность в режиме с установлением соединения	Да	*	*	*	*	*	Да	*

Окончание таблицы 1

Механизмы / Услуги	Шифрование	Цифровая подпись	Управление доступом	Целостность данных	Обмен аутентификацией	Заполнение трафика	Управление маршругизацией	Нотаризация
Конфиденциальность в режиме без установления соединения	Да	*	*	*	*	*	Да	*
Конфиденциальность выбранного поля	Да	*	*	*	*	*	*	*
Конфиденциальность потока трафика	Да	*	*	*	*	Да	Да	*
Целостность в режиме с установлением соединения с восстановлением	Да	*	*	Да	*	*	*	*
Целостность в режиме с установлением соединения без восстановления	Да	*	*	Да	*	*	*	*
Целостность выборочного поля в режиме с установлением соединения	Да	*	*	Да	*	*	*	*
Целостность в режиме без установления соединения	Да	Да	*	Да	*	*	Да	*
Целостность выборочного поля в режиме без установления соединения	Да	Да	*	Да	*	*	*	*
Безотказность отправителя	*	Да	*	Да	*	*	*	Да
Безотказность получателя	*	Да	*	Да	*	*	*	Да

Обозначения
Да — механизм считается возможным для использования как в отдельности, так и в сочетании с другими механизмами;
* — механизм считается невозможным для использования.

6 Взаимодействие услуг, механизмов и уровней

6.1 Принципы уровневой структуры защиты

6.1.1 Для определения распределения услуг защиты по уровням и последующего размещения по уровням механизмов защиты используются следующие принципы:

a) количество альтернативных способов предоставления услуги должно быть минимальным;

b) допускается построение систем защиты путем обеспечения услуг защиты на нескольких уровнях;

c) дополнительные функциональные возможности, необходимые для защиты, не обязательно должны дублировать существующие функции ВОС;

d) должно быть исключено нарушение независимости уровня;

e) объем доверительной функциональности должен быть минимальным;

f) в тех случаях, когда логический объект зависит от механизма защиты, обеспечиваемого каким-либо логическим объектом нижерасположенного уровня, любые промежуточные уровни должны быть построены таким образом, чтобы нарушение защиты было практически невозможным;

g) там, где это возможно, дополнительные функции защиты уровня должны быть определены таким образом, чтобы реализация отдельного(ых) самостоятельного(ых) модуля(ей) была исключена;

h) настоящий стандарт предполагается применять к открытым системам, которые состоят из оконечных систем, содержащих все семь уровней, и к ретрансляционным системам.

6.1.2 На каждом уровне могут потребоваться модификации определений услуг с целью обеспечения запросов для услуг защиты, независимо от того, обеспечиваются ли запрашиваемые услуги на данном или нижерасположенном уровнях

6.2 **Модель привлечения, административного управления и использования защищенных (N)-услуг**

Данный подраздел должен рассматриваться совместно с разделом 8, который содержит общее описание принципов административного управления защитой. Предполагается, что механизмы и услуги защиты могут быть активизированы логическим объектом административного управления через интерфейс административного управления и/или путем привлечения услуги.

6.2.1 Определение средств защиты для сеанса связи

6.2.1.1 *Общие положения*

В данном подразделе приведено описание привлечения средств защиты для сеансов обмена данными в режимах с установлением и без установления соединения. В случае сеансов обмена данными в режиме с установлением соединения, услуги защиты обычно запрашиваются/подтверждаются во время установления соединения. В случае привлечения услуги защиты в режиме без установления соединения защита запрашивается/подтверждается для каждого примитива БЛОК-ДАННЫХ запрос.

Для упрощения последующего описания термин «запрос услуги» будет в дальнейшем означать либо установления соединения, либо передачу примитива БЛОК-ДАННЫХ запрос. Привлечение защиты для выбранных данных может осуществляться путем запроса защиты выбранных полей. Например, эта процедура может быть выполнена путем установления нескольких соединений, каждому из которых может быть присвоен различный тип или уровень защиты.

Такая архитектура защиты взаимоувязывает различные стратегии защиты, включая те, которые основаны на правилах, на идентификации и смешанного типа. Архитектура защиты также приспосабливает защиту, на которую налагаются административные требования, динамически выбираемую защиту, а также защиту смешанного типа.

6.2.1.2 *Запросы услуги*

При каждом запросе (N)-услуги (N+1)-логический объект может запросить необходимый тип желаемой защиты. Запрос (N)-услуги должен определить услугу защиты вместе с параметрами и любой дополнительной информацией, относящейся к защите (например, информацией о чувствительности и/или о метках защиты), для обеспечения заданного типа желаемой защиты.

Перед каждым сеансом обмена данными (N+1)-уровень должен обратиться к информационной базе административного управления защитой (ИБАУЗ) (см. 8.1). ИБАУЗ должна содержать информацию о требованиях, предъявляемых к защите административным управлением, относительно (N+1)-логического объекта. Доверительная функциональность необходима для усиления этих требований, предъявляемых к защите со стороны административного управления.

Обеспечение средств защиты во время сеанса обмена данными в режиме с установлением соединения может потребовать согласования запрашиваемых услуг защиты. Процедуры, необходимые для согласования механизмов и параметров защиты, могут выполняться в виде отдельной процедуры или являться неотъемлемой частью обычной процедуры установления соединения.

Если согласование выполняется в виде отдельной процедуры, результаты согласования (т.е. согласованный тип механизма защиты и параметры защиты, необходимые для обеспечения соответствующих услуг защиты) вводятся в ИБАУЗ (см. 8.1).

Если согласование выполняется как неотъемлемая часть обычной процедуры установления соединения, результаты согласования между (n)-логическими объектами будут временно сохранены в ИБАУЗ. Перед согласованием каждый (n)-логический объект должен иметь доступ к ИБАУЗ для получения информации, необходимой для согласования.

(N)-уровень должен отклонить запрос услуги, если он не подчиняется требованиям административного управления, которые записываются в ИБАУЗ для (N+1)-логического объекта.

(N)-уровень должен также дополнительно к запрашиваемым услугам защиты привлекать любые услуги защиты, которые определены в ИБАУЗ как обязательные для достижения заданного типа желаемой защиты.

Если (N+1)-логический объект не определяет заданного типа желаемой защиты, (N)-уровень будет подчиняться стратегии защиты в соответствии с информацией, записанной в ИБАУЗ. Это может привести к обмену данными с использованием средств защиты по умолчанию, предусмотренных в рамках, определенных для (N+1)-логического объекта в ИБАУЗ.

6.2.2 Предоставление услуг защиты

После определения комбинации требований к защите со стороны административного управления и динамически выбранных требований, как описано в 6.2.1, (N+1)-уровень будет пытаться обеспечить, как минимум, заданный тип желаемой защиты. Это может быть достигнуто одним или двумя следующими методами:

a) привлечение механизмов защиты непосредственно внутри (N)-уровня;

b) запрос услуг защиты из (N-1)-уровня. В этом случае область применения защиты должна быть расширена на (N)-услугу путем сочетания доверительной функциональности и/или специальных механизмов защиты в (N)-уровне.

Примечание — Последнее необязательно означает, что все функциональные возможности на (N)-уровне должны быть доверительными.

Таким образом, (N)-уровень определяет свою способность обеспечить запрашиваемую желаемую защиту. Если он не имеет таких возможностей, обмен данными не происходит.

6.2.2.1 *Установление защищенного (N)-соединения*

Последующее рассмотрение касается предоставления услуг внутри (N)-уровня (в отличие от использования функций (N-1)-услуг).

В некоторых протоколах для обеспечения гарантированной желаемой защиты решающей является последовательность операций.

Предоставляются следующие услуги:

a) контроль исходящего доступа;

(N)-уровень может предусматривать средства контроля исходящего доступа, т.е. он может локально определять (со стороны ИБАУЗ), разрешено ли ему установление защищенного (N)-соединения.

b) аутентификация равноправного логического объекта;

Если желаемая защита включает аутентификацию равноправного логического объекта или если известно (со стороны ИБАУЗ), что (N)-объект получателя будет запрашивать аутентификацию равноправного логического объекта, то должен иметь место обмен информацией аутентификации. Выполнение последней процедуры может потребовать использования двух- или трехнаправленного квитирования для обеспечения запрашиваемой односторонней или взаимной аутентификации.

Иногда обмен информацией аутентификации может происходить в рамках обычных процедур установления (N)-соединения. При других обстоятельствах обмен информацией аутентификации может быть выполнен отдельно от процедуры установления (N)-соединения.

c) услуга управления доступом;

(N)-логический объект получателя или промежуточные логические объекты могут подчиняться требованиям управления доступом. Если удаленный механизм управления доступом запрашивает специальную информацию, то инициирующий (N)-логический объект предоставляет эту информацию внутри протокола (N)-уровня или через каналы административного управления.

d) конфиденциальность;

Если была выбрана услуга полной или избирательной конфиденциальности, должно быть установлено защищенное (N)-соединение. Эта процедура может включать установление соответствующих рабочих ключей и согласование криптографических параметров данного соединения. Это может быть достигнуто путем выполнения предварительных действий в процессе обмена информацией аутентификации или с помощью отдельного протокола.

e) целостность данных;

Если была выбрана целостность всех (N)-пользовательских данных с восстановлением или без него либо целостность выбранных полей, должно быть установлено защищенное (N)-соединение. Это соединение может быть тем же, которое установлено для обеспечения услуги конфиденциальности и может обеспечивать аутентификацию. К данной услуге применимы те же самые требования, что и к услуге конфиденциальности для защищенного (N)-соединения;

f) услуга «безотказность».

Если была выбрана услуга «безотказность» с подтверждением отправителя, то должны быть установлены соответствующие криптографические параметры или защищенное соединение с логическим объектом нотаризации.

Если была выбрана услуга «безотказность» с подтверждением доставки, то должны быть установлены соответствующие параметры (которые отличаются от запрашиваемых параметров при услуге безотказности с подтверждением отправителя) или защищенное соединение с логическим объектом нотаризации.

Примечание —Установление защищенного (N)-соединения может оказаться безуспешным в связи с потерей согласованности криптографических параметров (возможно с отсутствием обладания соответствующими ключами) или из-за отклонения такого соединения со стороны механизма управления доступом.

6.2.3 Функционирование защищенного (N)-соединения

6.2.3.1 В фазе передачи данных по защищенному (N)-соединению должны обеспечиваться согласованные услуги защиты.

Следующие услуги должны наблюдаться на границе (N)-услуги:

a) аутентификация равноправного логического объекта (по интервалам);

b) защита выбранных полей;

c) уведомление об активном вторжении (например, когда происходит манипуляция данных и предоставляемая услуга представляет собой «Целостность в режиме с установлением соединения без восстановления» см. 5.2.4.2).

Кроме того, могут потребоваться следующие услуги:

a) регистрация данных отслеживания защиты;

b) обнаружение и обработка события.

6.2.3.2 Следующие услуги используются для выборочного применения:

a) конфиденциальность;

b) целостность данных (возможно с аутентификацией);

c) безотказность (получателя или отправителя).

Примечания

1 Предлагается использовать два метода маркировки тех элементов данных, выбранных применяемой услугой. Первый метод включает использование строгой типизации. Предполагается, что уровень представления будет распознавать некоторые из таких типов, которые требуют применения определенных услуг защиты. Второй метод предполагает некоторую форму присвоения признаков отдельным элементам данных, требующих применения специальных услуг защиты.

2 Предполагается, что одна из причин обеспечения выборочного применения услуг защиты «безотказность» может вытекать из следующего сценария. Перед тем, как оба (N)-логических объекта придут к согласию, что окончательная версия элемента данных является обоюдно приемлемой, между ними по ассоциации происходит некоторая форма диалога согласования. В этот момент намеченный получатель может запросить отправителя применить услуги «безотказность» (с подтверждением как отправителя, так и доставки) для получения окончательной согласованной версии элемента данных. Отправитель запрашивает и получает эти услуги, передает элемент данных и впоследствии принимает уведомление о приеме и подтверждении получателем указанного элемента данных. Услуги защиты «безотказность» оповещают отправителя и получателя элемента данных о том, что этот элемент был успешно принят.

3 Обе услуги защиты «безотказность» (т.е. с подтверждением отправителя и доставки) привлекаются инициатором.

6.2.4 Обеспечение защищенной передачи данных в режиме без установления соединения

Не все услуги защиты, используемые в протоколах режима с установлением соединения, доступны для протоколов режима без установления соединения. В частности, на верхних уровнях, работающих в режиме с установлением соединения, должна быть предусмотрена, при необходимости, защита от удалений, вставок и воспроизведений. С помощью механизма установления отметок времени может обеспечиваться ограниченная защита от угрозы воспроизведений. Кроме того, многие другие услуги защиты не способны обеспечить такую же степень усиления защиты, которая может быть достигнута протоколами режима с установлением соединения.

К услугам защиты, которые применимы для передачи данных в режиме без установления соединения, относятся следующие:

a) аутентификация равноправного объекта (см. 5.2.1.1);

b) аутентификация отправителя данных (см. 5.2.1.2);

c) услуга управления доступом (см. 5.2.2);

d) конфиденциальность в режиме без установления соединения (см. 5.2.3.2);

e) конфиденциальность выбранных полей (см. 5.2.3.3);

f) целостность данных в режиме без установления соединения (см. 5.2.4.4);

g) целостность выбранных полей в режиме без установления соединения (см. 5.2.4.5);

h) услуга защиты «безотказность» с подтверждением отправителя (см. 5.2.5.1).

Эти услуги обеспечиваются с помощью механизмов шифрования, цифровой подписи, управления доступом, маршрутизации, целостности данных и/или нотаризации (см. 5.3).

Инициатор передачи данных в режиме без установления соединения должен обеспечить, чтобы его отдельный СБД содержал всю информацию, необходимую для распознавания этого СБД на стороне получателя.

7 Размещение услуг и механизмов защиты

В данном разделе определены те услуги защиты, которые должны обеспечиваться в рамках базовой эталонной модели ВОС, и описаны методы получения этих услуг. Обеспечение любой услуги защиты является факультативным и зависит от предъявляемых требований.

Если в данном разделе конкретная услуга защиты определена как факультативно обеспечиваемая определенным уровнем, то эта услуга обеспечивается механизмами защиты, функционирующими внутри этого уровня, если не оговорено иное. Как описано в разделе 6, многие уровни могут предлагать обеспечение конкретных услуг защиты. Такие уровни не всегда предусматривают услуги защиты внутри самих себя, однако они могут использовать соответствующие услуги защиты, обеспечиваемые нижерасположенными уровнями. Даже если в рамках какого-то уровня не предусмотрено никаких услуг защиты, определения услуг этого уровня могут потребовать некоторой модификации, чтобы позволить выдачу на нижерасположенный уровень запросов на услуги защиты.

Примечания

1 Общеархитектурные механизмы защиты (см. 5.4) не рассматриваются в настоящем разделе.

2 Выбор позиции механизмов шифрования для прикладных применений рассмотрен в приложении С.

7.1 Физический уровень

7.1.1 Услуги

На физическом уровне предусматриваются только следующие услуги защиты, используемые как по отдельности, так и в сочетании:

a) конфиденциальность в режиме с установлением соединения;

b) конфиденциальность потока трафика.

Услуга конфиденциальности потока трафика может принимать две формы:

a) полная конфиденциальность потока трафика, которая может обеспечиваться только в определенных ситуациях, например, при дуплексной одновременной синхронной двухпунктовой передаче;

b) ограниченная конфиденциальность потока трафика, которая может обеспечиваться при других типах передачи, например, асинхронной.

Эти услуги защиты ограничиваются только ситуациями пассивных угроз и могут использоваться на двух- и многопунктовых звеньях данных.

7.1.2 Механизмы

На физическом уровне основным механизмом защиты является механизм полного шифрования потока данных.

Специфичной формой шифрования, приемлемой только на физическом уровне, является защита передачи (т.е. защита по ширине частотного спектра).

Защита физического уровня обеспечивается устройством шифрования, которое работает в прозрачном режиме. Назначение защиты на физическом уровне состоит в том, чтобы защитить полностью битовый поток сервисных данных физического уровня и обеспечить конфиденциальность потока трафика.

7.2 Уровень звена данных

7.2.1 Услуги

На уровне звена данных обеспечиваются только следующие услуги защиты:

a) конфиденциальность в режиме с установлением соединения;

b) конфиденциальность в режиме без установления соединения.

7.2.2 Механизмы

На уровне звена данных для обеспечения услуг защиты используется механизм шифрования (см., однако, приложение С).

Функции защиты на уровне звена данных выполняются до выполнения обычных функций уровня по передаче и после выполнения обычных функций уровня по приему, т.е. механизмы защиты строятся на основе обычных функций уровня и используют их.

Механизмы шифрования на уровне звена данных чувствительны к протоколу уровня звена.

7.3 Сетевой уровень

Внутренняя структура сетевого уровня предназначена для обеспечения протокола(ов), выполняющего(их) следующие операции:

a) доступ к подсети;

b) сходимость, зависящая от подсети;

c) сходимость, не зависящая от подсети;

d) ретрансляция и маршрутизация (см. 2.4).

7.3.1 Услуги

Услуги защиты, которые обеспечиваются протоколом, выполняющим функции доступа к подсети, относящиеся к обеспечению услуг сетевого уровня ВОС, перечислены ниже:

a) аутентификация равноправного логического объекта;

b) аутентификация отправителя данных;

c) услуга управления доступом;

d) конфиденциальность в режиме с установлением соединения;

e) конфиденциальность в режиме без установления соединения;

f) конфиденциальность потока трафика;

g) целостность данных в режиме с установлением соединения без восстановления;

h) целостность данных в режиме без установления соединения.

Эти услуги защиты могут обеспечиваться как по отдельности, так и в сочетании. Услуги защиты, которые предусматриваются протоколом, выполняющим операции ретрансляции и маршрутизации между оконечными системами в соответствии с предоставляемыми услугами сетевого уровня ВОС, аналогичны услугам, которые обеспечивает протокол, выполняющий операции доступа к подсети.

7.3.2 Механизмы

7.3.2.1 Протоколы, выполняющие операции доступа к подсети, ретрансляции и маршрутизации между оконечными системами в соответствии с предоставляемыми услугами сетевого уровня ВОС, используют идентичные механизмы защиты. На этом уровне выполняется маршрутизация, и поэтому в нем предусмотрено управление маршрутизацией. Обеспечиваются следующие перечисленные ниже услуги защиты:

a) услуга аутентификации равноправного логического объекта, обеспечиваемая соответствующим сочетанием обменов криптографически полученной или защищенной информацией аутентификации, паролями защиты или механизмами подписи;

b) услуга аутентификации отправителя данных, которая может быть предоставлена механизмами шифрования или подписи;

c) услуга управления доступом, обеспечиваемая путем соответствующего использования конкретных механизмов управления доступом;

d) услуга конфиденциальности в режиме с установлением соединения, обеспечиваемая механизмами шифрования и/или управления маршрутизацией;

e) услуга конфиденциальности в режиме без установления соединения, обеспечиваемая механизмами шифрования или управления маршрутизацией;

f) услуга конфиденциальности потока трафика, обеспечиваемая механизмом заполнения трафика совместно с услугой конфиденциальности на сетевом или нижерасположенном уровнях и/или механизмом управления маршрутизацией;

g) услуга целостности в режиме с установлением соединения без восстановления, обеспечиваемая путем использования механизма целостности данных, иногда в сочетании с механизмом шифрования, и

h) услуга целостности в режиме без установления соединения, обеспечиваемая путем использования механизма целостности данных, иногда в сочетании с механизмом шифрования.

7.3.2.2 Механизмы протокола, который выполняет операции доступа к подсети, связанные с услугами сетевого уровня ВОС, между оконечными системами, обеспечивают услуги в рамках отдельной подсети.

Защита подсети, устанавливаемая администрацией этой подсети, должна применяться в соответствии с требованиями протоколов доступа к подсети, но обычно она должна использоваться перед выполнением обычных функций подсети по передаче и после выполнения обычных функций подсети по приему.

7.3.2.3 Механизмы, обеспечиваемые протоколом, который выполняет операции ретрансляции и маршрутизации между двумя оконечными системами в сочетании с услугами сетевого уровня ВОС, обеспечивают услуги в рамках одной или нескольких взаимосвязанных сетей.

Эти механизмы должны привлекаться до выполнения функций ретрансляции и маршрутизации при передаче и после выполнения этих функций на принимающей стороне. В случае использования механизма управления маршрутизацией из БАУИЗ выбираются соответствующие ограничения на маршрутизацию перед выдачей функциям ретрансляции и маршрутизации данных вместе с необходимыми ограничениями маршрута.

7.3.2.4 Управление доступом на сетевом уровне может служить многим целям. Например, оно позволяет оконечной системе управлять установлением соединений сетевого уровня и отклонять

нежелательные вызовы. Оно позволяет также одной или нескольким подсетям управлять использованием ресурсов сетевого уровня. В некоторых случаях эта последняя функция связана с оплатой за пользование сетью.

Примечание — Установление соединения сетевого уровня может часто приводить к начислению оплаты со стороны администрации подсети. Минимизация стоимости может быть достигнута путем управления доступом, выбора реверсивной тарификации или других конкретных сетевых параметров.

7.3.2.5 Требования конкретной подсети могут обуславливать необходимость механизмов управления доступом со стороны протокола, который выполняет операции доступа к подсети, связанные с обеспечением сетевых услуг ВОС между оконечными системами. Если такие механизмы управления доступом обеспечиваются протоколом, который выполняет операции ретрансляции и маршрутизации, связанные с обеспечением сетевых услуг ВОС между оконечными системами, то они могут использоваться как для управления доступом к подсети со стороны логических объектов ретранслятора, так и для управления доступом к оконечным системам. Очевидно, что степень изоляции средств управления доступом может лишь весьма приблизительно определять различия между логическими объектами сетевого уровня.

7.3.2.6 Если заполнение трафика используется совместно с механизмом шифрования на сетевом уровне (или с услугой конфиденциальности, предоставляемой физическим уровнем), то может быть достигнут приемлемый уровень конфиденциальности потока трафика.

7.4 Транспортный уровень

7.4.1 Услуги

На транспортном уровне могут обеспечиваться следующие услуги защиты, используемые по отдельности или в сочетании:

a) аутентификация равноправного логического объекта;
b) аутентификация отправителя данных;
c) услуга управления доступом;
d) конфиденциальность в режиме с установлением соединения;
e) конфиденциальность в режиме без установления соединения;
f) целостность в режиме с установлением соединения с восстановлением;
g) целостность в режиме с установлением соединения без восстановления;
h) целостность в режиме без установления соединения.

7.4.2. Механизмы

Обеспечиваются следующие идентифицированные услуги защиты:

a) услуга аутентификации равноправного логического объекта, которая обеспечивается соответствующей комбинацией криптографической или защищенной обмениваемой информацией аутентификации, защитных паролей и механизмов подписи;

b) услуга аутентификации отправителя данных, которая может обеспечиваться механизмами шифрования или подписи;

c) услуга управления доступом, обеспечиваемая путем соответствующего использования специальных механизмов управления доступом;

d) услуга конфиденциальности в режиме с установлением соединения, обеспечиваемая механизмами шифрования;

e) услуга конфиденциальности в режиме без установления соединения, обеспечиваемая механизмами шифрования;

f) услуга целостности в режиме с установлением соединения с восстановлением, обеспечиваемая путем использования механизма целостности данных, иногда в сочетании с механизмом шифрования;

g) услуга целостности в режиме с установлением соединения без восстановления, обеспечиваемая путем использования механизма целостности данных, иногда в сочетании с механизмом шифрования;

h) услуга целостности в режиме без установления соединения, обеспечиваемая путем использования механизма целостности данных, иногда в сочетании с механизмом шифрования.

Механизмы защиты должны функционировать таким образом, чтобы услуги защиты могли привлекаться для отдельных соединений транспортного уровня. Защита должна быть такой, чтобы отдельные соединения транспортного уровня можно было изолировать от всех остальных соединений транспортного уровня.

7.5 Сеансовый уровень

7.5.1 Услуги

На сеансовом уровне не предусматривается никаких услуг защиты.

7.6 **Уровень представления**

7.6.1. Услуги

Уровень представления должен обеспечивать функциональные возможности в поддержку следующих услуг защиты, которые предоставляет прикладной уровень прикладным процессам:

a) конфиденциальность в режиме с установлением соединения;

b) конфиденциальность в режиме без установления соединения;

c) конфиденциальность выбранных полей.

Функциональные возможности уровня представления данных могут также поддерживать предоставление прикладным уровнем прикладным процессам следующих услуг защиты:

d) конфиденциальность потока трафика;

e) аутентификация равноправного логического объекта;

f) аутентификация отправителя данных;

g) целостность в режиме с установлением соединения с восстановлением;

h) целостность в режиме с установлением соединения без восстановления;

j) целостность выбранных полей в режиме с установлением соединения;

k) целостность в режиме без установления соединения;

m) целостность выбранных полей в режиме без установления соединения;

n) безотказность с подтверждением отправителя;

p) безотказность с подтверждением доставки.

Примечание — Функциональные возможности уровня представления должны использовать механизмы, которые могут функционировать только в соответствии с правилами кодирования данных на основе синтаксиса передачи, включая, например, такие механизмы, которые базируются на криптографических методах.

7.6.2. Механизмы

Для следующих услуг защиты поддерживающие механизмы могут быть размещены на уровне представления, и в этом случае они могут использоваться совместно с механизмами защиты прикладного уровня для поддержки его услуг защиты:

a) услуга аутентификации равноправного логического объекта может быть обеспечена механизмами преобразования синтаксиса (например, шифрованием);

b) услуга аутентификации отправителя данных может быть обеспечена механизмами шифрования или подписи;

c) услуга конфиденциальности в режиме с установлением соединения может быть обеспечена механизмом шифрования;

d) услуга конфиденциальности в режиме без установления соединения может быть обеспечена механизмом шифрования;

e) услуга конфиденциальности выборочного поля может быть обеспечена механизмом шифрования;

f) услуга конфиденциальности потока трафика может быть обеспечена механизмом шифрования;

g) услуга целостности в режиме с установлением соединения с восстановлением может быть обеспечена механизмом целостности данных, иногда совместно с механизмом шифрования;

h) услуга целостности в режиме с установлением соединения без восстановления может быть обеспечена механизмом целостности данных, иногда совместно с механизмом шифрования;

j) услуга целостности выбранных полей в режиме с установлением соединения может быть обеспечена механизмом целостности данных, иногда совместно с механизмом шифрования;

k) услуга целостности в режиме без установления соединения может быть обеспечена механизмом целостности данных, иногда совместно с механизмом шифрования;

m) услуга целостности выбранных полей в режиме без установления соединения может быть обеспечена механизмом целостности данных, иногда совместно с механизмом шифрования;

n) услуга «безотказность» с подтверждением отправителя может быть обеспечена соответствующей комбинацией механизмов целостности данных, подписи и нотаризации;

p) услуга «безотказность» с подтверждением доставки может быть обеспечена соответствующей комбинацией механизмов целостности данных, подписи и нотаризации.

При размещении на верхних уровнях механизмов шифрования, используемых для обеспечения передачи данных, они должны располагаться на уровне представления.

Некоторые из перечисленных выше услуг защиты могут быть альтернативно обеспечены механизмами защиты, целиком расположенными на прикладном уровне.

Услуги защиты, которые относятся только к конфиденциальности, могут быть полностью обеспечены механизмами защиты, содержащимися на уровне представления.

Механизмы защиты на уровне представления функционируют в качестве последней стадии преобразования в синтаксис передачи в режиме передачи данных и в качестве начальной стадии процесса преобразования в режиме приема данных.

7.7 **Прикладной уровень**

7.7.1 Услуги

Прикладной уровень может обеспечить одну или несколько следующих основных услуг защиты, используемых как по отдельности, так и в сочетании:

a) аутентификация равноправного логического объекта;
b) аутентификация отправителя данных;
c) услуга управления доступом;
d) конфиденциальность в режиме с установлением соединения;
e) конфиденциальность в режиме без установления соединения;
f) конфиденциальность выбранных полей;
g) конфиденциальность потока трафика;
h) целостность в режиме с установлением соединения с восстановлением;
j) целостность в режиме с установлением соединения без восстановления;
k) целостность выбранных полей в режиме с установлением соединения;
m) целостность в режиме без установления соединения;
n) целостность выбранных полей в режиме без установления соединения;
p) безотказность с подтверждением отправителя;
q) безотказность с подтверждением доставки.

Аутентификация партнеров, желающих обмениваться данными, предусматривает поддержку средств управления доступом к ресурсам как в рамках ВОС, так и вне ВОС (например, файлы, программное обеспечение, терминалы, принтеры) в реальных открытых системах.

Определение специальных требований к защите в сеансе обмена данными, включая конфиденциальность данных, целостность и аутентификацию, может осуществляться административным управлением защиты ВОС или административным управлением прикладного уровня на основе информации, содержащейся в ИБАУЗ в дополнение к запросам, выдаваемым прикладным процессом.

7.7.2 Механизмы

Услуги защиты на прикладном уровне обеспечиваются с помощью следующих механизмов:

a) услуга аутентификации равноправного объекта может быть обеспечена путем использования информации аутентификации, передаваемой между прикладными объектами, защищенными механизмами шифрования, уровня представления или нижерасположенного уровня;

b) услуга аутентификации отправителя данных может быть обеспечена путем использования механизмов подписи или механизмов шифрования смежного нижнего уровня;

c) услуга управления доступом к тем аспектам реальной открытой системы, которые являются постоянными для ВОС, например, способности реальной открытой системы связываться с конкретными системами или удаленными прикладными объектами, может быть обеспечена сочетанием механизмов управления доступом на прикладном и нижерасположенных уровнях;

d) услуга конфиденциальности в режиме с установлением соединения может быть обеспечена путем использования механизма шифрования нижерасположенного уровня;

e) услуга конфиденциальности в режиме без установления соединения может быть обеспечена путем использования механизма шифрования нижерасположенного уровня;

f) услуга конфиденциальности выбранных полей может быть обеспечена путем использования механизма шифрования на уровне представления;

g) услуга конфиденциальности ограниченного потока трафика может быть обеспечена путем совместного использования механизма заполнения трафика на прикладном уровне и услуги конфиденциальности на нижерасположенном уровне;

h) услуга целостности данных в режиме с установлением соединения с восстановлением может быть обеспечена путем использования механизма целостности данных на нижерасположенном уровне, иногда совместно с механизмом шифрования;

j) услуга целостности данных в режиме с установлением соединения без восстановления может быть обеспечена путем использования механизма целостности данных на нижерасположенном уровне, иногда совместно с механизмом шифрования;

k) услуга целостности выбранных полей в режиме с установлением соединения может быть обеспечена путем использования механизма целостности данных, иногда совместно с механизмом шифрования на уровне представления;

m) услуга целостности данных в режиме без установления соединения может быть обеспечена путем использования механизма целостности данных на нижерасположенном уровне, иногда совместно с механизмом шифрования;

n) услуга целостности выбранных полей в режиме без установления соединения может быть обеспечена путем использования механизма целостности данных, иногда совместно с механизмом шифрования на уровне представления;

p) услуга «безотказность» с подтверждением отправителя может быть обеспечена соответствующей комбинацией механизмов целостности данных и подписи на нижерасположенном уровне, возможно в сочетании с нотаризацией третьей стороной;

q) услуга «безотказность» с подтверждением доставки может быть обеспечена соответствующей комбинацией механизмов целостности данных и подписи на нижерасположенном уровне, возможно в сочетании с нотаризацией третьей стороной.

Если для обеспечения услуги защиты «безотказность» используется механизм нотаризации, он должен функционировать как доверенная третья сторона. Этот механизм может содержать запись блоков данных, ретранслируемую в их формате передачи (т.е. в синтаксисе передачи) и предназначенную для разрешения соперничества. Механизм нотаризации может также использовать услуги защиты, предоставляемые нижерасположенными уровнями.

7.7.3 Услуги защиты, не входящие в сферу ВОС

Прикладные процессы могут сами практически обеспечивать все услуги и использовать те же типы механизмов, которые были описаны в настоящем стандарте как механизмы, соответствующим образом размещенные в различных уровнях архитектуры. Такое использование не входит в область распространения ВОС, однако оно не является несовместимым с определениями услуг и протоколов и с архитектурой ВОС.

7.8 Иллюстрация взаимоотношения между услугами защиты и уровнями

В таблице 2 приведены уровни эталонной модели, которые могут обеспечивать конкретные услуги защиты. Описания услуг защиты приведены в 5.2. Обоснование размещения услуг защиты на конкретных уровнях приведено в приложении В.

Таблица 2

Услуга	Уровень						
	1	2	3	4	5	6	7*
Аутентификация равноправного логического объекта	•	•	Да	Да	•	•	Да
Аутентификация источника данных	•	•	Да	Да	•	•	Да
Услуга управления доступом	•	•	Да	Да	•	•	Да
Конфиденциальность в режиме с установлением соединения	Да	Да	Да	Да	•	•	Да
Конфиденциальность в режиме без установления соединения	•	Да	Да	Да	•	•	Да
Конфиденциальность выборочного поля	•	•	•	•	•	•	Да
Конфиденциальность потока трафика	Да	•	Да	•	•	•	Да
Целостность в режиме с установлением соединения с восстановлением	•	•	•	Да	•	•	Да
Целостность в режиме с установлением соединения без восстановления	•	•	Да	Да	•	•	Да
Целостность выборочного поля в режиме с установлением соединения	•	•	•	•	•	•	Да
Целостность в режиме без установления соединения	•	•	Да	Да	•	•	Да
Целостность выборочного поля в режиме без установления соединения	•	•	•	•	•	•	Да

Окончание таблицы 2

Услуга	Уровень						
	1	2	3	4	5	6	7*
Безотказность с подтверждением отправителя	•	•	•	•	•	•	Да
Безотказность с подтверждением доставки	•	•	•	•	•	•	Да

Обозначения

Да — услуга должна предусматриваться в стандартах по соответствующему уровню в качестве факультативной возможности поставщика;

• — не обеспечивается;

* — относительно уровня 7 следует заметить, что прикладной процесс сам может обеспечивать услуги защиты.

Примечания

1 При составлении таблицы 2 не ставилась задача показать, что ее элементы имеют одинаковый вес и значимость; наоборот, существует значительная градация масштаба относительно элементов таблицы.

2 Размещение услуг защиты внутри сетевого уровня описано в 7.3.2. Позиция услуг защиты внутри сетевого уровня существенным образом влияет на характер и область применения обеспечиваемых им услуг.

3 Уровень представления содержит ряд средств защиты, которые обеспечивают предоставление услуг защиты прикладным уровнем.

8 Административное управление защитой

8.1 Общие положения

8.1.1 Административное управление защитой ВОС касается тех аспектов административного управления защитой, которые относятся к ВОС и к защите административного управления ВОС. Аспекты административного управления защитой ВОС связаны с теми операциями, которые не относятся к обычным сеансам обмена данными, но которые необходимы для обеспечения и контроля аспектов защиты этих обменов данными.

Примечание — Доступность услуги обмена данными определяется построением сети и/или протоколами административного управления сетью. Для предотвращения отклонения услуги необходим соответствующий выбор последних.

8.1.2 Может существовать несколько стратегий защиты, устанавливаемых администрацией(ями) распределенных открытых систем, и стандарты административного управления защитой ВОС должны обеспечивать такие стратегии. Объекты, которые подчиняются отдельной стратегии защиты, устанавливаемой отдельным полномочным административным органом, иногда объединяются в так называемую «область защиты». Области защиты и их взаимосвязи являются важной сферой для будущего расширения.

8.1.3 Административное управление защитой ВОС относится к административному управлению услугами и механизмами защиты ВОС. Такое управление требует распределения информации административного управления между этими услугами и механизмами, а также сбора информации, относящейся к работе этих услуг и механизмов. Примерами могут служить распределение криптографических ключей, установка административно назначаемых параметров выбора защиты, выдача сообщений как о нормальных, так и об аварийных ситуациях защиты (данные отслеживания защиты), а также активизация и деактивизация услуг. Административное управление защитой не касается прохождения информации, относящейся к защите, в протоколах, которые привлекают специальные услуги защиты (например, в параметрах запросов на соединение).

8.1.4 Информационная база административного управления защитой (ИБАУЗ) является концептуальным хранилищем всей информации, относящейся к защите, необходимой открытым системам. Такой подход не устанавливает какой-либо формы для хранения информации или ее реализации. Однако каждая оконечная система должна содержать необходимую локальную информацию, позволяющую ей приводить в действие соответствующую стратегию защиты. ИБАУЗ является распределенной информационной базой с такой степенью распределения, которая необходима для обеспечения согласованной стратегии защиты в (логической или физической) группировке оконечных систем. На практике области ИБАУЗ могут входить или не входить в состав ИБАУ.

Примечание — Может существовать множество реализаций ИБАУЗ, например:

a) таблица данных;

b) файл;

c) данные или правила, содержащиеся в рамках программного или аппаратного обеспечения реальной открытой системы.

8.1.5 Протоколы административного управления, особенно протоколы административного управления защитой, и каналы передачи данных, передающие информацию административного управления, являются потенциально уязвимыми. Поэтому особое внимание следует уделять обеспечению таких протоколов и информации административного управления защитой, чтобы средства защиты, предоставляемые для обычных сеансов обмена данными, не были ослаблены.

8.1.6 Административное управление защитой может потребовать обмена информацией, относящейся к защите, между различными системными администраторами с целью установления или расширения ИБАУЗ. В некоторых случаях информация, относящаяся к защите, будет проходить через маршруты обмена данными, существующие вне ВОС, и локальные системные администраторы будут модифицировать содержимое ИБАУЗ методами, не стандартизованными в рамках ВОС. В других случаях может оказаться целесообразным организовать обмен подобной информацией по маршрутам обмена данными ВОС, когда информация будет передаваться между двумя прикладными системами административного управления защитой, реализованными в рамках реальной открытой системы. Прикладные системы административного управления защитой будет использовать передаваемую по маршрутам обмена данными информацию для модификации ИБАУЗ. Такая модификация ИБАУЗ может потребовать предварительного предоставления полномочий соответствующему администратору защиты.

8.1.7 Прикладные протоколы должны быть определены для обмена информацией, относящейся к защите, по каналам обмена данных ВОС.

8.2 **Категории административного управления защитой ВОС**

Существует три категории активностей административного управления защитой ВОС:

a) административное управление защитой системы;

b) административное управление услугами защиты;

c) административное управление механизмами защиты.

Кроме того, должна быть рассмотрена защита самого административного управления ВОС (см. 8.2.4). Ключевые функции, выполняемые этими категориями административного управления защитой, обобщены ниже.

8.2.1 Административное управление защитой системы

Административное управление защитой системы рассматривается с точки зрения аспектов административного управления защитой всей функциональной среды ВОС. Приводимый ниже перечень является типичным для активностей, попадающих в эту категорию административного управления защитой:

a) административное управление общей стратегией защиты, включая модификации и поддержание совместимости;

b) взаимодействие с другими функциями административного управления ВОС;

c) взаимодействие с административным управлением услугами и механизмами защиты;

d) административное управление обработкой событий (см. 8.3.1);

e) административное управление анализом процедур защиты (см. 8.3.2);

f) административное управление восстановлением защиты (см. 8.3.3).

8.2.2 Административное управление услугами защиты

Административное управление услугами защиты относится к административному управлению конкретными услугами защиты. Приводимый ниже перечень является типичным для активностей, выполняемых при административном управлении конкретной услугой защиты:

a) определение и присвоение средства желаемой защиты при заданной услуге;

b) присвоение и поддержание правил выбора (при наличии альтернатив) конкретного механизма защиты, используемого для обеспечения запрашиваемой услуги защиты;

c) согласование (локальное или удаленное) доступных механизмов защиты, требующих предварительной настройки административного управления;

d) привлечение конкретных механизмов защиты через соответствующую функцию административного управления механизмами защиты, например, для обеспечения административно-назначаемых услуг защиты;

e) взаимодействие с другими функциями административного управления услугами и механизмами защиты.

8.2.3 Административное управление механизмами защиты

Административное управление механизмами защиты относится к административному управлению конкретными механизмами защиты. Следующий перечень функций административного управления механизмами защиты является типичным, но не исчерпывающим:

a) административное управление ключами;
b) административное управление шифрованием;
c) административное управление цифровой подписью;
d) административное управление доступом;
e) административное управление целостностью данных;
f) административное управление аутентификацией;
g) административное управление заполнением трафика;
h) административное управление маршрутизацией;
j) административное управление нотаризацией;

Каждая из вышеперечисленных функций административного управления механизмами защиты более подробно рассмотрена в 8.4.

8.2.4 Защита административного управления ВОС

Защита всех функций административного управления ВОС и обмена информацией административного управления ВОС является важной составной частью защиты ВОС. Эта категория административного управления защитой потребует соответствующего выбора вышеперечисленных услуг и механизмов защиты ВОС с целью обеспечения адекватной защиты протоколов и информации административного управления (см. 8.1.5). Например, обмен данными между логическими объектами административного управления с использованием информационной базы административного управления, в общем случае, потребует некоторой формы защиты.

8.3 **Конкретные активности административного управления защитой системы**

8.3.1 Административное управление обработкой событий

Аспекты административного управления обработкой событий, распознаваемых в ВОС, представляют собой удаленную выдачу сообщений об очевидных попытках нарушения защиты системы и изменении допустимых значений, используемых для реализации результатов этих сообщений об ошибках.

8.3.2 Административное управление анализом процедур защиты

Административное управление анализом процедур защиты может включать следующие функции:

a) выбор событий, подлежащих регистрации и/или удаленному сбору;
b) разрешение и запрещение регистрации в системном журнале данных отслеживания защиты выбранных событий;
c) удаленный сбор выбранных записей анализа процедур;
d) подготовка отчетов об анализе процедур защиты.

8.3.3 Административное управление восстановлением защиты

Административное управление восстановлением защиты может охватывать следующие функции:

a) обслуживание правил реагирования на реальные или предполагаемые нарушения защиты;
b) удаленная выдача сообщений об очевидных нарушениях защиты системы;
c) взаимодействия администратора защиты.

8.4 **Функции административного управления механизмами защиты**

8.4.1 Административное управление ключами

Административное управление ключами может охватывать следующие функции:

a) генерация соответствующих ключей в соизмеримые с требуемым уровнем защиты интервалы времени;
b) определение в соответствии с требованиями к управлению доступом тех логических объектов, которые должны получить копию каждого ключа;
c) обеспечение защищенной доступности или распределения ключей по запросам объектов в реальной открытой системе.

Предполагается, что некоторые функции административного управления ключами должны осуществляться вне функциональной среды ВОС. Сюда относится физическое распределение ключей доверительными методами.

Обмен рабочими ключами, используемыми во время действия ассоциации, является нормальной функцией уровневого протокола. Выбор рабочих ключей может также осуществляться посредством доступа к центру распределения ключей или путем предварительного распределения через протоколы административного управления.

8.4.2 Административное управление шифрованием

Административное управление шифрованием может включать следующие функции:

a) взаимосвязь с административным управлением ключами;

b) установление криптографических параметров;

c) криптографическая синхронизация.

Наличие механизма шифрования предполагает использование административного управления ключами и общих методов обращения к криптографических алгоритмам.

Степень избирательности защиты, обеспечиваемая шифрованием, определяется теми логическими объектами внутри функциональной среды ВОС, которым присваиваются независимые ключи. Это, в свою очередь, определяется, в общем случае, архитектурой защиты и особенно механизмом административного управления ключами.

Общей ссылкой для криптографических алгоритмов может служить использование соответствующего регистра криптографических алгоритмов или предварительное согласование между логическими объектами.

8.4.3 Административное управление цифровой подписью

Административное управление цифровой подписью включает следующие функции:

a) взаимосвязь с административным управлением ключами;

b) установление криптографических параметров и алгоритмов;

c) использование протокола между связанными логическими объектами, а возможно, и третьей стороной.

Примечание — В общем случае существует большая аналогия между административным управлением цифровой подписью и шифрованием.

8.4.4 Административное управление доступом

Административное управление доступом может предусматривать распределение атрибутов защиты (включая пароли) или модификации списков управления доступом или списков возможностей. Оно может также предусматривать использование протокола между взаимодействующими логическими объектами и другими логическими объектами, обеспечивающими услуги управления доступом.

8.4.5 Административное управление целостностью данных

Административное управление целостностью данных может включать следующие функции:

a) взаимосвязь с административным управлением ключами;

b) установление криптографических параметров и алгоритмов;

c) использование протокола между взаимодействующими логическими объектами.

Примечание — При использовании криптографических методов для обеспечения целостности данных существует большая аналогия между административным управлением целостностью данных и шифрованием.

8.4.6 Административное управление аутентификацией

Административное управление аутентификацией может предусматривать распределение описательной информации, паролей или ключей (с использованием административного управления ключами) между логическими объектами, запрашиваемыми для выполнения аутентификации. Оно может также включать использование протокола между связанными логическими объектами и другими логическими объектами, предоставляющими услуги аутентификации.

8.4.7 Административное управление заполнением трафика

Административное управление заполнением трафика может предусматривать поддержание правил, используемых для заполнения трафика. Например, оно может включать следующие функции:

a) предварительное установление скоростей передачи данных;

b) установление произвольных скоростей передачи данных;

c) установление характеристик сообщений, таких как длина, и

d) изменение спецификации, возможно, в зависимости от времени суток и/или дня недели.

8.4.8 Административное управление маршрутизацией

Административное управление маршрутизацией может охватывать определение звеньев данных или подсетей, которые считаются защищенными или достоверными относительно конкретных критериев.

8.4.9 Административное управление нотаризацией

Административное управление нотаризацией может включать следующие функции:

a) распределение информации о нотариусах;

b) использование протокола между нотариусом и взаимодействующими объектами;

c) взаимодействие с нотариусом.

ПРИЛОЖЕНИЕ А
(справочное)

Общие принципы построения защиты в рамках ВОС

А.1 Основные положения

Данное приложение содержит:

a) информацию о защите ВОС, предназначенную для определения некоторых перспектив развития настоящего стандарта;

b) общие положения по архитектурным применениям различных средств защиты и требований к ним.

Защита в функциональной среде ВОС представляет собой как раз один из аспектов защиты обработки/передачи данных. Для обеспечения эффективности средств защиты, используемых в функциональной среде ВОС, необходимо наличие поддерживающих средств, находящихся вне ВОС. Например, информация, передаваемая между системами, может быть зашифрована, но, если на доступ к самим системам не будет наложено никаких физических ограничений защиты, шифрование может оказаться безуспешным. Кроме того, к ВОС относится только взаимосвязь систем. Для обеспечения эффективности средств защиты ВОС, они должны использоваться совместно со средствами, не входящими в область распространения ВОС.

А.2 Требования к защите

А.2.1 Что понимается под защитой?

Термин «защита» используется в смысле минимизации уязвимости средств и ресурсов. Любое средство обладает какой-либо ценностью. Уязвимость — это некая слабость, которую можно использовать для нарушения системы или содержащейся в ней информации. Угроза — это потенциально возможное нарушение защиты.

А.2.2 Обоснование защиты в открытых системах

Международная организация по стандартизации (ИСО) признала необходимой разработку семейства стандартов, обеспечивающих защиту в рамках архитектуры взаимосвязи открытых систем. Такая необходимость обусловлена следующими причинами:

a) увеличением зависимости общества от вычислительных машин, которые доступны через каналы передачи данных или взаимосвязаны этими каналами и которые требуют наличия защиты от различных угроз;

b) появлением во многих странах законов по «защите данных», которое обязывает производителей демонстрировать целостность и частную принадлежность системы;

c) желанием различных организаций использовать стандарты ВОС, расширяемые при необходимости, при создании существующих и планируемых на будущее закрытые системы.

А.2.3 Что подлежит защите?

В общем случае защите подлежат следующие компоненты:

a) информация и данные (включая программное обеспечение и относящиеся к средствам защиты пассивные данные, такие как пароли);

b) услуги передачи и обработки данных;

c) оборудование и средства.

А.2.4 Угрозы

Угрозы системе передачи данных означают следующее:

a) разрушение информации и/или других ресурсов;

b) искажение или модификацию информации;

c) хищение, удаление или потерю информации и/или других ресурсов;

d) раскрытие информации;

e) прерывание обслуживания.

Угрозы могут классифицироваться на случайные и преднамеренные и могут быть активными и пассивными.

А.2.4.1 *Случайные угрозы*

Случайные угрозы — это те угрозы, которые возникают непреднамеренно. Примерами реальных случайных угроз могут служить отказы системы, операционные грубые ошибки и ошибки в программных комплектах.

А.2.4.2 *Преднамеренные угрозы*

Преднамеренные угрозы могут быть различных видов: от небрежного анализа, использующего легко доступные средства управления, до изощренных вторжений с использованием специальных сведений о системе. Реализуемая преднамеренная угроза может рассматриваться как «вторжение».

А.2.4.3 *Пассивные угрозы*

К пассивным угрозам относятся те, которые при их реализации не приводят к какой-либо модификации любой информации, содержащейся в системе(ах), и где работа и состояние системы не изменяются. Использование пассивного перехвата для анализа информации, передаваемой по каналам связи, представляет собой реализацию пассивной угрозы.

А.2.4.4 *Активные угрозы*

Активные угрозы системе означают изменение информации, содержащейся в системе, либо изменения состояния или работы системы. Примером активной угрозы служит умышленное изменение таблиц маршрутизации системы неполномочным пользователем.

А.2.5 Некоторые конкретные виды вторжений

Ниже кратко рассмотрены некоторые из вторжений, специально касающихся функциональной среды передачи/обработки данных. В последующих разделах встречаются термины «полномочный» и «неполномочный». «Полномочие» означает «предоставление прав». Такое определение подразумевает два аспекта: рассматриваемые права являются правами на выполнение некоторой активности (такой как доступ к данным); и эти права предоставлены некоторому логическому объекту, агенту или процессу. Таким образом, полномочное поведение является рабочей характеристикой тех активностей, для выполнения которых предоставляются (и не аннулируются) права. Более подробное описание концепции полномочия приведено в А.3.3.1.

А.2.5.1 *Маскирование*

Маскирование имеет место, когда какой-либо логический объект претендует на то, чтобы выглядеть подобно другому логическому объекту. Маскирование обычно используется совместно с некоторыми другими формами активных вторжений, особенно, с воспроизведением и модификацией сообщений. Например, после того, как имела место действительная последовательность аутентификации, могут быть перехвачены и воспроизведены другие последовательности аутентификации. Полномочный логический объект, обладающий небольшим числом привилегий, может использовать маскирование для получения дополнительных привилегий путем исполнения роли логического объекта, имеющего такие привилегии.

А.2.5.2 *Воспроизведение*

Воспроизведение происходит, когда сообщение или часть сообщения повторяется с целью получения неполномочного результата. Например, действительное сообщение, содержащее информацию аутентификации, может быть воспроизведено другим логическим объектом для того, чтобы заявить о своей подлинности (как чего-то такого, чего не существует).

А.2.5.3 *Модификация сообщений*

Модификация сообщений происходит, когда происходит необнаруживаемое изменение содержимого передачи, и приводит к некоторому неполномочному результату, как, например, в случае, когда сообщение «Разрешить 'Джону Смиту' считать секретный файл 'счетные данные'» заменяется на сообщение «Разрешить 'Фреду Брауну' считать секретный файл 'счетные данные'».

А.2.5.4 *Отклонение услуги*

Отклонение услуги происходит, когда логический объект неспособен выполнять свойственные ему функции или он действует таким образом, что препятствует другим логическим объектам выполнять свойственные им функции. Это вторжение может быть всеобщим, если логический объект подавляет передачу всех сообщений, или оно может иметь конкретную цель, если логический объект подавляет передачу всех сообщений, направляемых в сторону конкретного получателя, в качестве которых может быть услуга проверки защиты. Это вторжение может включать подавление трафика, как описано в данном примере, или может генерировать дополнительный трафик. Возможна также генерация сообщений, предназначенных для нарушения работы сети, особенно если сеть имеет ретрансляционные логические объекты, которые принимают решения о маршрутизации на основе отчетов о состоянии, полученных от других ретрансляционных логических объектов.

А.2.5.5 *Внутренние вторжения*

Внутренние вторжения происходят, когда уполномоченные пользователи системы ведут себя непреднамеренным или неполномочным образом. Наиболее широко распространенное нарушение работы вычислительной машины подразумевает внутренние вторжения, которые компрометируют защиту системы. К используемым методам защиты от внутренних вторжений относятся следующие:

a) тщательная проверка персонала;

b) тщательное исследование аппаратного и программного обеспечения, стратегии защиты и конфигураций системы с такой степенью гарантии, которая обеспечила бы их правильную работу (так называемая доверительная функциональность);

c) данные отслеживания, предназначенные для повышения вероятности обнаружения подобных вторжений.

А.2.5.6 *Внешние вторжения*

Внешние вторжения могут использовать следующие методы:

a) подсоединение к линии (активное и пассивное);

b) перехват излучений;

c) маскирование под полномочных пользователей системы или под ее компоненты;

d) обход механизмов аутентификации или управления доступом.

А.2.5.7 *«Лазейка»*

Когда логический объект системы изменяется таким образом, что он разрешает нарушителю произвести неполномочное воздействие либо на команду, либо на заранее определенное событие, либо на последовательность таких событий, результат этого действия рассматривается как вторжение типа «лазейка». Например, аутентификация пароля может быть изменена таким образом, чтобы дополнительно к обычным действиям проверялась правильность пароля нарушителя.

А.2.5.8 *«Троянский конь»*

При введении в систему вторжение типа «троянский конь» в дополнение к его полномочным функциям получает некоторые неполномочные функции. Действие ретранслятора, который копирует сообщения также и в неполномочные каналы, представляет собой вторжение типа «троянский конь».

А.2.6 Оценка угроз, степени риска и мер противодействия

Средства защиты обычно повышают стоимость системы и могут усложнить ее использование. Поэтому перед разработкой системы защиты необходимо определить конкретные угрозы, от которых требуется защита. Такая спецификация известна как оценка угрозы. Система уязвима по многим параметрам, однако только некоторые из них используются, поскольку нарушитель обладает ограниченными возможностями или потому что достигаемые результаты не оправдывают его усилий и риска быть обнаруженным. Хотя детализация целей оценки угрозы не входит в предмет рассмотрения данного приложения, в общих чертах такие оценки включают в себя:

a) идентификацию уязвимых мест системы;

b) анализ вероятности угроз, направленных на использование таких уязвимых мест;

c) оценку последствия успешного выполнения угрозы;

d) оценку стоимости каждого вторжения;

e) анализ стоимости возможных мер противодействия;

f) выбор удовлетворительных механизмов защиты (возможно путем использования стоимостного анализа получаемых выгод).

Нетехнические средства, такие как страхование, могут служить экономичными альтернативами технических средств защиты. Совершенная техническая защита, так же как и совершенная физическая защита невозможны. Поэтому задача состоит в достижении того, чтобы стоимость вторжения была достаточно высокой для уменьшения степени риска до приемлемых уровней.

А.3 **Стратегия защиты**

В данном разделе рассматривается стратегия защиты, в том числе необходимость в подходящем определении стратегии защиты, ее роль, методы использования стратегии и ее уточнение применительно к конкретным ситуациям. Эти принципы затем могут быть применены к системам передачи данных.

А.3.1 Необходимость и назначение стратегии защиты

Вся область защиты сложна и трудно реализуема. Любой в разумных пределах полный анализ приведет к обескураживающему множеству подробностей. Приемлемая стратегия защиты должна сконцентрировать внимание на тех аспектах ситуации, которые должны учитываться при рассмотрении на высоком уровне полномочий. По существу, стратегия защиты устанавливает в общих понятиях, что допустимо и что недопустимо в области защиты в процессе основных операций рассматриваемой системы. Стратегия обычно не является конкретной, она исходит из того, что является делом первостепенной важности, не определяя в точности, каким образом можно достичь желаемых результатов. Стратегия защиты устанавливает наивысший уровень спецификации защиты.

А.3.2 Применения определения стратегии. Процесс уточнения

Поскольку стратегия имеет достаточно общий характер, то вначале не совсем ясно, как можно совместить ее с конкретным применением. Часто наилучший способ достижения этого состоит в том, чтобы сориентировать стратегию на успешное проведение процесса уточнения путем добавления на каждой стадии все больших подробностей конкретного применения. Для выяснения необходимых деталей требуется подробное изучение области применения в свете общей стратегии. Такое рассмотрение должно определить проблемы, возникающие из попыток наложения условий на стратегию в данном применении. Процесс уточнения приведет к новой установке общей стратегии в очень точных понятиях, непосредственно вытекающих из данного применения. Эта заново установленная стратегия облегчает определение деталей реализации.

А.3.3 Компоненты стратегии защиты

Имеются два аспекта, относящихся к существующим стратегиям защиты. Оба они зависят от принципа полномочного поведения.

А.3.3.1 *Полномочие*

Все рассмотренные выше виды угроз охватывают понятия полномочного и неполномочного поведения. Определение сущности полномочия отражено в стратегии защиты. Общая стратегия защиты может устанавливать: «информация не может быть предоставлена, быть доступной либо допускать вмешательство и не может быть ресурсом, используемым теми, кто не имеет соответствующих полномочий». Характер полномочий как раз и определяет отличия различных стратегий. Основываясь на соответствующем характере полномочий, все стратегии могут быть подразделены на два отдельных вида: стратегии, основанные на правилах, и стратегии, основанные на идентификации. Первые используют правила, основанные на небольшом числе общих атрибутов или классов чувствительности, которые имеют универсальное применение. Вторые охватывают критерий полномочий, основанный на конкретных индивидуальных атрибутах. Некоторые атрибуты предполагаются постоянно связанными с логическим объектом их применения, другие могут временно присваиваться логическому объекту (такие как функциональные возможности) и передаваться другим логическим объектам. Можно также различать административно назначаемые и динамически выбираемые средства полномочий. Стратегия защиты должна определять те элементы системной защиты, которые всегда применимы и остаются в силе (например, компоненты стратегии, основанные на правилах и идентификации при их наличии) и те из них, которые пользователь может выбрать для использования по своему усмотрению.

А.3.3.2 *Стратегия защиты, основанная на идентификации*

Аспекты стратегии защиты, основанных на идентификации, частично соответствуют принципам защиты,

известным как «необходимость опознавания». Цель ее состоит в фильтрации доступа к данным или ресурсам. Имеются два основных фундаментальных способа реализации стратегий, основанных на идентификации, в зависимости от того, сохраняется ли информация о правах на доступ получателем или она является частью данных, которые должны быть доступными. Первая служит примером принципов привилегий или функциональных возможностей, предоставляемых пользователям и используемых процессами по их поручению. Примерами последней служат списки управления доступом (СУД). В обоих случаях размер области данных (от полного файла до элемента данных), который может быть поименован в функциональной возможности или который переносит свой собственный СУД, может изменяться в широких пределах.

А.3.3.3 *Стратегия защиты, основанная на правилах*

Полномочия в стратегии защиты, основанной на правилах, обычно основаны на чувствительности. В закрытой системе данные или ресурсы должны быть помечены метками защиты. Процессам, действующим по инициативе персонала, может быть присвоена метка защиты, соответствующая их инициатору.

А.3.4 Стратегия, взаимосвязи и метки защиты

Концепция присвоения меток выполняет важную роль в среде обмена данными. Метки, переносящие атрибуты, выполняют различные функции. Имеются элементы данных, которые перемещаются во время обмена данными; существуют процессы и логические объекты, которые инициируют обмен данными, а также такие, которые выдают ответы; существуют каналы и другие ресурсы самой системы, используемые во время обмена данными. Всем им может быть тем или иным способом присвоена метка с соответствующими атрибутами. Стратегии защиты должны указывать, как атрибуты каждой из них могут использоваться для обеспечения требуемой защиты. Для установления надлежащей значимости защиты конкретных помеченных атрибутов может потребоваться согласование. Когда метки защиты присваиваются как доступным процессам, так и доступным данным, должна быть соответствующим образом помечена дополнительная информация, необходимая для обеспечения управления доступом на основе идентификации. Если стратегия защиты основана на идентификации пользователя, имеющего доступ к данным непосредственно или с помощью процесса, то метки защиты должны содержать информацию об идентификации пользователя. Правила присвоения конкретных меток должны быть представлены в стратегии защиты в базе административной информации защиты (БАУИЗ) и/или согласованы, при необходимости, с оконечными системами. Метка может быть добавлена с помощью атрибутов, которые квалифицируют соответствующую чувствительность для определения средств обработки и распределения, ограничения таймирования и местоположения и четкого определения требований, специфичных для данной оконечной системы.

А.3.4.1 *Метки процесса*

При аутентификации полная идентификация тех процессов или логических объектов, которые инициируют сеанс обмена данными или отвечают на него, в совокупности со всеми соответствующими атрибутами имеет обычно фундаментальную важность. Поэтому БАУИЗ должны содержать достаточную информацию о тех атрибутах, которые важны для любой административно назначаемой стратегии.

А.3.4.2 *Метки области данных*

По мере перемещения областей данных в процессе сеансов обмена данными каждая из них должна быть тесно связана со своей меткой. (Эта связь является существенной, и в некоторых случаях применения стратегий, основанных на правилах, существует требование, чтобы метка составляла специальную часть области данных перед тем, как она будет предъявлена прикладному применению.) Средства для сохранения целостности области данных должны также поддерживать точность и сцепление меток. Эти атрибуты могут быть использованы функциями управления маршрутизацией на уровне звена данных базовой эталонной модели ВОС.

А.4 Механизмы защиты

Стратегия защиты может быть реализована путем использования отдельного или сочетания различных механизмов в зависимости от целей защиты и применяемых механизмов. В общем случае такой механизм должен принадлежать к одному из трех (перекрывающихся) классов:

a) предотвращение;

b) обнаружение;

c) восстановление.

Механизмы защиты, соответствующие среде обмена данными, рассматриваются ниже.

А.4.1 Методы криптографирования и шифрование

Криптография основана на множестве средств и механизмов защиты. Функции криптографирования могут быть использованы как часть шифрования, дешифрования, целостности данных, обменов аутентификацией, хранения и проверки пароля и др. для обеспечения конфиденциальности, целостности и/или аутентичности. Шифрование, используемое для обеспечения конфиденциальности, преобразует чувствительные данные (т.е. данные, подлежащие защите) для получения менее чувствительных форм. При использовании в целях обеспечения целостности или аутентичности криптографические методы применяются для машинного выполнения второстепенных функций.

Шифрование первоначально выполняется над открытым текстом для получения шифротекста. Результатом дешифрования является либо открытый текст, либо шифротекст с некоторым закрытием. При машинном выполнении легко использовать открытый текст для его общей обработки; его семантическое содержимое доступно. За исключением специальных методов (например, первичного дешифрования или точного согласования) при машинном выполнении нелегко обработать шифротекст, так как его семантическое содержимое закрыто. Шифрование иногда умышленно делают необратимым (например, путем усечения или потери данных), когда даже нежелательно получить исходный открытый текст, например, пароли.

Криптографические функции используют криптопеременные и оперируют с полями, блоками данных и/или потоками блоков данных. К двум таким криптопеременным относятся ключ, который управляет конкретными преобразованиями, и переменная инициализации, которая необходима в некоторых криптографических протоколах для сохранения явной произвольности шифротекста. Ключ должен обычно оставаться конфиденциальным, и как криптографическая функция, так и переменная инициализации могут увеличить задержку и снизить пропускную способность. Это усложняет внесение «прозрачных» и «обеспечивающих свободный доступ» криптографических дополнений к существующим системам.

Криптографические переменные могут быть симметричными или асимметричными, охватывая как шифрование, так и дешифрование. Ключи, используемые в асимметричных алгоритмах, являются математически относительными; один ключ не может быть вычислен из остальных. Эти алгоритмы иногда называют алгоритмами «ключа общего пользования», поскольку один ключ может быть сделан ключом общего пользования, а другой — закрытым.

Шифротекст может быть подвергнут криптоанализу, когда при машинном выполнении легко восстановить шифротекст без сведений о ключе. Это может иметь место при использовании слабой или недействительной криптографической функции. Перехваты и анализ трафика могут привести к вторжениям в криптосистему, включая вставку, удаление и изменение поля/сообщения, искажение правильного шифротекста и маскирование. Поэтому криптографические протоколы проектируются с целью сопротивления вторжениям, а также иногда — анализу трафика. Специальные меры противодействия анализу трафика, «конфиденциальность потока трафика» помогают закрыть наличие или отсутствие данных и их характеристик. Если шифротекст ретранслируется в ретрансляторах и шлюзах, то адрес должен находиться в открытом виде. Если данные шифруются только в каждом звене данных, а дешифруются (и таким образом уязвимы) в ретрансляторе и шлюзе, архитектура определяет использование «позвенного шифрования». Если в ретрансляторе или шлюзе в открытом виде находится только адрес (и аналогичные управляющие данные), архитектура определяет использование «межоконечного шифрования». Межоконечное шифрование является более желательным с точки зрения защиты, но архитектурно значительно более сложным, особенно, если обеспечивается внутриполосное распределение электронных ключей (функция административного управления ключом). Позвенное и межоконечное шифрования могут использоваться в совокупности для достижения нескольких целей защиты. Целостность данных часто обеспечивается путем подсчета криптографического контрольного значения. Контрольное значение может быть получено за один или несколько шагов и является математической функцией криптопеременных и данных. Эти контрольные значения связаны с данными, подлежащими защите. Криптографические контрольные значения иногда называются кодами обнаружения манипуляции.

Криптографические средства могут обеспечить или помочь обеспечить защиту от:

a) наблюдения потока сообщения и/или его модификации;

b) анализа трафика;

c) самоотказа;

d) маскирования;

e) неполномочного соединения;

f) модификации сообщений.

А.4.2 Аспекты административного управления ключами

Административное управление ключами обеспечивается путем использования криптографических алгоритмов. Оно охватывает генерацию, распределение и управление криптографическими ключами. Выбор метода административного управления ключами основан на личностной оценке среды, в которой он должен использоваться. К вопросам, касающимся этой среды, относятся угрозы, от которых необходима защиты (как внутренняя по отношению к организации, так и внешняя), используемые методы, архитектурная структура и размещение обеспечиваемых криптографических услуг, а также физическая структура и размещение поставщиков криптографических услуг.

К вопросам административного управления ключами относятся следующие:

a) использование понятия «время существования», основанного на времени, использовании или другом критерии, который явно или неявно определен для каждого ключа;

b) надлежащая идентификация ключей в соответствии с их функцией таким образом, чтобы, например, их использование можно было зарезервировать только для этих функций. Ключи, предназначенные для услуги конфиденциальности, не должны применяться для услуги целостности и наоборот;

c) вопросы, относящиеся к функциям не-ВОС, таким как физическое распределение и архивация ключей.

К вопросам административного управления ключами для симметричных алгоритмов ключа относятся:

a) использование услуги конфиденциальности в протоколе административного управления ключами для передачи ключей;

b) использование иерархии ключей. Должны допускаться различные ситуации, например:

1)«плоскостные» иерархии ключей, использующие только ключи шифрования данных, явно или неявно выбранные из набора с помощью идентификатора или индекса ключа;

2) многоуровневые иерархии ключей;

3) ключи шифрования-ключа никогда не следует использовать для защиты данных и ключи шифрования данных никогда не следует использовать для защиты ключей шифрования-ключа;

c) такое разделение ответственностей, при котором никто из обслуживающего персонала не обладает копией важного ключа.

К вопросам административного управления ключами для асимметричных алгоритмов ключа относятся:

a) использование услуги конфиденциальности в протоколе административного управления ключами для передачи закрытых ключей;

b) использование услуг целостности или «безотказность» с подтверждением отправителя в протоколе административного управления ключами для передачи ключей общего пользования. Эти услуги могут быть обеспечены путем использования симметричных и/или асимметричных криптографических алгоритмов.

А.4.3 Механизмы цифровой подписи

Понятие цифровой подписи используется для указания конкретного метода, который может быть применен для обеспечения таких услуг защиты, как «безотказность» и аутентификации. Механизмы цифровой подписи требуют использования асимметричных криптографических алгоритмов. Важной характеристикой механизма цифровой подписи является то, что подписанный блок данных не может быть создан без использования личного ключа. Это означает, что:

a) подписанный блок данных не может быть создан каким бы то ни было лицом, за исключением лица, обладающего личным ключом;

b) получатель не может создать подписанный блок данных.

Из того следует, что использование доступной информации общего пользования возможно только для идентификации подписчика блока данных единственно в качестве лица, обладающего личным ключом. В случае возникновения последующего конфликта между участниками последнее означает возможность предоставить проверку идентификации подписчика блока данных надежной третьей стороне, которая привлекается при анализе аутентичности подписанного блока данных. Этот тип цифровой подписи называется схемой прямой подписи (см. рисунок 1). В других случаях может потребоваться дополнительное свойство (c):

c) отправитель не может отклонить передачу подписанного блока данных.

Надежная третья сторона (арбитр) обеспечивает получателю в этом случае источник и целостность информации. Этот тип цифровой подписи иногда называют схемой арбитражной подписи (см. рисунок 2).

Примечание — Отправитель может потребовать, чтобы получатель не смог позднее отклонить прием подписанного блока данных. Это может быть выполнено с помощью услуги «безотказность» с подтверждением доставки соответствующей комбинацией цифровой подписи, целостности данных и механизмов нотаризации.

А.4.4 Механизмы управления доступом

К механизмам управления доступом относятся те, которые используются для задействования стратегии ограниченного доступа к ресурсам только со стороны полномочных пользователей. К таким методам относятся использование списков или матриц управления доступом (которые обычно содержат идентификаторы конкретных управляемых объектов и полномочных пользователей, например, персонала или процессов), паролей и функциональных возможностей, меток или маркеров, обладание которыми может быть использовано для указания права на доступ. При использовании функциональных возможностей они должны быть сохранены в неизменном виде и переданы достоверно.

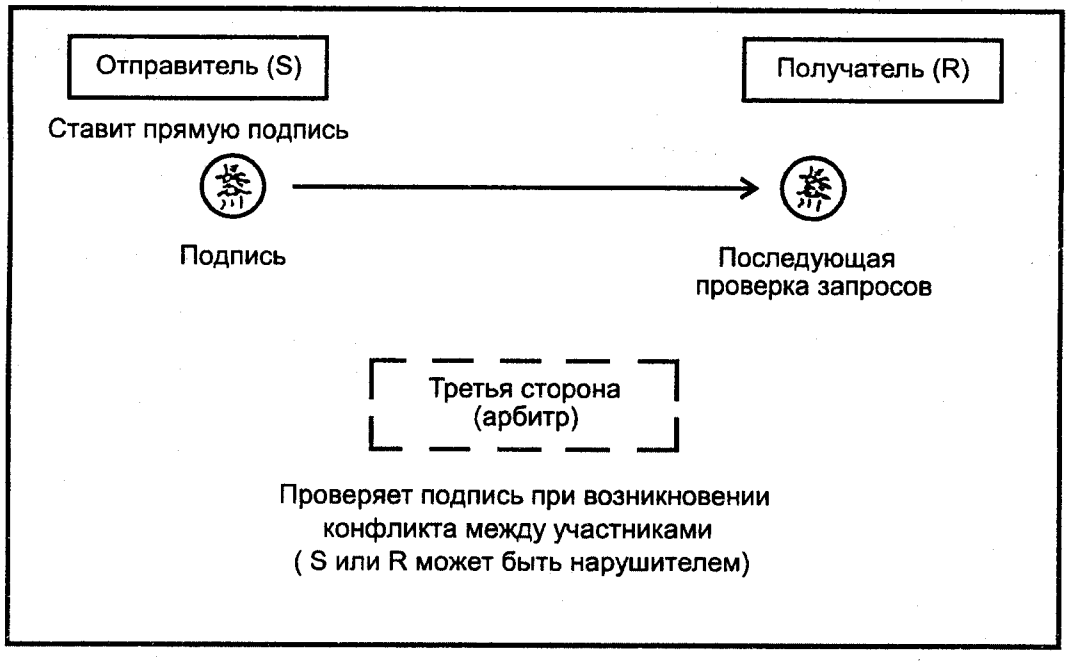


Рисунок 1 — Схема прямой подписи

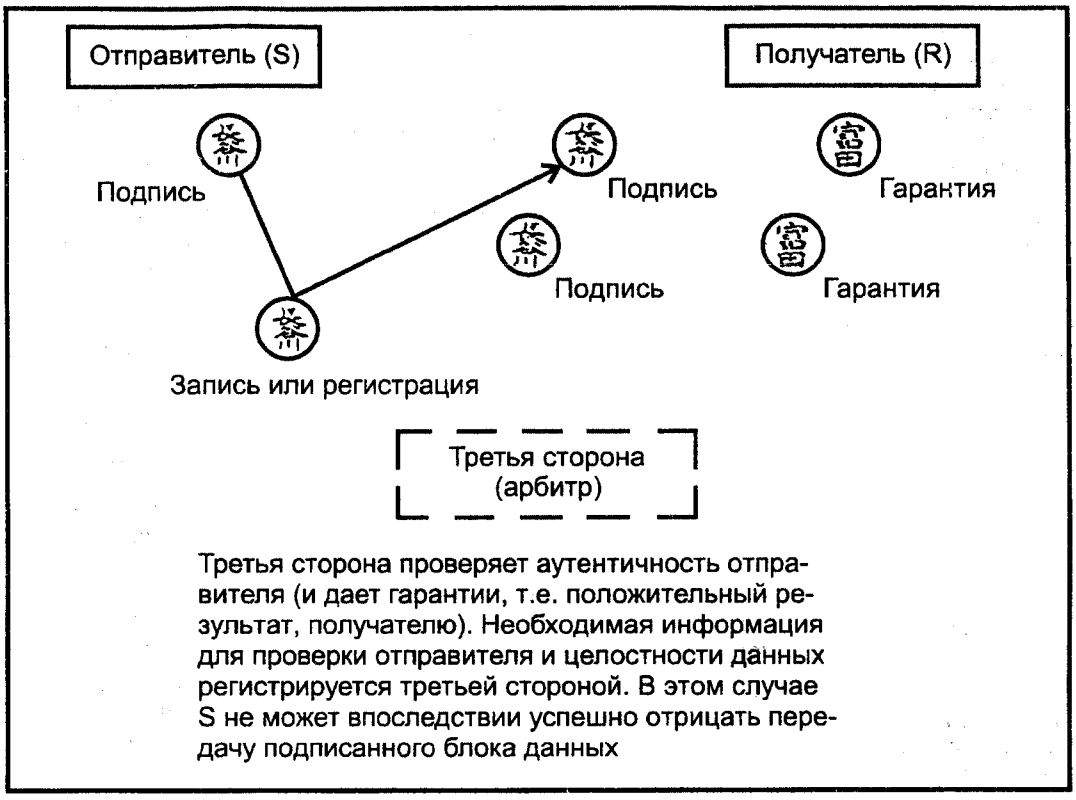


Рисунок 2 — Схема арбитражной подписи

А.4.5 Механизмы целостности данных

Существует два типа механизмов целостности данных: одни используются для защиты целостности отдельного блока данных, а другие — для защиты целостности как отдельного блока данных, так и последовательности полного потока блоков данных по соединению.

А.4.5.1 *Обнаружение модификации потока сообщений*

Методы обнаружения разрушения информации, обычно связанные с обнаружением ошибок битов, блоков и последовательностей, вносимых каналами связи и сетями, могут быть использованы также для обнаружения модификации потока сообщений. Однако, если протокольные заголовки и окончания не защищены механизмами целостности, нарушитель информации может успешно обойти такой контроль. Таким образом, успешное обнаружение модификации потока сообщений может быть достигнуто только путем использования средств обнаружения разрушений в сочетании с последующей информацией. Это может не предотвратить модификацию потока сообщений, но обеспечит уведомление о вторжениях.

А.4.6 Механизмы обмена информацией аутентификации

А.4.6.1 *Выбор механизма*

Существует множество вариантов и комбинаций механизмов обмена информацией аутентификации, соответствующих различным ситуациям. Например:

a) если равноправные логические объекты и средства обмена данными достоверны, идентификация равноправного логического объекта может быть подтверждена паролем. Пароль защищает от ошибки, но не гарантирует от злонамеренных нарушений (особенно от воспроизведения информации). Взаимная аутентификация может быть осуществлена путем использования в каждом направлении различных паролей;

b) если каждый логический объект уверен в соответствующем равноправном логическом объекте, но не уверен в средствах обмена данными, защита от активных вторжений может быть обеспечена путем комбинаций паролей и шифрования или путем криптографических методов. Защита от вторжения воспроизведения информации требует двунаправленного квитирования (с параметрами защиты) или установки временных отметок (с достоверными счетчиками). Взаимная аутентификация с защитой от воспроизведения информации может быть достигнута путем использования трехнаправленного квитирования;

c) если логические объекты не уверены (или чувствуют, что уверенность в дальнейшем исчезнет) в соответствующих равноправных логических объектах или в средствах обмена данными, можно использовать услуги «безотказность». Услуга «безотказность» может быть реализована путем использования цифровой подписи и/или механизмов нотаризации. Эти механизмы могут использоваться в сочетании с механизмами, описанными выше в b).

А.4.7 Механизмы заполнения трафика

Путем генерации ложного трафика и протокольных блоков данных заполнителей постоянной длины можно обеспечить ограниченную защиту от анализа трафика. Для успешного выполнения уровень ложного трафика должен быть приближен к наивысшему ожидаемому уровню реального трафика. Кроме того, содержимое протокольных блоков данных должно быть зашифровано или замаскировано таким образом, чтобы ложный трафик нельзя было опознать и отличить от реального трафика.

А.4.8 Механизм управления маршрутизацией

Спецификация запретов на использование маршрутов для передачи данных (включая спецификацию полного маршрута) может применяться для обеспечения того, чтобы данные передавались только по маршрутам, имеющим физическую защиту, или для обеспечения передачи чувствительной информации только по маршрутам с соответствующей степенью защиты.

А.4.9 Механизм нотаризации

Механизм нотаризации основан на концепции доверенной третьей стороны (нотариуса), удостоверяющей определенные свойства информации, которой обмениваются два логических объекта, например такие, как ее отправитель, ее целостность или время ее передачи или приема.

А.4.10 Физическая или персональная защита

Для обеспечения полной защиты всегда будут необходимы средства физической защиты. Физическая защита обходится дорого, и необходимость в ней часто пытаются минимизировать путем использования других (более дешевых) средств. Вопросы физической и персональной защиты не входят в область распространения ВОС, хотя все системы должны в конечном счете полагаться на некоторые формы физической защиты и на надежность обслуживающего персонала системы. Должны быть определены операционные процедуры для обеспечения надлежащей работы и определения ответственности персонала.

А.4.11 Надежное аппаратное/программное обеспечение

К методам, используемым для получения уверенности в правильном функционировании логического объекта, относятся методы формальных проверок, верификации и проверки корректности, обнаружения и регистрации обнаруженных попыток вторжений, а также построения логического объекта надежным персоналом в защищенной функциональной среде. Необходимо также соблюдать предосторожности от неслучайной или сознательной модификации логического объекта, которая компрометирует защиту в течение своего рабочего срока службы, например, в процессе эксплуатации или расширения. Некоторые логические объекты в системе должны также быть надежными для правильного функционирования при необходимости защиты. Методы установления доверительности не входят в область распространения ВОС.

ПРИЛОЖЕНИЕ В
(справочное)

Обоснование размещения услуг и механизмов защиты информации в разделе 7

В.1 **Общие положения**

Данное приложение содержит некоторые обоснования для обеспечения идентифицируемых услуг защиты информации в рамках различных уровней, рассмотренных в разделе 7. Принципы уровневой организации защиты, указанные в 6.1.1 настоящего стандарта, управляются этим процессом выбора.

Конкретная услуга защиты обеспечивается несколькими уровнями, если ее воздействие на общую защиту обмена данными может считаться различным (например, конфиденциальность соединения на уровнях от 1 до 4). Тем не менее, учитывая существующие функциональные возможности обмена данными ВОС (например, многозвенные процедуры, функции мультиплексирования, различные методы расширения услуг в режиме без установления соединения до услуг в режиме с установлением соединения) и для обеспечения работоспособности этих механизмов передачи может оказаться необходимым допустить обеспечение конкретной услуги на другом уровне, хотя ее воздействие на защиту не может считаться различным.

В.2 **Аутентификация равноправного логического объекта**

Уровни 1 и 2. Отсутствует, считается, что аутентификация равноправного логического объекта нецелесообразна на этих уровнях.

Уровень 3. Используется по отдельным подсетям и для маршрутизации и/или по внутренней сети.

Уровень 4. Используется, аутентификация от одной оконечной системы до другой на уровне 4 может служить для взаимной аутентификации двух или более логических объектов сеансового уровня до установления соединения и во время существования этого соединения.

Уровень 5. Отсутствует, нет преимуществ относительно обеспечения этой услуги на уровне 4 и/или вышерасположенных уровнях.

Уровень 6. Отсутствует, однако механизмы шифрования могут поддерживать эту услугу на прикладном уровне.

Уровень 7. Используется, аутентификация равноправных логических объектов должна обеспечиваться прикладным уровнем.

В.3 **Аутентификация отправителя данных**

Уровни 1 и 2. Отсутствует, считается, что аутентификация отправителя данных нецелесообразна на этих уровнях.

Уровни 3 и 4. Аутентификация отправителя данных может обеспечиваться как межоконечная с целью ретрансляции и маршрутизации на уровнях 3 и/или 4 следующим образом:

а) обеспечение аутентификации равноправного логического объекта во время установления соединения в сочетании с непрерывной аутентификацией на основе шифрования во время существования соединения фактически обеспечивает услугу аутентификации отправителя данных;

b) даже если а) не обеспечивается, аутентификация отправителя данных на основе шифрования может обеспечиваться с очень небольшими дополнительными затратами со стороны механизмов целостности данных, уже размещенных на этих уровнях.

Уровень 5. Отсутствует, нет преимуществ относительно обеспечением этой услуги на уровнях от 4 до 7.

Уровень 6. Отсутствует, однако механизмы шифрования могут поддерживать эту услугу на прикладном уровне.

Уровень 7. Используется, возможна в сочетании с механизмами на уровне представления данных.

В.4 **Управление доступом**

Уровни 1 и 2. Механизмы управления доступом не могут обеспечиваться на этих уровнях в системе, соответствующей всем протоколам ВОС, поскольку не существует оконечных средств, доступных такому механизму.

Уровень 3. Механизмы управления доступом могут применяться к протоколам, выполняющим роль доступа к подсети по требованиям конкретной подсети. При выполнении протоколами роли ретрансляции и маршрутизации механизмы доступа на сетевом уровне могут использоваться как для управления доступом к подсетям с помощью логических объектов ретрансляции, так и для управления доступом к оконечным системам. Очевидно, что эти градации доступов являются достаточно грубыми, различаясь только в логических объектах сетевого уровня.

Установление сетевого соединения может часто приводить к затратам администрации подсети. Минимизация стоимости может быть обеспечена путем контроля доступа и выбора реверсивной тарификации относительно конкретных параметров другой сети или подсети.

Уровень 4. Используется, механизмы управления доступом могут быть реализованы на основе межоконечных соединений транспортного уровня.

Уровень 5. Отсутствует, нет преимуществ относительно обеспечения этой услуги на уровнях от 4 до 7.

Уровень 6. Отсутствует, эта услуга не свойственна уровню 6.

Уровень 7. Используется, прикладные протоколы и/или прикладные процессы могут обеспечивать средства управления доступом, ориентированные на прикладное применение.

В.5 **Конфиденциальность всех (N)-данных пользователя в (N)-соединении**

Уровень 1. Используется, должен обеспечиваться, поскольку электрическое введение прозрачных пар устройств преобразования может обеспечить полную конфиденциальность по отношению к физическому соединению.

Уровень 2. Используется, но не обеспечивает дополнительных преимуществ защиты по сравнению с конфиденциальностью на уровнях с 1 до 3.

Уровень 3. Используется в протоколах, выполняющих роль доступа к подсети по отдельным подсетям и роль ретрансляции и маршрутизации по внутренней сети.

Уровень 4. Используется, поскольку отдельное соединение транспортного уровня предоставляет межоконечный механизм транспортного уровня и может обеспечивать изоляцию соединений сеансового уровня.

Уровень 5. Отсутствует, поскольку не обеспечивает дополнительных преимуществ по сравнению с конфиденциальностью на уровнях 3,4 и 7. Представляется нецелесообразным обеспечением этой услуги на данном уровне.

Уровень 6. Используется, поскольку механизмы шифрования обеспечивают чисто синтаксические преобразования.

Уровень 7. Используется в сочетании с механизмами нижерасположенных уровней.

В.6 **Конфиденциальность всех (N)-данных пользователя в отдельном (N)-СБД, передаваемом в режиме без установления соединения**

Обоснование аналогично конфиденциальности всех (N)-данных пользователя за исключением уровня 1, где не существует услуги режима без установления соединения.

В.7 **Конфиденциальность выборочных полей внутри (N)-данных пользователя некоторого СБД**

Эта услуга конфиденциальности обеспечивается путем шифрования на уровне представления и привлекается механизмами прикладного уровня в соответствии с семантиками данных.

В.8 **Конфиденциальность потока трафика**

Конфиденциальность полного потока трафика может быть достигнута только на уровне 1. Она может быть обеспечена путем физического введения в физический маршрут передачи пары устройств шифрования. Предполагается, что маршрут передачи должен быть дуплексным и синхронным, так что введение этих устройств будет воспроизводить все передачи (и даже их наличие) при нераспознаваемой физической среде.

На уровнях выше физического полная защита потока трафика невозможна. Некоторые из ее действий могут быть частично выполнены путем использования услуги конфиденциальности полного СБД на одном уровне и введения фиктивного трафика на смежном верхнем уровне. Такой механизм является дорогостоящим и потенциально предполагает большие объемы средств связи и коммутации.

Если конфиденциальность потока трафика обеспечивается на уровне 3, должны использоваться заполнение трафика и/или управление маршрутизации. Управление маршрутизацией может обеспечить ограниченную конфиденциальность потока трафика путем передачи сообщений маршрутизации по незащищенным звеньям данных или подсетям. Однако введение в состав уровня 3 функции заполнения трафика позволяет достичь более эффективного использования сети, например, путем предотвращения необязательных вставок и перегрузок сети.

Ограниченная конфиденциальность потока трафика может быть обеспечена на прикладном уровне путем генерации фиктивного трафика в сочетании с конфиденциальностью, предназначенной для предотвращения идентификации фиктивного трафика.

В.9 **Целостность всех (N)-данных пользователя в (N)-соединении (с восстановлением при ошибках)**

Уровни 1 и 2. Неспособны обеспечивать эту услугу. Уровень 1 не имеет механизмов обнаружения и восстановления, а механизмы уровня 2 функционируют только на двухпунктовой, а не межоконечной основе, в связи с чем данная услуга здесь неприемлема.

Уровень 3. Отсутствует, поскольку восстановлением при ошибках не для всех доступно.

Уровень 4. Используется, поскольку это обеспечивает действительное межоконечное соединение транспортного уровня.

Уровень 5. Отсутствует, поскольку восстановление при ошибках не является функцией уровня 5.

Уровень 6. Отсутствует, но механизмы шифрования могут обеспечивать эту услугу на прикладном уровне.

Уровень 7. Используется в сочетании с механизмами уровня представления.

В.10 **Целостность всех (N)-данных пользователя в (N)-соединении (без восстановления при ошибках)**

Уровни 1 и 2. Неспособны обеспечивать эту услугу. Уровень 1 не имеет механизмов обнаружения и восстановления, а механизмы уровня 2 функционируют только на двухпунктовой, а не межоконечной основе, в связи с чем данная услуга здесь неприемлема.

Уровень 3. Используется для обеспечения доступа к подсети по отдельным подсетям, а также для функций ретрансляции и маршрутизации по внутренней сети.

Уровень 4. Используется для тех случаев использования, когда допустимо прекращать обмен данными после обнаружения активного вторжения.

Уровень 5. Отсутствует, поскольку не обеспечивает дополнительных преимуществ по сравнению с целостностью данных на уровнях 3, 4 и 7.

Уровень 6. Отсутствует, однако механизмы шифрования могут обеспечивать эту услугу на прикладном уровне.

Уровень 7. Используется в сочетании с механизмами уровня представления.

В.11 **Целостность выбранных полей внутри (N)-данных пользователя (N)-СБД, передаваемого по (N)-соединению (без восстановления)**

Целостность выбранных полей может быть обеспечена механизмами шифрования уровня представления в сочетании с механизмами вызова и проверки прикладного уровня.

В.12 **Целостность всех (N)-данных пользователя в отдельном (N)-СБД, передаваемом в режиме без установления соединения**

Для минимизации дублирования функций целостность передач в режиме без установления соединения должна обеспечиваться только на тех уровнях, что и целостность без восстановления, т.е. на сетевом, транспортном и прикладном уровнях. Такие механизмы целостности могут иметь только очень ограниченную эффективность и они должны использоваться.

В.13 **Целостность выбранных полей в отдельном (N)-СБД, передаваемом в режиме без установления соединения**

Целостность выбранных полей может быть обеспечена механизмами шифрования на уровне представления в сочетании с механизмами вызова и проверки на прикладном уровне.

В.14 **Услуга «безотказность»**

Услуги «безотказность» отправителя и получателя могут быть обеспечены механизмом нотаризации, который может использовать ретрансляцию на уровне 7.

Использование механизма цифровой подписи для услуги «безотказность» требует тесной взаимосвязи между уровнями 6 и 7.

ПРИЛОЖЕНИЕ С
(справочное)

Выбор позиций шифрования для конкретных применений

С.1 Большинство применений не требуют использования шифрования на нескольких уровнях. Выбор уровня зависит от некоторых основных аспектов следующим образом:

а) при необходимости полной конфиденциальности потока трафика должно быть выбрано шифрование на физическом уровне или защита передачи (например, подходящие методы расширения спектра). Адекватная

физическая защита и доверительная маршрутизация, а также аналогичная функциональность ретрансляторов могут удовлетворить все требования конфиденциальности;

b) при необходимости сильной градации защиты (то есть, возможно, отдельный ключ для каждой прикладной ассоциации) и услуги «безотказность» или избирательной защиты полей должно быть выбрано шифрование на уровне представления. Избирательная защита полей может оказаться важной, поскольку алгоритмы шифрования потребляют большие мощности обработки. Шифрование на уровне представления может обеспечить целостность без восстановления, услугу «безотказность» и полную конфиденциальность;

c) при необходимости массовой защиты всех обменов данными между оконечными системами и/или внешних устройств шифрования (например, для обеспечения физической защиты алгоритма и ключей или защиты от сбоев программного обеспечения) должно быть выбрано шифрование на сетевом уровне. Это может обеспечить конфиденциальность и целостность без восстановления.

Примечание — Хотя процедуры восстановления не обеспечиваются на сетевом уровне, на транспортном уровне могут быть использованы обычные механизмы для восстановления от вторжений, обнаруженных сетевым уровнем;

d) при необходимости обеспечения целостности с восстановлением совместно с высокой градацией защиты должно быть выбрано шифрование на транспортном уровне. Это может обеспечить конфиденциальность и целостность с восстановлением или без него;

e) шифрование на уровне звена данных не рекомендуется для будущих разработок.

С.2 При рассмотрении двух или более из этих ключевых аспектов может потребоваться шифрование на нескольких уровнях.

УДК 681.324:006.354 ОКС 35.100 П85 ОКСТУ 4002

Ключевые слова: обработка данных, обмен информацией, взаимосвязь сетей, взаимосвязь открытых систем, эталонная модель, модели, режим передачи данных.

Редактор *В.П. Огурцов*
Технический редактор *О.Н. Власова*
Корректор *Н.Л. Шнайдер*
Компьютерная верстка *В.И. Грищенко*

Изд. лиц. № 021007 от 10.08.95. Сдано в набор 22.03.99. Подписано в печать 05.05.99. Усл. печ. л. 4,65.
Уч.-изд. л. 4,87. Тираж 227 экз. С2786. Зак. 376.

ИПК Издательство стандартов, 107076, Москва, Колодезный пер., 14.
Набрано в Издательстве на ПЭВМ
Филиал ИПК Издательство стандартов — тип. "Московский печатник", Москва, Лялин пер., 6.
Плр № 080102