ГОСУДАРСТВЕННЫЙ СТАНДАРТ УЗБЕКИСТАНА

Информационная технология

ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ БАЗОВАЯ ЭТАЛОННАЯ МОДЕЛЬ

Часть 2

Архитектура безопасности

(ISO 7498-2:1989, MOD)

Издание официальное

Узбекское агентство стандартизации, метрологии и сертификации
Ташкент

Предисловие

1 ПОДГОТОВЛЕН Государственным унитарным предприятием Центр научно-технических и маркетинговых исследований - «UNICON.UZ» Узбекского агентства связи и информатизации

2 ВНЕСЕН Техническим комитетом по стандартизации в сфере связи и информатизации № 7

3 ПРИНЯТ Постановлением Узбекского агентства стандартизации, метрологии и сертификации от 13.06.2011 № 05-309

4 Настоящий стандарт модифицирован относительно международ-ного стандарта ISO 7498-2:1989 «Системы обработки информации. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура безопасности» (ISO 7498-2:1989 «Information processing systems. Open Systems Interconnection. Basic Reference Model. Part 2. Security Architecture»).

Перевод с английского языка (en).

В стандарт включены следующие редакционные изменения:

a) слова «настоящий международный стандарт» заменены на «настоящий стандарт»;

b) слова «Системы обработки информации» заменены на «Информационная технология»;

c) из раздела 2 «Нормативные ссылки» исключены международные стандарты:

- ISO/IEC 7498-4:1989 Системы обработки информации. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 4. Основы управления;
- ISO 7498/Add.1 Системы обработки информации. Взаимосвязь открытых систем. Базовая эталонная модель. Приложение 1. Передача в режиме без установления соединения (заменен стандартом ISO/IEC 7498-1:1994);
- ISO 8648:1988 Системы обработки информации. Взаимосвязь открытых систем. Внутренняя организация сетевого уровня;

d) 3.2 ISO 7498-2 изменен следующим образом:

- термины «(N)-передача в режиме без установления соединения» и «оконечная система ВОС», определенные в O‘z DSt ISO/IEC 7498-1:2009, перенесены из 3.2 ISO 7498-2 в 3.1 настоящего стандарта;
- из перечня терминов исключена запись «UNITDATA (ISO 7498)», соответственно в сокращения добавлена запись «UNITDATA - примитив «ДАННЫЕ БЕЗ СОЕДИНЕНИЯ»;

- исключены записи «функции ретрансляции и маршрутизации (ISO 8648)» и «информационная база управления (ИБУ) (ISO 7498-4)», соответственно термины «(N)-ретрансляция», «маршрутизация» и «информационная база управления» с соответствующими определениями приведены в 3.3.

Официальные экземпляры международного стандарта, на основе которого разработан настоящий государственный стандарт, и государственного стандарта Узбекистана, на который даны ссылки, имеются в информационно-справочном центре агентства «Узстандарт».

Сведения о соответствии государственного стандарта Узбекистана ссылочному международному стандарту приведены в дополнительном приложении D.

Степень соответствия – модифицированная (MOD)

5 ВВЕДЕН ВПЕРВЫЕ

Содержание

Введение

Стандарт O‘z DSt ISO/IEC 7498 описывает базовую эталонную модель взаимосвязи открытых систем (ВОС) и устанавливает основу для скоординированного развития действующих и будущих стандартов в области ВОС.

Цель ВОС заключается в обеспечении такой взаимосвязи разнотипных вычислительных систем, которая позволит достигнуть эффективного обмена между прикладными процессами. Во многих случаях для обеспечения безопасности информации, которой обмениваются прикладные процессы, должны быть установлены элементы управления безопасностью. Использование таких элементов управления безопасностью будет способствовать тому, что стоимость получения или модификации данных станет выше потенциальной ценности этих данных, либо тому, что получение данных потребует продолжительного времени, по истечении которого эти данные утратят свою ценность.

Часть 2 стандарта O‘z DSt ISO/IEC 7498 определяет общую архитектуру элементов управления безопасностью, которые могут быть использованы соответствующим образом в тех случаях, когда необходимо обеспечить безопасность данных, передаваемых между открытыми системами. Также для обеспечения безопасности передаваемых данных в рамках эталонной модели часть 2 устанавливает рекомендации и ограничения по совершенствованию действующих или по разработке новых стандартов в области ВОС и тем самым определяет согласованный метод обеспечения безопасности информации в рамках ВОС.

Для понимания настоящего стандарта необходимо знать общие принципы в области безопасности информации. Читателю, недостаточно подготовленному в этой области, рекомендуется сначала ознакомиться с приложением А.

Настоящий стандарт расширяет базовую эталонную модель в части аспектов безопасности информации, которые являются общими элементами архитектуры для протоколов обмена данными, но которые не рассмотрены в базовой эталонной модели.

ГОСУДАРСТВЕННЫЙ СТАНДАРТ УЗБЕКИСТАНА

Ахборот технологияси
ОЧИҚ ТИЗИМЛАРНИНГ ЎЗАРО БОҒЛИҚЛИГИ
АСОСИЙ ЭТАЛОН МОДЕЛЬ
2-қисм.
Хавфсизлик архитектураси

Информационная технология
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ
БАЗОВАЯ ЭТАЛОННАЯ МОДЕЛЬ
Часть 2.
Архитектура безопасности

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

Дата введения 2011-07-01

1 Область применения

Настоящий стандарт:

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

b) определяет позиции в рамках эталонной модели, в которых могут быть обеспечены услуги и механизмы безопасности.

Настоящий стандарт расширяет область применения стандарта O‘z DSt ISO/IEC 7498-1, освещая вопросы безопасности информации при обмене данными между открытыми системами.

Для всех уровней базовой эталонной модели определены основные услуги и механизмы безопасности и соответствующее их размещение. Кроме того, определена архитектура взаимосвязи услуг и механизмов безопасности с базовой эталонной моделью. В оконечных системах, оборудовании и устройствах может понадобиться применение дополнительных мер безопасности. Эти меры применяются в различных контекстах приложений. Определение услуг безопасности, необходимых для обеспечения дополнительных мер безопасности, выходит за пределы рассмотрения настоящего стандарта.

Функции безопасности в рамках ВОС рассмотрены с учетом только тех видимых аспектов маршрутов обмена данными, которые позволяют оконечным системам обеспечивать безопасность информации при её передаче между ними.

Издание официальное

Безопасность в рамках ВОС не касается тех мер безопасности, которые необходимы для оконечных систем, оборудования и устройств, за исключением тех случаев, когда эти системы оказывают влияние на выбор и позицию услуг безопасности, наблюдаемых в рамках ВОС. Эти аспекты безопасности могут быть стандартизированы, но не в пределах стандартов в области ВОС.

Настоящий стандарт дополняет, не изменяя, концепции и принципы, установленные в O‘z DSt ISO/IEC 7498-1. Настоящий стандарт не является спецификацией и/или основой для оценки соответствия действующих реализаций.

2 Нормативные ссылки

В настоящем стандарте использована нормативная ссылка на следующий стандарт:

O‘z DSt ISO/IEC 7498-1:2009 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть. 1. Базовая модель

3 Термины, определения и сокращения

3.1 В настоящем стандарте использованы следующие термины, определенные в O‘z DSt ISO/IEC 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;
u) (N)-передача в режиме без установления соединения;
v) оконечная система ВОС.

3.2 В настоящем стандарте использованы следующие сокращения:

ВОС - взаимосвязь открытых систем

СБД - сервисный блок данных

ИБУ - информационная база управления

ИБУБ - информационная база управления безопасностью

UNITDATA - примитив «ДАННЫЕ БЕЗ СОЕДИНЕНИЯ»

3.3 В настоящем стандарте использованы следующие термины с соответствующими определениями:

3.3.1 **управление доступом:** Предотвращение несанкционированного использования ресурса, включая предотвращение использования ресурса несанкционированным 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 **подотчетность:** 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 безопасности информации, могут служить модификация сообщений, повтор сообщений, вставка ложных сообщений, маскировка какого-либо логического объекта под санкционированный объект и отказ в обслуживании.

3.3.5 **аудит:** См. аудит безопасности.

3.3.6 **журнал аудита:** См. журнал аудита безопасности.

3.3.7 **аутентификация:** См. аутентификация источника данных и аутентификация 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 достоверности идентификационной информации, предъявленной логическим объектом.

3.3.9 **обмен аутентификацией:** Механизм, предназначенный для подтверждения подлинности какого-либо логического объекта путем обмена информацией.

3.3.10 **авторизация:** Предоставление прав, которое включает предоставление доступа на основании прав доступа.

3.3.11 **доступность:** Свойство данных или ресурсов быть доступными и пригодными к использованию по запросу авторизованного логического объекта.

3.3.12 **полномочие:** Маркер, который используется в качестве идентификатора для ресурса, обозначающего, что владение им дает права доступа к данному ресурсу.

3.3.13 **канал:** Маршрут передачи информации.

3.3.14 **шифротекст:** Данные, получаемые в результате использования шифрования, семантическое содержимое которых не доступно без использования криптографических методов.

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

3.3.15 **открытый текст:** Данные, семантическое содержимое которых доступно без использования криптографических методов.

3.3.16 **конфиденциальность:** Свойство данных, позволяющее не давать права доступа к информации или не раскрывать ее неавторизованным лицам, процессам или другим логическим объектам.

3.3.17 **верительные данные:** Данные, передаваемые для установления заявленной подлинности логического объекта.

3.3.18 **криптоанализ:** Анализ криптографической системы и/или ее входов и выходов с целью получения чувствительных данных, включая открытый текст.

3.3.19 **криптографическое контрольное значение:** Информация, получаемая в результате выполнения криптографического преобразования (см. криптография) в блоке данных.

Примечание - Вывод контрольного значения может быть выполнен за один или несколько шагов, и это значение является результатом математической функции ключа и блока данных. Обычно используется для проверки целостности блока данных.

3.3.20 **криптография:** Дисциплина, охватывающая принципы, средства и методы преобразования данных, для сокрытия их семантического содержимого, предотвращения их несанкционированного использования или необнаруживаемой модификации.

Примечание – Криптография определяет методы, используемые при шифровании и дешифровании. Любое воздействие на принципы, средства или методы криптографии называется криптоанализом.

3.3.21 **целостность данных:** Способность данных не подвергаться изменению или уничтожению при несанкционированном доступе.

3.3.22 **аутентификация источника данных:** Подтверждение того, что источник полученных данных соответствует заявленному.

3.3.23 **дешифрование:** Процесс, обратный соответствующему обратимому процессу шифрования.

3.3.24 **дешифрация:** См. дешифрование.

3.3.25 **отказ в обслуживании:** Прекращение санкционированного доступа к ресурсам или задержка выполнения операций, критичных по времени.

3.3.26 **цифровая подпись:** Данные, добавленные к блоку данных, или криптографическое преобразование блока данных, которое позволяет получателю данных удостовериться в подлинности отправителя и целостности блока данных и защитить его от подделки, например, получателем.

3.3.27 **шифрование:** Криптографическое преобразование данных (см.криптография) для создания шифротекста.

Примечание - Шифрование может быть необратимым и в этом случае выполнение соответствующего процесса дешифрования невозможно.

3.3.28 **шифрация:** См. шифрование.

3.3.29 **сквозное шифрование:** Шифрование данных в пределах системы или на стороне отправителя с соответствующим дешифрованием, которое осуществляется только в пределах системы или на стороне получателя. (См. также канальное шифрование).

3.3.30 **идентификационная политика безопасности:** Политика безопасности, в основу которой положена идентификационная информация и/или атрибуты пользователей, групп пользователей или логических объектов, действующих от имени пользователей, а также ресурсов/объектов, к которым обеспечивается доступ.

3.3.31 **целостность:** См. целостность данных.

3.3.32 **ключ:** Последовательность символов, управляющая операциями шифрования и дешифрования.

3.3.33 **управление ключами:** Генерация, хранение, распределение, уничтожение, архивирование и использование ключей в соответствии с политикой безопасности.

3.3.34 **канальное шифрование:** Индивидуальное применение шифрования к данным на каждом звене системы телекоммуникаций. (См. также сквозное шифрование).

Примечание - При канальном шифровании данные на ретрансляторах находятся в форме открытого текста.

3.3.35 **обнаружение манипуляции:** Механизм, используемый для обнаружения модификации блока данных (случайной или умышленной).

3.3.36 **маскарад:** Поведение нарушителя, пытающегося выдать себя за законного пользователя.

3.3.37 **нотаризация:** Регистрация данных доверенной третьей стороной, которая обеспечит впоследствии подтверждение таких их характеристик, 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, состоящая, как правило, из строки символов.

3.3.40 **аутентификация равноправного логического объекта:** Подтверждение того, что равноправный логический объект в ассоциации является заявленным объектом.

3.3.41 **физическая безопасность:** Меры, предпринимаемые для обеспечения физической безопасности ресурсов от умышленных и случайных угроз.

3.3.42 **политика:** См. политика безопасности.

3.3.43 **личная тайна:** Право частного лица контролировать или воздействовать на то, какая касающаяся его информация может быть собрана и сохранена, а также кем и кому может быть открыто содержание этой информации.

Примечание - Учитывая, что данный термин относится к правам частных лиц, он не может быть предельно точным и следует воздерживаться от его использования за исключением случаев обоснования уровня необходимой безопасности.

3.3.44 **непризнание участия:** Отрицание одним 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 обходу конкретных сетей, линий или ретрансляторов.

3.3.46 **инструкционная политика безопасности:** Политика безопасности на основе глобальных правил, обязательных для всех пользователей. Эти правила обычно связаны со сравнением чувствительности ресурсов, к которым имеется доступ, и владением соответствующими атрибутами пользователей, групп пользователей или логических объектов, действующих от имени пользователей.

3.3.47 **аудит безопасности:** Независимый просмотр и анализ записей системы обработки данных и ее работы для проверки на адекватность управляющих функций системы, обеспечения соответствия принятой политике безопасности и операционным процедурам, обнаружения нарушений безопасности и выдачи рекомендаций по любым определенным изменениям в управлении, политике безопасности и процедурах.

3.3.48 **журнал аудита безопасности:** Данные, собираемые для последующего использования при проведении аудита безопасности.

3.3.49 **метка безопасности:** Маркировка, связанная с ресурсом (которым может быть блок данных), определяющая имя или обозначение атрибутов безопасности данного ресурса.

Примечание - Маркировка и/или присвоенное значение могут быть явными или неявными.

3.3.50 **политика безопасности:** Набор критериев для предоставления услуг безопасности (см. также идентификационная политика безопасности и инструкционная политика безопасности).

Примечание – Комплексная политика безопасности неизбежно затрагивает многие вопросы, выходящие за рамки ВОС.

3.3.51 **услуга безопасности:** Услуга, предоставляемая каким-либо уровнем открытых систем, которая гарантирует достаточную безопасность систем или процессов передачи данных.

3.3.52 **избирательная защита поля:** Защита конкретных полей в сообщении, которое подлежит передаче.

3.3.53 **чувствительность:** Характеристика ресурса, которая косвенно выражает его ценность или важность и может учитывать его уязвимость.

3.3.54 **подпись:** См. цифровая подпись.

3.3.55 **угроза:** Потенциальное нарушение безопасности.

3.3.56 **анализ трафика:** Анализ информации, полученной при наблюдении за потоками трафика (наличие, отсутствие, объем, направление и частота).

3.3.57 **конфиденциальность потока трафика:** Услуга конфиденциальности, обеспечивающая защиту трафика от анализа.

3.3.58 **заполнение трафика:** Генерация ложных сеансов связи, ложных блоков данных и/или ложных данных внутри подлинных блоков данных.

3.3.59 **доверенные функциональные возможности:** Функциональные возможности, которые воспринимаются как правильные относительно некоторых критериев, например, установленной политики безопасности.

3.3.60 **маршрутизация:** Функция внутри уровня, выполняющая преобразование символического имени логического объекта или адреса пункта доступа к услугам, к которому подсоединен логический объект, в маршрут, по которому может быть установлена связь с указанным логическим объектом.

3.3.61 **(N)-ретрансляция:** (N)-функция, посредством которой (N)-логический объект выполняет дальнейшую пересылку данных, полученных от одного связанного (N)-логического объекта другому связанному (N)-логическому объекту.

3.3.62 **информационная база управления:** Концептуальное хранилище информации административного управления в открытой системе.

4 Обозначения

В настоящем стандарте использована та же система обозначений по уровням, что и в O‘z DSt ISO/IEC 7498-1. Термин «услуга», если не оговорено иное, используют в смысле «услуга безопасности».

5 Общее описание услуг и механизмов безопасности

5.1 Краткий обзор

В данном разделе рассмотрены услуги безопасности, включенные в архитектуру безопасности ВОС, а также механизмы реализации этих услуг. Услуги безопасности, описанные ниже, являются базовыми услугами

безопасности. На практике они реализуются на соответствующих уровнях и в соответствующих комбинациях, обычно совместно с услугами и механизмами, которые не относятся к области рассмотрения ВОС, для выполнения требований политики безопасности и/или пользователя. Конкретные механизмы безопасности могут быть использованы для реализации комбинаций базовых услуг безопасности.

При практической реализации систем могут быть непосредственно использованы конкретные комбинации базовых услуг безопасности.

5.2 Услуги безопасности

Ниже приведено описание услуг безопасности, которые могут дополнительно предоставляться в рамках базовой эталонной модели ВОС. Для выполнения проверки подлинности логического объекта или источника данных услугам аутентификации необходима информация аутентификации, включающая локально хранимую информацию и переданные верительные данные.

5.2.1 Аутентификация

Ниже описаны услуги, которые обеспечивают аутентификацию равноправного логического объекта и источника данных.

5.2.1.1 Аутентификация равноправного логического объекта

Когда данная услуга предоставляется (N)-уровнем, то она обеспечивает для (N+1)-логического объекта подтверждение того, что равноправный логический объект является заявленным (N+1)-логическим объектом. Эта услуга предназначена для использования во время установления соединения или во время передачи данных с целью подтверждения идентичности одного или нескольких логических объектов, соединенных с одним или несколькими другими логическими объектами. Эта услуга обеспечивает доверие только на момент её использования, позволяя удостовериться в том, что никакой логический объект не пытался замаскироваться под другой логический объект или несанкционированно повторно использовать предыдущее соединение. Независимо от того, проводится или не проводится проверка отказоустойчивости для обеспечения различной степени защиты возможно использование односторонней и взаимной аутентификации равноправного логического объекта.

5.2.1.2 Аутентификация источника данных

Когда данная услуга предоставляется (N)-уровнем, то она обеспечивает для (N+1)-логического объекта подтверждение того, что источник данных является заявленным (N+1)-логическим объектом. Услуга аутентификации источника данных обеспечивает подтверждение подлинности источника блока данных. Эта услуга не обеспечивает безопасность от повтора или модификации блоков данных

5.2.2 Управление доступом

Эта услуга обеспечивает безопасность использования ресурсов от несанкционированного доступа через ВОС. Ресурсами, доступными через протоколы ВОС, могут быть ресурсы, используемые или не используемые в рамках ВОС. Данная услуга может применяться к ресурсам с различными видами доступа (например, использование ресурса для обмена данными; чтение, запись или удаление информационного ресурса; использование ресурса средств обработки) или ко всем доступным ресурсам.

Управление доступом должно рассматриваться в соответствии с различными политиками безопасности (6.2.1.1).

5.2.3 Конфиденциальность данных

Ниже описаны услуги, которые обеспечивают безопасность данных от несанкционированного раскрытия.

5.2.3.1 Конфиденциальность в режиме с установлением соединения

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

Примечание - В зависимости от используемого уровня эта услуга не может обеспечить защиту всех данных, например срочных данных или данных запроса на установление соединения.

5.2.3.2 Конфиденциальность в режиме без установления соединения

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

5.2.3.3 Конфиденциальность выбранного поля

Данная 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 за потоками трафика.

5.2.4 Целостность данных

Данная услуга противостоит активным угрозам и может принимать одну из нижеописанных разновидностей.

Примечание - Совместное использование услуги аутентификации равноправного логического объекта и услуги целостности данных в режиме с установлением соединения обеспечивает подтверждение подлинности источника всех блоков данных и целостность блоков данных, передаваемых по этому соединению, а также может дополнительно обеспечить обнаружение повтора блоков данных, например путем использования порядковых номеров.

5.2.4.1 Целостность в режиме с установлением соединения с восстановлением

Данная услуга обеспечивает целостность всех данных (N)-пользователя, передаваемых по (N)-соединению, и обнаруживает любую модификацию,

вставку, уничтожение или повторное использование любых данных внутри полной последовательности СБД (с попыткой восстановления).

5.2.4.2 Целостность в режиме с установлением соединения без восстановления

Данная 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

Данная услуга обеспечивает целостность выбранных полей внутри данных (N)-пользователя в составе какого-либо (N)-СБД, передаваемого по соединению, и определяет вид искажения выбранных полей: модификация, вставка, удаление или повторное использование.

5.2.4.4 Целостность данных в режиме без установления соединения

Данная услуга предоставляется (N)-уровнем и обеспечивает целостность данных для запрашивающего (N+1)-логического объекта.

Эта услуга обеспечивает целостность одного СБД, передаваемого в режиме без установления соединения, и может определить, был ли модифицирован принятый СБД. Дополнительно может быть предусмотрена ограниченная форма обнаружения повторного использования.

5.2.4.5 Целостность выбранного поля в режиме без установления соединения

Данная услуга обеспечивает целостность отдельных полей внутри одного СБД, передаваемого в режиме без установления соединения, и определяет, были ли модифицированы выбранные поля.

5.2.5 Неотказуемость

Данная услуга может принимать одну или обе из двух нижеописанных форм.

5.2.5.1 Неотказуемость с подтверждением источника

Получатель данных обеспечивается подтверждением источника данных. Эта услуга обеспечивает защиту от любой попытки источника данных ложно отрицать передачу данных или их содержимое.

5.2.5.2 Неотказуемость с подтверждением доставки

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

5.3 Специальные механизмы безопасности

В состав соответствующего (N)-уровня для предоставления некоторых услуг, описанных в 5.2, могут входить нижеперечисленные механизмы.

5.3.1 Шифрование

5.3.1.1 Шифрование может использоваться для обеспечения услуг конфиденциальности данных или конфиденциальности потока трафика, а также может поддерживать другие услуги в дополнение к механизмам безопасности, описанным в последующих разделах.

5.3.1.2 Алгоритмы шифрования могут быть обратимыми и необратимыми. Существует два вида обратимых механизмов шифрования:

a) симметричное шифрование (т.е. шифрование с секретным ключом), при котором знание ключа шифрования предполагает знание ключа дешифрования, и наоборот;

b) асимметричное шифрование (т.е. шифрование с открытым ключом), при котором знание ключа для шифрования не предполагает знание ключа дешифрования, или наоборот. Два ключа такой системы иногда называются «открытый ключ» и «личный ключ».

Ключ в алгоритмах необратимого шифрования используется не всегда. При использовании ключа он может быть либо открытым, либо секретным.

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

5.3.2 Механизмы цифровой подписи

Эти механизмы включают в себя две процедуры:

a) формирование цифровой подписи;

b) проверку цифровой подписи.

Первая процедура использует информацию, которая является персональной (т.е. уникальной и конфиденциальной) по отношению к подписывающему лицу. Вторая процедура использует общедоступную информацию, из которой не может быть выделена персональная информация подписывающего лица.

5.3.2.1 Процедура формирования цифровой подписи включает в себя шифрование блока данных или выработку криптографического контрольного значения блока данных с использованием персональной информации подписывающего лица в качестве личного ключа.

5.3.2.2 Процедура проверки цифровой подписи заключается в использовании общедоступной информации для определения, была ли цифровая подпись сформирована с помощью персональной информации подписывающего лица.

5.3.2.3 Существенной характеристикой механизма цифровой подписи является то, что она может быть сформирована только с использованием персональной информации подписывающего лица. Соответственно впоследствии при проверке цифровой подписи можно в любое время

доказать третьей стороне (например, судье или арбитру), что сформировать данную подпись мог исключительно только обладатель персональной информации.

5.3.3 Механизмы управления доступом

5.3.3.1 Эти механизмы используются для подтверждения подлинности логического объекта или информации о логическом объекте (например, принадлежность к некоторому множеству логических объектов), а также полномочий логического объекта с целью определения и присвоения права доступа этому логическому объекту. Если логический объект попытается получить несанкционированный доступ к ресурсу или санкционированный доступ к ресурсу с запрещенным ему типом доступа, то функция управления доступом отклонит эту попытку, а также дополнительно выдаст уведомление об этом инциденте с помощью сгенерированного сигнала тревоги и/или зарегистрирует событие информационной безопасности, что будет необходимо впоследствии для аудита безопасности. Любое уведомление источника данных об отказе в обслуживании при передаче данных в режиме без установления соединения обеспечивается только отправителем данных с помощью управления доступом.

5.3.3.2 Механизмы управления доступом могут использовать, например, следующие виды и источники информации:

a) информационные базы данных управления доступом, где поддерживаются права доступа равноправных логических объектов. Эта информация может обслуживаться центрами авторизации или логическим объектом, к которому осуществляется доступ, и может быть оформлена в виде списка управления доступом или в форме матрицы доступа иерархической или распределенной структуры.

Этот фактор предполагает, что аутентификация равноправного логического объекта обеспечена;

b) информацию аутентификации, например, пароли, владение и последующее представление которых подтверждается авторизацией логического объекта, осуществляющего доступ;

c) полномочия, владение и последующее представление которых подтверждается наличием у логического объекта или ресурса права доступа, определяемого данными полномочиями;

Примечание - Полномочия должны исключать возможность подделки и должны быть предоставлены надежным способом.

d) метки безопасности, которые при присвоении какому-либо логическому объекту должны использоваться для получения или отказа в праве на доступ в соответствии с политикой безопасности;

e) время попытки получения доступа;

f) маршрут попытки получения доступа;

g) длительность доступа.

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

Управление доступом, задействованное в источнике или любом промежуточном пункте, используется для определения того, что уполномочен ли источник на обмен данными с получателем и/или использование запрашиваемых ресурсов.

Требования, предъявляемые к механизмам управления доступом на равноправных уровнях со стороны получателя при передаче данных в режиме без установления соединения, должны быть заранее известны источнику, а также должны быть зарегистрированы в ИБУБ (6.2, 8.1).

5.3.4 Механизмы целостности данных

5.3.4.1 Различают два типа целостности данных: целостность отдельного блока данных или поля и целостность потока блоков данных или отдельных полей. В общем случае, контроль двух видов целостности осуществляется различными механизмами, хотя контролировать целостность потока, не проверяя целостность отдельного блока данных, нецелесообразно.

5.3.4.2 Процедура контроля целостности отдельного блока данных включает в себя два процесса, один из которых выполняется на передающем логическом объекте, а другой - на принимающем. Передающий логический объект добавляет к блоку данных некоторую контрольную величину, которая является функцией от самих данных. Этой контрольной величиной может быть дополнительная информация, например, код проверки блока или криптографическое контрольное значение, данная информация может быть 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 обеспечивает защиту от повторного использования отдельного блока данных. Контроль работы с данными на соответствующих уровнях архитектуры может привести в действие процедуру восстановления (например, путем повторной передачи или исправления ошибок) на данном или вышерасположенном уровне.

5.3.4.3 Для проверки целостности потока блоков данных (то есть для защиты от изменения порядка следования, потерь, повторного использования, вставок или модификации данных) при передаче данных в режиме с установлением соединения используются порядковая нумерация, временные метки или криптографическое сцепление.

5.3.4.4 При передаче данных в режиме без установления соединения использование временных меток обеспечивает также и ограниченную защиту от повторного использования отдельных блоков данных.

5.3.5 Механизмы обмена информацией аутентификации

5.3.5.1 Для обмена информацией аутентификации могут быть использованы некоторые из нижеперечисленных методов:

a) использование информации аутентификации, например, паролей, которые создаются передающим логическим объектом, а проверяются принимающим логическим объектом;

b) криптографические методы;

c) использование характеристик и/или принадлежностей логического объекта.

5.3.5.2 Вышеперечисленные механизмы могут использоваться на (N)-уровне для аутентификации равноправного логического объекта. Если механизму не удалось выполнить аутентификацию логического объекта, то это может привести к отклонению или завершению соединения, а также к появлению сообщения в журнале аудита безопасности и/или к уведомлению центра управления безопасностью.

5.3.5.3 Криптографические методы могут использоваться вместе с протоколами обмена с квитированием (handshaking) с целью защиты от повторной передачи перехваченных сообщений (т.е. для обеспечения отказоустойчивости).

5.3.5.4 Выбор методов обмена информацией аутентификации во многом зависит от условий их использования. В большинстве случаев эти методы используются в сочетании со следующими процедурами:

a) использование временных меток и синхронизированных часов;

b) двух- и трехнаправленный обмен с квитированием (для односторонней и взаимной аутентификации соответственно);

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

5.3.6 Механизм заполнения трафика

Механизм заполнения трафика применяется для обеспечения различных уровней защиты от анализа трафика. Применение механизма заполнения трафика может быть эффективным только в сочетании с услугой конфиденциальности.

5.3.7 Механизм управления маршрутизацией

5.3.7.1 Маршруты могут выбираться как динамически, так и статически, т.е. путем предварительного их планирования, при этом должны использоваться только физически защищенные подсети, ретрансляторы или каналы передачи данных.

5.3.7.2 При обнаружении постоянных попыток модификации данных оконечные системы могут передать провайдеру команду на установление соединения по другому маршруту.

5.3.7.3 Передача данных, имеющих определённые метки безопасности, через некоторые подсети, ретрансляторы или каналы передачи данных может

быть запрещена политикой безопасности. Кроме того, инициатор соединения (или источник блока данных в режиме без установления соединения) может установить запрет на использование определенных подсетей, каналов передачи данных или ретрансляторов.

5.3.8 Механизм нотаризации

Использование механизма нотаризации при передаче данных между двумя или несколькими логическими объектами обеспечивает подтверждение соответствия таких их характеристик, как целостность, источник, время и получатель. Подтверждение обеспечивается надежной третьей стороной (нотариусом), которой доверяют взаимодействующие логические объекты и которая обладает достаточной информацией, необходимой для предоставления запрашиваемого подтверждения посредством метода, допускающего проверку. Каждый сеанс обмена данными может использовать механизмы цифровой подписи, шифрования и целостности в соответствии с видом услуги, предоставляемой нотариусом. При использовании механизма нотаризации данные передаются между двумя взаимодействующими логическими объектами с помощью защищенных сеансов обмена информацией и через нотариуса.

5.4 Универсальные механизмы безопасности

В данном подразделе описаны механизмы, которые не являются специфичными для каждой отдельной услуги. Эти механизмы неявно описаны в разделе 7, как принадлежащие к любому отдельному уровню. Некоторые из этих универсальных механизмов безопасности могут рассматриваться как аспекты управления безопасностью (раздел 8). Назначение этих механизмов в основном прямо зависит от необходимого уровня безопасности.

5.4.1 Доверенные функциональные возможности

5.4.1.1 Доверенные функциональные возможности используются для расширения области применения или повышения эффективности других механизмов безопасности. Любые функциональные возможности, непосредственно обеспечивающие механизмы безопасности или доступ к ним, должны пользоваться доверием.

5.4.1.2 Процедуры, гарантирующие использование доверенных функциональных возможностей в соответствующих аппаратных и программных средствах, 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, реализация таких процедур дорогостояща и сложна. Эти проблемы могут быть минимизированы при выборе архитектуры, позволяющей реализовывать функции безопасности в модулях,

которые выполнены отдельно от функций, не связанных с безопасностью, 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, соответствующими доверенными функциональными возможностями.

5.4.2 Метки безопасности

Любые ресурсы, включающие элементы данных, могут иметь связанные с ними метки безопасности, предназначенные, например, для обозначения уровня чувствительности. Зачастую с передаваемыми данными необходимо передавать и соответствующую метку безопасности. Метка безопасности 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 источника или маршрута. Неявные метки безопасности 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 безопасности, включает в себя выявление видимых нарушений безопасности, а также обнаружение таких «стандартных» событий, как успешное получение права доступа (или вход в систему). События, относящиеся к безопасности, могут распознаваться логическими объектами в рамках ВОС, включая механизмы безопасности. Спецификация параметров, составляющих какое-либо событие, обеспечивается управлением обработкой событий (8.3.1).

Обнаружение событий, относящихся к безопасности, может, например, вызвать одно или несколько следующих действий:

a) выдача локального сообщения о событии;

b) выдача дистанционного сообщения о событии;

c) регистрация события в журнале аудита безопасности (5.4.4);

d) действие процедуры восстановления (5.4.5).

Примерами событий, относящихся к безопасности, могут быть следующие ситуации:

a) определённое нарушение безопасности;

b) выбранное специфическое событие;

c) переполнение счетчика количества ситуаций.

5.4.3.2 Стандартизация в области обнаружения события должна учитывать передачу соответствующей информации, которая связана 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 Журнал аудита безопасности

5.4.4.1 Журналы аудита безопасности обеспечивают надежный механизм безопасности, поскольку они предоставляют потенциальную возможность обнаружения и исследования нарушений безопасности путем проведения аудита безопасности.

Аудит безопасности предусматривает независимый просмотр и анализ системных записей и работы системы, позволяющий проверять адекватность системных функций управления, гарантировать соответствие принятой политике безопасности и операционным процедурам, обнаруживать нарушения безопасности и выдать рекомендации по любым конкретным изменениям в управлении, политике безопасности и процедурах.

Аудит безопасности требует регистрации соответствующей информации, относящейся к безопасности, в журнале аудита безопасности, анализа информации, извлекаемой из журнала аудита безопасности, а также уведомления о его результатах. Документирование или регистрация в журнале аудита безопасности рассматриваются в качестве механизма безопасности и описаны в настоящем разделе. Анализ и генерирование отчетов рассматриваются в качестве функции управления аудитом безопасности (8.3.2).

5.4.4.2 Сбор информации в журналах аудита безопасности может быть приспособлен к различным требованиям путем определения событий, относящихся к безопасности и подлежащих регистрации (например, видимые нарушения безопасности или успешные попытки доступа к системе). Сведения о наличии журналов аудита безопасности могут служить сдерживающим фактором для некоторых потенциальных нарушителей безопасности.

5.4.4.3 До начала ведения журналов аудита безопасности ВОС должно быть определено, какие события могут создавать записи, какая информация и при каких обстоятельствах должна дополнительно регистрироваться, а также какие синтаксические и семантические определения должны использоваться для обмена информацией с другими журналами аудита безопасности.

5.4.5 Процедура восстановления безопасности

5.4.5.1 Процедура восстановления безопасности, связанная с запросами от таких механизмов, как например, функции обработки событий и управления, выполняет действия по восстановлению в соответствии с используемым набором правил. Вышеуказанные действия могут быть трех типов:

a) немедленные;

b) временные;

c) долгосрочные.

Например

1 Немедленные действия могут привести к непосредственному прекращению операций, подобному разъединению соединения.

2 Временные действия могут привести к временной неработоспособности логического объекта.

3 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 управления восстановлением безопасности (8.3.3).

5.5 Иллюстрация взаимодействия услуг и механизмов безопасности

В таблице 1 приведены примеры механизмов, которые по отдельности или в сочетании с другими механизмами рассматриваются как приемлемые в некоторых случаях для обеспечения каждой услуги. Эта таблица представляет краткий обзор такого взаимодействия и не является исчерпывающей. Услуги и механизмы, приведенные в этой таблице, описаны в 5.2 и 5.3. Более подробное описание взаимодействия приведено в разделе 6.

Таблица 1 - Иллюстрация взаимодействия услуг и механизмов безопасности

Услуги	Механизмы							
	Шифрование	Цифровая подпись	Управление доступом	Целостность данных	Обмен данными аутентификации	Заполнение трафика	Управление маршрутизацией	Нотаризация
1	2	3	4	5	6	7	8	9
Аутентификация равноправного логического объекта	Да	Да	*	*	Да	*	*	*
Аутентификация источника данных	Да	Да	*	*	*	*	*	*
Услуга управления доступом	*	*	Да	*	*	*	*	*
Конфиденциальность в режиме с установлением соединения	Да	*	*	*	*	*	Да	*

Окончание таблицы 1

1	2	3	4	5	6	7	8	9
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 выбранного поля в режиме с установлением соединения	Да	*	*	Да	*	*	*	*
Целостность данных, передаваемых в режиме без установления соединения	Да	Да	*	Да	*	*	*	*
Целостность выбранного поля в режиме без установления соединения	Да	Да	*	Да	*	*	*	*
Неотказуемость с подтверждением источника	*	Да	*	Да	*	*	*	Да
Неотказуемость с подтверждением доставки	*	Да	*	Да	*	*	*	Да
Да – механизм считается приемлемым для использования, как в отдельности, так и в сочетании с другими механизмами; * - механизм считается неприемлемым для использования.								

6 Взаимодействие услуг, механизмов и уровней

6.1 Принципы многоуровневой безопасности

6.1.1 При распределении услуг безопасности по уровням с последующим размещением по уровням механизмов безопасности, используются следующие принципы:

a) количество альтернативных способов предоставления услуги должно быть минимальным;

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

c) необходимые для безопасности дополнительные функциональные возможности не должны дублировать существующие функции ВОС;

d) нарушение независимости уровня должно быть исключено;

e) количество доверенных функциональных возможностей должно быть минимальным;

f) если логический объект зависит от механизма безопасности, который обеспечивается каким-либо логическим объектом нижерасположенного уровня, то любые промежуточные уровни должны быть построены таким образом, чтобы нарушение безопасности было бы практически невозможным;

g) дополнительные функции безопасности уровня по возможности должны быть определены таким образом, чтобы реализация отдельного(ых) самостоятельного(ых) модуля(ей) была исключена;

h) настоящий стандарт применим к открытым системам, состоящим из оконечных систем, которые содержат все семь уровней, и к ретрансляционным системам.

6.1.2 На каждом уровне, в целях обеспечения запросов для услуг безопасности, независимо от того, обеспечиваются ли запрашиваемые услуги на данном или нижерасположенном уровнях, могут потребоваться модификации определений услуг.

6.2 Модель вызова, управления и использования защищенных (N)-услуг

Данный подраздел необходимо рассматривать совместно с разделом 8, который содержит общее описание принципов управления безопасностью. Имеется в виду, что услуги и механизмы безопасности могут быть активизированы логическим объектом управления через интерфейс управления и/или посредством вызова услуги.

6.2.1 Определение средств защиты для сеансов обмена данными

6.2.1.1 Общие положения

В данном подразделе описано использование средств защиты для сеансов обмена данными в режимах с установлением и без установления соединения. В случае сеанса обмена данными в режиме с установлением соединения, услуги безопасности обычно запрашиваются/подтверждаются во время установления соединения. В случае сеанса обмена данными в режиме без установления соединения услуги безопасности запрашиваются/подтверждаются при каждом вызове примитива «UNITDATA запрос».

В дальнейшем, для упрощения описания термин «запрос услуги» будет означать установление соединения или передачу примитива «UNITDATA запрос». Вызов защиты для выбранных данных может быть произведен с помощью запроса защиты выбранных полей.

Например, это может быть выполнено посредством установления нескольких соединений, отличающихся по типам или уровням защиты.

Такая архитектура безопасности позволяет использовать разнообразные политики безопасности, включая идентификационную и инструкционную политики безопасности, а также политики безопасности смешанного типа. Архитектура безопасности также позволяет использовать административно заданную защиту, динамически выбранную защиту или защиту смешанного типа.

6.2.1.2 Запросы услуги

При каждом запросе (N)-услуги (N+1)-логический объект может запросить защиту, определенную в задании по безопасности. При запросе (N)-услуги одновременно определяются как услуга безопасности, так параметры и необходимая дополнительная информация (например, чувствительность информации и/или метки безопасности) согласно заданию по безопасности.

Перед каждым сеансом обмена данными (N+1)-уровень должен обратиться к ИБУБ (8.1). ИБУБ содержит информацию об административно заданных требованиях по безопасности относительно (N+1)-логического объекта. Доверенные функциональные возможности необходимы для усиления этих требований.

При предоставлении средств защиты во время сеанса обмена данными в режиме с установлением соединения может потребоваться согласование запрашиваемых услуг безопасности. Процедуры, необходимые для согласования механизмов и параметров безопасности, могут выполняться как отдельные процедуры или являться неотъемлемой частью обычных процедур установления соединения.

Когда согласование выполняется как отдельная процедура, то результаты согласования (т.е. согласованные тип механизма и параметры безопасности, необходимые для обеспечения соответствующих услуг безопасности) вводятся в ИБУБ (8.1).

Когда же согласование выполняется как неотъемлемая часть обычной процедуры установления соединения, то результаты согласования между (N)-логическими объектами будут временно сохранены в ИБУБ. Перед согласованием каждый (N)-логический объект должен обратиться к ИБУБ для получения информации, необходимой для согласования.

(N)-уровень должен отклонить запрос услуги, если при этом нарушаются административно заданные требования, которые зарегистрированы в ИБУБ для (N+1)-логического объекта.

(N)-уровень дополнительно к запрашиваемым услугам безопасности должен предоставить любые услуги безопасности, которые определены в ИБУБ как обязательные для выполнения требований задания по безопасности.

Если для (N+1)-логического объекта не определено задание по безопасности, то (N)-уровень будет подчиняться политике безопасности в соответствии с информацией, имеющейся в ИБУБ. В результате по умолчанию обмен данными будет происходить с использованием средств защиты в пределах диапазона, определенного в ИБУБ для (N+1)-логического объекта.

6.2.2 Предоставление услуг безопасности

После определения совокупности административно заданных и динамически выбранных требований, как описано в 6.2.1, (N+1)-уровень будет пытаться достичь, как минимум, заданной защиты.

Это может быть достигнуто одним или двумя следующими методами:

a) запуск механизмов безопасности непосредственно в пределах (N)-уровня; и/или

b) запрос услуг безопасности из (N-1)-уровня. В этом случае область применения безопасности должна быть распространена на (N)-услугу с помощью совокупности доверенных функциональных возможностей и/или специальных механизмов безопасности в (N)-уровне.

Примечание - Последнее не обязательно означает, что все функциональные возможности на (N)-уровне должны быть доверенными.

Таким образом, (N)-уровень определяет свою способность выполнить требования заданной защиты. При отсутствии у него таких возможностей обмен данными не происходит.

6.2.2.1 Установление защищенного (N)-соединения

Далее будет подробно рассмотрено предоставление услуг в пределах (N)-уровня (в отличие от использования функций (N-l)-услуг).

В некоторых протоколах для гарантированного выполнения требований заданной защиты критической является последовательность следующих операций:

a) управление исходящим доступом. (N)-уровень может предусматривать средства управления исходящим доступом, т.е. он может локально определять (со стороны ИБУБ) разрешено ли ему установление защищенного (N)-соединения;

b) аутентификация равноправного логического объекта. Если защита конкретного объекта включает аутентификацию равноправного логического объекта или если известно (со стороны ИБУБ), что (N)-объект получателя будет запрашивать аутентификацию равноправного логического объекта, то должен иметь место обмен информацией аутентификации. При выполнении последней процедуры может потребоваться использование двух- или трехнаправленного квитирования для обеспечения 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, а также промежуточные логические объекты могут наложить ограничения на управление доступом. Если удаленный механизм управления доступом запрашивает специальную информацию, то инициирующий (N)-логический объект предоставляет эту информацию в пределах протокола (N)-уровня или по каналам управления;

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

e) целостность данных. Если была выбрана целостность всех (N)-данных пользователя с восстановлением или без восстановления, либо целостность отдельных полей, то должно быть установлено защищенное (N)-соединение. Это соединение может быть тем же, которое было 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 неотказуемости. Если выбрана услуга неотказуемости с подтверждением источника, то должны быть установлены соответствующие криптографические параметры или защищенное соединение с логическим объектом нотаризации. Если была выбрана услуга неотказуемости с подтверждением доставки, то должны быть установлены соответствующие параметры (которые отличаются от запрашиваемых параметров при услуге неотказуемости с подтверждением источника) или защищенное соединение с логическим объектом нотаризации.

Примечание — Установление защищенного (N)-соединения может оказаться безуспешным из-за несогласованности криптографических параметров (возможно из-за отсутствия соответствующих ключей) или из-за отказа механизма управления доступом.

6.2.3 Функционирование защищенного (N)-соединения

6.2.3.1 На этапе передачи данных по защищенному (N)-соединению должны обеспечиваться согласованные услуги безопасности.

На границе (N)-услуги должны наблюдаться следующие услуги:

a) аутентификация равноправного логического объекта (по интервалам);

b) защита выбранных полей;

c) уведомление об активной атаке (например, когда происходит модификация данных и предоставляется услуга «Целостность в режиме с установлением соединения без восстановления» - 5.2.4.2).

Кроме того, может потребоваться:

a) запись в журнал аудита безопасности;

b) обнаружение и обработка события.

6.2.3.2 Также могут выборочно использоваться следующие услуги:

a) конфиденциальность;

b) целостность данных (возможно с аутентификацией);

c) неотказуемость (получателя или источника).

Примечания

1 Для маркировки тех элементов данных, к которым будут применяться выбранные услуги, предлагается использовать два метода.

Первый метод предполагает использование строгого контроля данных. Предполагается, что уровень представления данных будет распознавать определенные данные, которые требуют применения определенных услуг безопасности.

Второй метод предполагает маркировку отдельных элементов данных, к которым будут применяться специальные услуги безопасности.

2 Одна из причин избирательного применения услуги безопасности «неотказуемость» может вытекать из следующего сценария. Перед тем, как оба (N)-логических объекта придут к соглашению, что окончательная версия элемента данных является взаимоприемлемой, между ними по ассоциации происходит некоторый диалог согласования. Предполагаемый получатель может запросить у источника данных услугу «неотказуемость» (с подтверждением как источника, так и доставки) для получения окончательной согласованной версии элемента данных. Источник запрашивает и получает обе услуги, затем передает элемент данных и впоследствии принимает уведомление и подтверждение о приеме получателем указанного элемента данных. Услуга безопасности «неотказуемость» оповещает источник и получателя элемента данных о том, что этот элемент был успешно принят.

3 Обе услуги безопасности «неотказуемость» (т.е. с подтверждением источника и доставки) активизируются источником.

6.2.4 Обеспечение защищенной передачи данных в режиме без установления соединения

Не все услуги безопасности, 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, необходимо предусмотреть защиту от удаления, вставок и повторной передачи перехваченных сообщений. Ограниченная защита информации от угрозы повторного использования

может быть обеспечена с помощью механизма установления временных меток. Кроме того, многие услуги безопасности не способны обеспечивать ту степень безопасности, которая может быть достигнута в протоколах режима с установлением соединения.

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

a) аутентификация равноправного логического объекта (5.2.1.1);

b) аутентификация источника данных (5.2.1.2);

c) управление доступом (5.2.2);

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

e) конфиденциальность выбранного поля (5.2.3.3);

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

g) целостность выбранного поля в режиме без установления соединения (5.2.4.5);

h) неотказуемость с подтверждением источника (5.2.5.1).

Эти услуги обеспечиваются с помощью механизмов шифрования, цифровой подписи, управления доступом, маршрутизации, целостности данных и/или нотаризации (5.3). Инициатор передачи данных в режиме без установления соединения должен гарантировать, что каждый отдельный СБД содержит всю информацию, которая необходима для распознавания этого СБД на стороне получателя.

7 Размещение услуг и механизмов безопасности

В данном разделе определены те услуги безопасности, которые должны обеспечиваться в рамках базовой эталонной модели ВОС, а также описаны методы получения этих услуг. В зависимости от предъявляемых требований дополнительно предоставляется любая услуга безопасности.

Если в данном разделе конкретная услуга безопасности определена как дополнительно предоставляемая на определенном уровне, то, если не оговорено иное, эта услуга обеспечивается механизмами безопасности, которые функционируют внутри этого уровня. Как описано в разделе 6, многие уровни могут предложить конкретные услуги безопасности.

Такие уровни не всегда могут обеспечить услуги безопасности самостоятельно, однако они могут использовать необходимые услуги безопасности, которые предоставляют нижерасположенные уровни.

В том случае, когда внутри какого-либо уровня не предусмотрены какие-либо услуги безопасности, то может потребоваться некоторая модификация определённых услуг этого уровня, позволяющая запрашивать услуги безопасности из нижерасположенного уровня.

Примечания

1 В настоящем разделе не рассматриваются универсальные механизмы безопасности (5.4).

2 Выбор позиции механизмов шифрования для приложений рассмотрен в приложении С.

7.1 Физический уровень

7.1.1 Услуги

На физическом уровне предусматриваются следующие услуги безопасности, которые используются 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) конфиденциальность всего потока трафика, которая может быть обеспечена только в определенных ситуациях, например, при полнодуплексной, синхронной и двухпунктовой передаче;

b) конфиденциальность ограниченного потока трафика, которая может быть обеспечена при других типах передачи, например, при асинхронной передаче.

Эти услуги безопасности могут нейтрализовать только пассивные угрозы при использовании двух- и многопунктовых звеньев данных.

7.1.2 Механизмы

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

Специфическая форма шифрования, применяемая только на физическом уровне, обеспечивает безопасность передачи (т.е. безопасность трафика в среде передачи).

Безопасность физического уровня обеспечивается устройством шифрования, работающим в прозрачном режиме. Предназначение безопасности на физическом уровне заключается в том, чтобы полностью защитить цифровой поток службы обработки и передачи данных физического уровня, а также обеспечить конфиденциальность потока трафика.

7.2 Канальный уровень

7.2.1 Услуги

Канальный уровень обеспечивает следующие услуги безопасности:

a) конфиденциальность в режиме с установлением соединения;

b) конфиденциальность в режиме без установления соединения.

7.2.2 Механизмы

Для обеспечения услуг безопасности на канальном уровне используются механизмы шифрования (приложение С).

Функции безопасности на канальном уровне выполняются до выполнения обычных функций уровня по передаче и после выполнения

обычных функций уровня по приему, т.е. механизмы безопасности строятся на основе обычных функций уровня и используют эти функции.

Механизмы шифрования на канальном уровне чувствительны к протоколу канального уровня.

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, независящая от подсети;

d) ретрансляция и маршрутизация (2.4).

7.3.1 Услуги

К услугам безопасности, которые обеспечиваются протоколом, выполняющим функции доступа к подсети, относящиеся к обеспечению услуг сетевого уровня ВОС, относятся:

a) аутентификация равноправного логического объекта;

b) аутентификация источника данных;

c) управление 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 безопасности могут обеспечиваться как по отдельности, так и в комбинации. Услуги безопасности, 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 безопасности.

На этом уровне выполняется маршрутизация и, следовательно, поэтому в нем предусмотрено управление маршрутизацией. Определённые услуги безопасности обеспечиваются следующим образом:

a) услуга аутентификации равноправного логического объекта обеспечивается соответствующей комбинацией обмена криптографически

полученной или защищенной информацией аутентификации, защищенного обмена паролями или механизмов цифровой подписи;

b) услуга аутентификации источника данных обеспечивается механизмами шифрования или цифровой подписи;

c) услуга управления доступом обеспечивается конкретными механизмами управления доступом;

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

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

f) услуга конфиденциальности потока трафика обеспечивается 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 обеспечивается механизмом целостности данных, иногда в комбинации с механизмом шифрования;

h) услуга целостности в режиме без установления соединения также обеспечивается механизмом целостности данных, иногда в комбинации с механизмом шифрования.

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

Защита подсети, устанавливаемая её администрацией в соответствии с требованиями протоколов доступа к подсети, обычно используется перед выполнением обычных функций подсети по передаче и после выполнения обычных функций подсети по приему.

7.3.2.3 Механизмы протокола, выполняющего операции ретрансляции и маршрутизации между двумя оконечными системами в комбинации с услугами сетевого уровня ВОС, обеспечивают услуги в рамках одной или нескольких взаимосвязанных сетей.

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

7.3.2.4 Управление доступом на сетевом уровне служит многим целям. Например, оно позволяет оконечной системе управлять установлением соединений и отклонять нежелательные вызовы. Управление доступом на сетевом уровне также позволяет одной или нескольким подсетям управлять

использованием ресурсов сетевого уровня. В некоторых случаях эта последняя функция связана с начислением оплаты за пользование сетью.

Примечание – При установлении соединения сетевого уровня часто может производиться начисление 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 Необходимость механизмов управления доступом со стороны протокола, выполняющего операции доступа к подсети, связанные с обеспечением сетевых услуг ВОС между оконечными системами, может быть оговорена в требованиях конкретной подсети. Если такие механизмы управления доступом обеспечиваются протоколом, выполняющим 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 только весьма приблизительно определять различия между логическими объектами сетевого уровня.

7.3.2.6 В том случае, если на сетевом уровне заполнение трафика используется совместно с механизмом шифрования (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 безопасности, используемые по отдельности или в комбинации:

a) аутентификация равноправного логического объекта;

b) аутентификация источника данных;

c) управление 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 безопасности:

a) аутентификация равноправного логического объекта обеспечивается соответствующей комбинацией криптографически полученной или

защищенной информации обменной аутентификации, защищенного обмена паролями и механизмов цифровой подписи;

b) аутентификация источника данных обеспечивается механизмами шифрования или цифровой подписи;

c) управление доступом обеспечивается путем соответствующего использования конкретных механизмов управления доступом;

d) конфиденциальность в режиме с установлением соединения обеспечивается механизмом шифрования;

e) конфиденциальность в режиме без установления соединения обеспечивается механизмом шифрования;

f) целостность в режиме с установлением соединения с восстановлением обеспечивается путем использования механизма целостности данных, иногда в комбинации с механизмом шифрования;

g) целостность в режиме с установлением соединения без восстановления обеспечивается путем использования механизма целостности данных, иногда в комбинации с механизмом шифрования;

h) целостность в режиме без установления соединения обеспечивается путем использования механизма целостности данных, иногда в комбинации с механизмом шифрования.

Механизмы безопасности должны функционировать таким образом, чтобы услуги безопасности можно было использовать для отдельных соединений транспортного уровня. Необходимо обеспечить такую защиту, при которой отдельные соединения транспортного уровня будут изолированы от всех его остальных соединений.

7.5 Сеансовый уровень

7.5.3 Услуги

На сеансовом уровне не предусматриваются какие-либо услуги безопасности.

7.6 Уровень представления данных

7.6.1 Услуги

Уровень представления данных обеспечивает функциональные возможности в поддержку следующих услуг безопасности, 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 безопасности:

d) конфиденциальность потока трафика;

e) аутентификация равноправного логического объекта;

f) аутентификация источника 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) неотказуемость с подтверждением источника;

p) неотказуемость с подтверждением доставки.

Примечание - Функциональные возможности уровня представления данных 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

На уровне представления данных могут быть размещены механизмы, поддерживающие нижеперечисленные услуги безопасности (в этом случае они могут использоваться совместно с механизмами безопасности прикладного уровня для поддержки его услуг безопасности):

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

b) услуга аутентификации источника данных может быть обеспечена механизмами шифрования или цифровой 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 выбранного 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 неотказуемости с подтверждением источника может быть обеспечена соответствующей комбинацией механизмов целостности данных, цифровой подписи и нотаризации;

p) услуга неотказуемости с подтверждением доставки может быть обеспечена соответствующей комбинацией механизмов целостности данных, цифровой подписи и нотаризации.

Механизмы шифрования, используемые для обеспечения передачи данных и расположенные на верхних уровнях, должны удерживаться и на уровне представления данных.

Некоторые из перечисленных выше услуг безопасности могут быть альтернативно обеспечены механизмами безопасности, которые целиком расположены в пределах прикладного уровня.

Только услуги безопасности, которые относятся к конфиденциальности, могут быть полностью обеспечены механизмами безопасности, содержащимися на уровне представления данных.

Механизмы безопасности на уровне представления данных функционируют в качестве заключительной стадии преобразования синтаксиса 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 безопасности, используемых как по отдельности, так и в комбинации:

a) аутентификация равноправного логического объекта;

b) аутентификация источника данных;

c) управление 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) неотказуемость с подтверждением источника;

q) неотказуемость 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 безопасности в сеансе обмена данными, включая конфиденциальность данных, целостность и аутентификацию, может осуществляться управлением безопасностью ВОС или управлением прикладного уровня на основе информации, которая содержится в ИБУБ в дополнение к запросам, выдаваемым прикладным процессом.

7.7.2 Механизмы

Услуги безопасности на прикладном уровне обеспечиваются с помощью следующих механизмов:

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

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

c) услуга управления доступом к тем аспектам реальной открытой системы, которые являются постоянными для ВОС, например, способность реальной открытой системы связываться с конкретными системами или удаленными прикладными объектами, может быть обеспечена комбинацией 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 данных;

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 данных;

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 данных;

p) услуга неотказуемости с подтверждением источника может быть обеспечена соответствующей комбинацией механизмов целостности данных и цифровой подписи на нижерасположенном уровне, возможно в комбинации с нотаризацией третьей стороной;

q) услуга неотказуемости с подтверждением доставки может быть обеспечена соответствующей комбинацией механизмов целостности данных и цифровой подписи на нижерасположенном уровне, возможно в комбинации с нотаризацией третьей стороной.

Для обеспечения услуги неотказуемости используется механизм нотаризации, который 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 разногласий. Механизм нотаризации может также использовать услуги безопасности, предоставляемые нижерасположенными уровнями.

7.7.3 Услуги безопасности, не входящие в сферу ВОС

Прикладные процессы могут сами по существу обеспечивать все услуги и использовать те же типы механизмов, которые были описаны в настоящем стандарте как механизмы, соответствующим образом размещен-

ные на различных уровнях архитектуры. Такое использование не входит в область рассмотрения ВОС, однако оно не является несовместимым с определениями услуг и протоколов, а также с архитектурой ВОС.

7.8 Иллюстрация взаимодействия услуг и уровней безопасности

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

Таблица 2 - Иллюстрация взаимодействия услуг и уровней безопасности

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 выбранного поля	●	●	●	●	●	●	Да
Конфиденциальность потока трафика		●	Да	●	●	●	Да
Целостность в режиме с установлением соединения с восстановлением	Да	●	●	Да	●	●	Да
Целостность в режиме с установлением соединения без восстановления	●	●	Да	Да	●	●	Да
Целостность выбранного поля в режиме с установлением соединения	●	●	●	●	●	●	Да
Целостность данных, передаваемых в режиме без установления соединения	●	●	Да	Да	●	●	Да
Целостность выбранного поля в режиме без установления соединения	●	●	●	●	●	●	Да
Неотказуемость с подтверждением источника	●	●	●	●	●	●	Да
Неотказуемость с подтверждением доставки	●	●	●	●	●	●	Да

Да - применимость данного типа услуги на определенном уровне;

● - не обеспечивается.

* - относительно 7 уровня следует отметить, что прикладной процесс может сам обеспечивать услуги безопасности

Примечания

1 При составлении таблицы 2 не ставилась задача показать, что ее элементы имеют одинаковую важность и значимость; наоборот, существует значительная градация масштаба в пределах табличных данных.

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

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

8 Управление безопасностью

8.1 Общие положения

8.1.1 Управление безопасностью ВОС касается тех аспектов управления безопасностью, которые относятся к ВОС и к безопасности управления ВОС.

Аспекты управления безопасностью ВОС связаны с теми операциями, которые не относятся к обычным сеансам обмена данными, но которые необходимы для управления и обеспечения аспектами безопасности этих обменов данными.

Примечание - Доступность услуги обмена данными определяется построением сети и/или протоколами управления сетью. Для предотвращения отказа в обслуживании необходим соответствующий выбор этих протоколов.

8.1.2 Может существовать несколько политик безопасности распределенных открытых систем, разработанных администрацией(ями) в соответствии со стандартами управления безопасностью ВОС. Объекты, которые подчиняются отдельной политике безопасности, разработанной отдельной администрацией, иногда объединяются в так называемую «область безопасности». Области безопасности и их взаимосвязи являются важной сферой для будущего расширения.

8.1.3 Управление безопасностью ВОС относится к управлению услугами и механизмами безопасности ВОС. Такое управление требует распределения информации управления между услугами и механизмами, а также сбора информации, относящейся к работе этих услуг и механизмов. Примерами могут служить распределение криптографических ключей, установка административно задаваемых параметров выбора безопасности, выдача сообщений как о стандартных, так и об аварийных ситуациях безопасности (журнал аудита безопасности), а также активизация и дезактивизация услуг. Управление безопасностью не касается прохождения информации, относящейся к безопасности, в протоколах, которые привлекают специальные услуги безопасности (например, в параметрах запроса на соединение).

8.1.4 ИБУБ является концептуальным хранилищем всей информации, относящейся к безопасности, которая необходима открытым системам. Эта

концепция не рекомендует использование какой-либо формы для хранения или реализации информации. Тем не менее, каждая оконечная система должна содержать необходимую локальную информацию, которая позволяет ей приводить в действие соответствующую политику безопасности. ИБУБ является распределенной информационной базой с такой степенью распределения, которая необходима для обеспечения согласованной политики безопасности в (логической или физической) группе оконечных систем. На практике области ИБУБ могут и не входить в состав ИБУ.

Примечание - Может существовать множество реализаций ИБУБ, например:

a) таблица данных;

b) файл;

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

8.1.5 Протоколы управления, особенно протоколы управления безопасностью, и каналы передачи данных, по которым передается информация управления, являются потенциально уязвимыми. Вследствие этого особое внимание следует уделять проверке защиты этих протоколов и информации управления безопасностью, чтобы не была ослаблена защита безопасности, предоставляемая для обычных сеансов обмена данными.

8.1.6 При управлении безопасностью может возникнуть потребность в обмене информацией, относящейся к безопасности, между различными системными администраторами, с целью установления или расширения ИБУБ. В некоторых случаях информация, относящаяся к безопасности, будет проходить по маршрутам обмена данными, которые существуют вне ВОС, и тогда локальные системные администраторы будут модифицировать содержимое ИБУБ методами, не стандартизованными в рамках ВОС. В других случаях целесообразно организовать обмен подобной информацией по маршрутам обмена данными ВОС, тогда информация будет передаваться между двумя прикладными системами управления безопасностью, реализованными в рамках реальной открытой системы. Прикладные системы управления безопасностью будут использовать передаваемую по маршрутам обмена данными информацию для модификации ИБУБ. Это может потребовать предварительной авторизации соответствующего администратора безопасности.

8.1.7 Для обмена информацией, относящейся к безопасности, по каналам обмена данными ВОС должны быть определены прикладные протоколы.

8.2 Категории управления безопасностью ВОС

Существует три категории деятельности в области управления безопасностью ВОС:

a) управление безопасностью системы;

b) управление услугами безопасности;

c) управление механизмами безопасности.

Кроме того необходимо учитывать безопасность самого управления ВОС (8.2.4). Ниже описаны ключевые функции, выполняемые этими категориями управления безопасностью.

8.2.1 Управление безопасностью системы

Управление безопасностью системы рассматривается с точки зрения аспектов управления безопасностью всей функциональной среды ВОС. Приведенный ниже перечень типичен для действий, которые попадают в категорию управления безопасностью:

a) управление общей политикой безопасности, включая корректировку и поддержание совместимости;

b) взаимодействие с другими функциями управления ВОС;

c) взаимодействие с управлением услугами и механизмами безопасности;

d) управление обработкой событий (8.3.1);

e) управление аудитом безопасности (8.3.2);

f) управление восстановлением безопасности (8.3.3).

8.2.2 Управление услугами безопасности

Управление услугами безопасности относится к управлению конкретными услугами безопасности. Приведенный ниже перечень типичен для действий, которые выполняются при управлении конкретной услугой безопасности:

a) определение в задании по безопасности и предоставление необходимой защиты для услуги;

b) назначение и поддержание правил выбора (при наличии альтернативы) конкретного механизма безопасности, используемого для обеспечения запрашиваемой услуги безопасности;

c) согласование (локальное или удаленное) доступных механизмов безопасности, которые требуют предварительной настройки управления;

d) привлечение конкретных механизмов безопасности посредством соответствующей функции управления механизмами безопасности, например, для обеспечения административно задаваемых услуг безопасности;

e) взаимодействие с другими функциями управления услугами и механизмами безопасности.

8.2.3 Управление механизмами безопасности

Управление механизмами безопасности относится к управлению конкретными механизмами безопасности. Приведенный ниже перечень функций управления механизмами безопасности является типичным, но не исчерпывающим:

a) управление ключами;

b) управление шифрованием;

c) управление цифровой подписью;
d) управление контролем доступа;
e) управление целостностью данных;
f) управление аутентификацией;
g) управление заполнением трафика;
h) управление маршрутизацией;
j) управление нотаризацией.

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

8.2.4 Безопасность управления ВОС

Безопасность всех функций управления и обмена информацией управления ВОС является важной составной частью безопасности ВОС. В целях обеспечения адекватной безопасности протоколов и информации управления (8.1.5), данная категория управления безопасностью требует соответствующего выбора вышеперечисленных услуг и механизмов безопасности ВОС. Например, при обмене данными между логическими объектами управления с использованием ИБУ, обычно необходимо выбрать какую-то форму защиты.

8.3 Специальные функции управления безопасностью системы

8.3.1 Управление обработкой событий

Аспекты управления обработкой событий, распознаваемых в ВОС, представляют собой удаленную выдачу сообщений об очевидных попытках нарушения безопасности системы и изменении допустимых значений, используемых для инициирования выдачи сообщений об этих событиях.

8.3.2 Управление аудитом безопасности

Управление аудитом безопасности может включать следующие функции:

a) выбор событий, подлежащих регистрации и/или удаленному сбору;
b) разрешение и запрещение регистрации отдельных событий в системном журнале аудита безопасности;
c) удаленный сбор отдельных записей аудита;
d) подготовка отчетов по результатам аудита безопасности.

8.3.3 Управление восстановлением безопасности

Управление восстановлением безопасности может включать следующие функции:

a) поддержание правил реагирования на реальные или предполагаемые нарушения безопасности;

b) удаленная выдача сообщений об очевидных нарушениях безопасности системы;

c) взаимодействие администраторов безопасности.

8.4 Функции управления механизмами безопасности

8.4.1 Управление ключами

Управление ключами может включать следующие функции:

a) генерация соответствующих ключей в интервалы времени, соизмеримые с требуемым уровнем безопасности;

b) определение в соответствии с требованиями по управлению доступом тех логических объектов, которые должны получать копию каждого ключа;

c) обеспечение безопасного доступа или распределения ключей по запросам логических объектов в реальных открытых системах.

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

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

8.4.2 Управление шифрованием

Управление шифрованием может включать следующие функции:

a) взаимосвязь с управлением ключами;

b) установление криптографических параметров;

c) криптографическая синхронизация.

Наличие механизма шифрования подразумевает использование управления ключами и общих методов ссылок к криптографическим алгоритмам.

Степень избирательности защиты, обеспечиваемой шифрованием, определяется теми логическими объектами внутри функциональной среды ВОС, которым присваиваются независимые ключи. В общем случае, это определяется архитектурой безопасности и в частности механизмом управления ключами.

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

8.4.3 Управление цифровой подписью

Управление цифровой подписью включает следующие функции:

a) взаимосвязь с управлением ключами;

b) установление криптографических параметров и алгоритмов;

c) использование протокола между взаимодействующими логическими объектами, а может быть и с третьей стороной.

Примечание - В общем случае управление цифровой подписью во многом аналогично управлению шифрованием.

8.4.4 Управление доступом

Управление доступом может предусматривать распределение атрибутов безопасности (включая пароли) или модификацию списков управления доступом или списков полномочий. Оно также может предусматривать использование протокола между взаимодействующими логическими объектами и другими логическими объектами, обеспечивающими услуги управления доступом.

8.4.5 Управление целостностью данных

Управление целостностью данных включает следующие функции:

a) взаимосвязь с управлением ключами;

b) установление криптографических параметров и алгоритмов;

c) использование протокола между взаимодействующими логическими объектами.

Примечание - Обеспечение целостности данных с помощью криптографических методов во многом аналогично управлению целостностью данных и управлению шифрованием.

8.4.6 Управление аутентификацией

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

8.4.7 Управление заполнением трафика

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, например, длины;

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

8.4.8 Управление маршрутизацией

Управление маршрутизацией может охватывать определение звеньев данных или подсетей, которые считаются защищенными или доверенными относительно конкретных критериев.

8.4.9 Управление нотаризацией

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 безопасности в рамках ВОС

А.1 Основные положения

Данное приложение содержит:

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

b) основные положения архитектуры по применению различных средств безопасности и требований к ним.

Безопасность функциональной среды ВОС представляет собой один из аспектов безопасности обработки/передачи данных. Для обеспечения эффективности средств защиты, используемых в функциональной среде ВОС, необходимо наличие дополнительных средств, находящихся вне ВОС. Например, информация, передаваемая между системами, может быть зашифрована, но в том случае, если при управлении доступом к системам не используются физические меры защиты, шифрование окажется напрасным.

Кроме того, только взаимосвязанные системы имеют отношение к ВОС. Для обеспечения большей эффективности средств защиты ВОС, необходимо использовать их совместно со средствами, находящимися вне ВОС.

А.2 Требования к безопасности

А.2.1 Что понимается под безопасностью?

Смысл термина «безопасность» означает минимизацию уязвимостей активов и ресурсов. Любой актив обладает какой-либо ценностью. Уязвимость - это слабое место, которое может быть использовано для нарушения целостности системы или содержащейся в ней информации. Угроза - это потенциально возможное нарушение безопасности.

А.2.2 Обоснование безопасности в открытых системах

Международная организация по стандартизации (International Organization for Standardization, ISO**)** признала необходимость разработки целого семейства стандартов в области безопасности архитектуры ВОС. Такая необходимость обусловлена следующими причинами:

a) увеличение зависимости общества от средств вычислительной техники, которые доступны по каналам передачи данных или взаимосвязаны посредством этих каналов, и которым требуется защита от воздействия различных угроз;

b) появление во многих странах законодательства в области защиты данных, которое обязывает провайдеров обеспечивать целостность систем и защиту персональной информации;

c) желание различных организаций использовать стандарты ВОС, при необходимости усовершенствованные, на действующих и проектируемых безопасных системах.

A.2.3 Что подлежит защите?

В общем случае защите подлежит нижеследующее:

a) информация и данные (включая программное обеспечение и данные, относящиеся к пассивным мерам безопасности, например, пароли);

b) услуги передачи и обработки данных;

c) оборудование и средства.

A.2.4 Угрозы

Угрозами для системы передачи данных являются:

a) разрушение информации и/или других ресурсов;

b) искажение или модификация информации;

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

d) раскрытие информации;

e) прекращение обслуживания.

Угрозы могут быть классифицированы как случайные и преднамеренные, а также как активные и пассивные.

A.2.4.1 Случайные угрозы

Случайные угрозы - это угрозы, возникающие непреднамеренно. Примерами реализации случайных угроз могут служить нарушения работоспособности системы, грубые эксплуатационные ошибки и ошибки в программном обеспечении.

A.2.4.2 Преднамеренные угрозы

К преднамеренным угрозам относятся различные угрозы: от угрозы случайного анализа, использующего легкодоступную проверку инструментальных средств до угрозы изощренных атак с использованием специальных сведений о системе. Реализация преднамеренной угрозы рассматривается как «атака».

A.2.4.3 Пассивные угрозы

К пассивным угрозам относятся угрозы, которые при их реализации не приводят к какой-либо модификации информации, содержащейся в системе(ах), и которые не влияют на работу и состояние системы. Реализация пассивной угрозы представляет собой пассивный перехват информации, передаваемой по каналам передачи данных.

A.2.4.4 Активные угрозы

Реализация активных угроз предполагает внесение изменений в информацию, содержащуюся в системе, режим работы или состояние

системы. Примером реализации активной угрозы служит умышленное изменение таблиц маршрутизации системы неправомочным пользователем.

A.2.5 Некоторые специфичные виды атак

Далее будут кратко рассмотрены некоторые виды атак, специфичные для функциональной среды передачи/обработки данных. В следующих разделах будут встречаться термины «авторизованный» («санкционированный») и «неавторизованный» («несанкционированный»). «Авторизация» означает «предоставление прав». Такое определение подразумевает два аспекта:

- рассматриваемые права являются правами на выполнение некоторых действий (например, доступ к данным);
- права предоставлены некоторому логическому объекту, доверенному лицу или процессу.

Таким образом, санкционированное поведение является рабочей характеристикой тех действий, для выполнения которых предоставляются (а не аннулируются) права. Более подробное описание процесса авторизации приведено в A.3.3.1.

A.2.5.1 Маскарад

Маскарад имеет место быть, когда какой-либо логический объект претендует на то, чтобы выглядеть подобно другому логическому объекту. Маскарад обычно используется вместе с некоторыми другими формами активных атак, особенно, с повторным использованием и модификацией сообщений. Например, имевшие место действительные последовательности аутентификации могут быть перехвачены и затем повторно использованы. Авторизованный логический объект, обладающий небольшим числом привилегий, может использовать маскарад для получения дополнительных привилегий путем исполнения роли логического объекта, имеющего такие привилегии.

A.2.5.2 Повторное использование

Повторное использование имеет место быть, когда сообщение или часть сообщения повторяется с целью получения несанкционированного результата. Например, действительное сообщение, содержащее информацию аутентификации, может быть повторно использовано другим логическим объектом для того, чтобы заявить о своей подлинности (как о чём-то таком, чего не существует).

A.2.5.3 Модификация сообщений

Модификация сообщений имеет место быть тогда, когда не обнаруживаются изменения содержимого передачи, и это приводит к некоторому несанкционированному результату, как например, в случае, когда сообщение «Разрешить Джону Смиту читать секретный файл "счета"» заменяется на сообщение «Разрешить Фреду Брауну читать секретный файл "счета"».

A.2.5.4 Отказ в обслуживании

Отказ в обслуживании происходит, когда логический объект перестает выполнять свойственные ему функции или он действует таким образом, что препятствует другим логическим объектам выполнять свойственные им функции. Атака может быть общей, это когда логический объект блокирует передачу всех сообщений, или же она может преследовать определенную цель, тогда логический объект блокирует передачу всех сообщений, отправляемых конкретному получателю, например, сообщений услуги аудита безопасности. Результатом этой атаки может быть блокирование трафика, как описано в данном примере, или генерация дополнительного трафика. Возможна также генерация сообщений, предназначенных для нарушения работы сети, особенно если в сети имеются логические объекты-ретрансляторы, которые принимают решения о маршрутизации на основе отчетов о состоянии, полученных от других логических объектов-ретрансляторов.

A.2.5.5 Внутренние атаки

Внутренние атаки производятся авторизованными пользователями системы, совершающими непреднамеренные или несанкционированные действия. Внутренние атаки, которые компрометируют безопасность системы, составляют большую часть известных компьютерных преступлений. К методам защиты от внутренних атак относятся:

a) доскональная проверка персонала;

b) тщательное исследование аппаратных средств, программного обеспечения, политики безопасности и конфигураций системы с такой степенью гарантии, которая обеспечила бы их правильную работу (так называемые доверенные функциональные возможности);

c) проведение аудита безопасности, предназначенного для повышения вероятности обнаружения таких атак.

A.2.5.6 Внешние атаки

При реализации внешних атак возможно использование следующих методов:

a) перехват сообщений (активный и пассивный);

b) перехват излучений;

c) маскарад под авторизованных пользователей системы или под ее компоненты;

d) обход механизмов аутентификации или управления доступом.

A.2.5.7 Люк

Когда логический объект системы изменен таким образом, который позволяет нарушителю несанкционированно воздействовать на команду, заранее определенное событие или на последовательность таких событий, то результат этого изменения называется «люк». Например, подтверждение правильности пароля может быть изменено таким образом, чтобы в дополнение к его обычным действиям проверялась и правильность пароля нарушителей.

A.2.5.8 «Троянский конь»

При активизации в системе вредоносной программы типа «троянский конь» система в дополнение к санкционированным функциям приобретает еще и некоторые недекларированные функции. Примером атаки типа «троянский конь» является передача ретранслятором скопированных сообщений по скрытым каналам.

A.2.6 Оценка угроз, рисков и контрмер

Применение средств защиты обычно повышает стоимость системы и может усложнить ее использование. Вследствие этого до начала проектирования безопасной системы необходимо определить конкретные угрозы, от которых необходима защита, т.е. произвести оценку угроз. Система имеет много уязвимых мест, однако используются они не все, т.к. нарушитель обладает ограниченными возможностями или если достигаемый результат не оправдывают его усилий и риска быть обнаруженным. Хотя подробное описание вопросов оценки угроз выходит за пределы данного приложения, в общих чертах оценка угроз включает:

a) идентификацию уязвимостей системы;

b) анализ вероятности реализации угроз путем использования этих уязвимостей;

c) оценку последствий успешной реализации угрозы;

d) оценку стоимости каждой атаки;

e) анализ стоимости возможных мер противодействия;

f) выбор обоснованных механизмов безопасности (возможно путем проведения анализа затрат и получаемых выгод).

Эффективной альтернативой для технических средств защиты могут служить нетехнические средства, например, страхование. Создать совершенную техническую безопасность, также как и совершенную физическую безопасность, невозможно. Следовательно, необходимо сделать так, чтобы стоимость реализации атаки была достаточно высока, это позволит уменьшить степень риска до приемлемого уровня.

A.3 Политика безопасности

В данном разделе рассматривается ряд аспектов политики безопасности, в том числе ее необходимость и назначение, соответствие политики определению и её роль, методы использования, а также корректировка с учётом конкретной ситуации. Эти аспекты затем могут быть применены к системам передачи данных.

A.3.1 Необходимость и назначение политики безопасности

Вся область безопасности сложна и трудно реализуема. Любой всеобъемлющий её анализ даст множество обескураживающих деталей. Приемлемая политика безопасности должна быть сосредоточена на тех аспектах, которые рассматриваются и учитываются на самых верхних уровнях руководства. По существу политика безопасности должна в общих понятиях устанавливать, что разрешено и что недопустимо в процессе реализации основных операций рассматриваемой системы с точки зрения безопасности. Политика обычно описывает безопасность в обобщенных терминах без специфических деталей, исходя из того, что является делом первостепенной важности, не определяя при этом, каким образом должны быть получены желаемые результаты. Политика безопасности устанавливает наивысший уровень требований по безопасности.

A.3.2 Процесс корректировки политики безопасности

Поскольку политика имеет общий характер, то не всегда ясно, как можно конкретно ее применить. Чаще всего наилучший способ достижения этого заключается в том, что политику необходимо подвергнуть последовательному процессу корректировки, добавляя на каждом этапе все больше конкретных деталей. Для уточнения необходимых деталей требуется подробное изучение общей политики в области применения. В результате должны быть определены проблемы относительно применения и состояния политики. Процесс корректировки позволит использовать в новой версии политики очень точные термины, непосредственно связанные с применением. Эта вновь заявленная политика облегчит выполнение определенных деталей реализации.

A.3.3 Компоненты политики безопасности

Имеются два аспекта, относящихся к существующей политике безопасности. Оба они зависят от концепции санкционированного поведения.

A.3.3.1 Авторизация

Все рассмотренные выше виды угроз охватывают понятия санкционированного и несанкционированного поведения. В политике безопасности отражено определение сущности авторизации. Общая политика безопасности может устанавливать: «информация не предоставляется, не может быть доступной, а также не допускается вмешательство, и она не может быть ресурсом, который используют те, кто не имеет соответствующей авторизации».

Характер авторизации как раз и определяет отличие различных политик. Основываясь на соответствующем характере авторизации, все политики могут быть подразделены на два отдельных вида: инструкционная и идентификационная. Первый вид использует правила, основанные на небольшом количестве общих атрибутов или классов чувствительности, которые имеют универсальное применение. Второй охватывает критерий

авторизации, основанный на конкретных индивидуальных атрибутах. Некоторые атрибуты, принадлежащие логическому объекту, присваиваются ему бессрочно, другие атрибуты могут присваиваться логическому объекту временно (например, полномочия) и передаваться другим логическим объектам. Также можно различать административно назначаемые и динамически выбираемые средства авторизации. Политика безопасности должна определять те элементы системной безопасности, которые всегда применимы и остаются в силе (например, компоненты инструкционной и идентификационной политик - при их наличии) и те из них, которые пользователь может использовать по своему усмотрению.

А.3.3.2 Идентификационная политика безопасности

Один из аспектов идентификационной политики безопасности частично соответствует принципу безопасности, известному как «положено знать». Задачей его является фильтрация доступа к данным или ресурсам. В зависимости от того, сохраняется ли информация о правах доступа пользователя или она является частью данных, которые должны быть доступными, имеются два основных фундаментальных способа реализации идентификационной политики. Примером первого служат принципы привилегий или полномочий, предоставляемых пользователям и используемых процессами по их поручению. Примером второго служат списки управления доступом (СУД). В обоих случаях размер области данных (от полного файла до элемента данных), которая может быть поименована в полномочиях или которая имеет свой собственный СУД, может изменяться в широких пределах.

А.3.3.3 Инструкционная политика безопасности

Авторизация в инструкционной политике безопасности обычно основывается на чувствительности. В закрытой системе данным и/или ресурсам должны быть присвоены метки безопасности. Процессам, выполняемым по инициативе персонала, могут быть присвоены метки безопасности, соответствующие этим пользователям.

А.3.4 Политика безопасности, взаимодействие и метки безопасности

Концепция присвоения меток безопасности выполняет важную роль в среде обмена данными. Метки, содержащие атрибуты, выполняют различные функции. Имеются элементы данных, которые перемещаются во время обмена данными; существуют процессы и логические объекты, которые инициируют обмен данными, а также те, 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 безопасности с соответствующими атрибутами. Политика безопасности должна содержать указания, как может использоваться каждый атрибут для обеспечения требуемой безопасности. При установлении конкретных атрибутов меток безопасности может потребоваться согласо-

вание. В том случае, когда метка безопасности присваивается доступным процессам и доступным данным, то соответствующим образом должна быть помечена и дополнительная информация, которая необходима для управления доступом на основе идентификации. Если политика безопасности основана на идентификации пользователя, имеющего доступ к данным непосредственно или с помощью процесса, то метка безопасности должна содержать информацию об идентификации пользователя. Правила присвоения конкретных меток должны быть представлены в политике безопасности ИБУБ и/или согласованы, при необходимости, с оконечными системами. Метка может быть добавлена с помощью атрибутов, которые квалифицируют соответствующую чувствительность для определения и распределения средств обработки, ограничивают время и местоположение, а также четко определяют требования, специфичные для данной оконечной системы.

A.3.4.1 Метки процесса

При аутентификации полная идентификация тех процессов или логических объектов, которые инициируют сеанс обмена данными или отвечают на него при аутентификации, в совокупности со всеми соответствующими атрибутами имеет фундаментальную важность. Вследствие этого ИБУБ должны содержать достаточную информацию о тех атрибутах, которые важны для любой административно установленной политики безопасности.

A.3.4.2 Метки области данных

В процессе сеансов обмена данными каждая область данных при перемещении должна быть тесно связана со своей меткой. (Эта связь является существенной. В некоторых случаях, при применении инструкционной политики безопасности, задается требование, чтобы метка была присвоена специальной части области данных до того, как она будет присвоена приложению). Средства для сохранения целостности области данных должны также поддерживать точность и связность метки. Эти атрибуты могут быть использованы функциями управления маршрутизацией на уровне звена данных базовой эталонной модели ВОС.

A.4 Механизмы безопасности

Политика безопасности может быть реализована с помощью различных механизмов безопасности, используемых как по отдельности, так и в комбинации в зависимости от целей политики безопасности и применяемых механизмов. В общем случае эти механизмы должны принадлежать к одному из трех (перекрывающих друг друга) классов:

a) предотвращение;

b) обнаружение;

c) восстановление.

Ниже рассматриваются механизмы безопасности, соответствующие среде обмена данными.

A.4.1 Криптографические методы и шифрование

Криптография лежит в основе множества услуг и механизмов безопасности. Криптографические функции могут быть использованы в частности для шифрования, дешифрования, обеспечения целостности данных, обмена аутентификацией, хранения и проверки пароля и др., для обеспечения конфиденциальности, целостности и/или аутентификации. При использовании шифрования для обеспечения конфиденциальности, чувствительные данные (т.е. данные, подлежащие защите) преобразуются в менее чувствительные формы. При обеспечении целостности или аутентификации криптографические методы используются, чтобы при вычислении исключить возможность модификации функций.

Первоначально выполняется шифрование открытого текста, в результате чего получают шифротекст. Результатом дешифрования является открытый текст или шифротекст с некоторым закрытием. При выполнении вычислений проще использовать открытый текст для его общей обработки; его семантическое содержимое доступно. Так как семантическое содержимое шифротекста закрыто, то при выполнении вычислений его трудно обработать, если только не использовать специальные методы (например, первичное дешифрование или точное согласование).

Иногда, когда получение исходного открытого текста, например, паролей, нежелательно, шифрование умышленно делают необратимым (например, путем отбрасывания или потери данных).

Криптографические функции используют криптографические переменные и оперируют с полями, блоками данных и/или потоками блоков данных. К двум таким криптографическим переменным относятся ключ, который управляет конкретными преобразованиями, и инициализированная переменная, которая необходима в некоторых криптографических протоколах для сохранения явной произвольности шифротекста. Ключ обычно должен оставаться конфиденциальным, а криптографическая функция и инициализированная переменная могут увеличивать задержку и снижать пропускную способность. Это усложняет внесение в существующие системы «прозрачных» и «встраиваемых» криптографических дополнений.

В зависимости от процедур шифрования или дешифрования криптографические переменные могут быть как симметричными, так и асимметричными. Ключи, используемые в асимметричных алгоритмах, математически связаны между собой; один ключ не может быть вычислен из другого. Эти алгоритмы иногда называют «алгоритмами с открытым ключом», поскольку один ключ является открытым, а другой - секретным.

Шифротекст может быть подвергнут криптоанализу, когда при выполнении вычислений легко восстановить шифротекст без знания ключа. Это может случиться при использовании слабой или имеющей недостатки

криптографической функции. Перехват и анализ трафика могут привести к таким атакам на криптосистему, как вставка, удаление и изменение сообщения/поля, искажение правильного шифротекста и маскарад. Следовательно, криптографические протоколы предназначены для противодействия атакам, а также иногда и для противодействия анализу трафика. Специальные контрмеры, препятствующие анализу трафика, иначе называемые «конфиденциальность потока трафика», помогают скрыть наличие или отсутствие данных и их характеристики. При передаче шифротекста через ретрансляторы и шлюзы адрес сообщения должен находиться в открытом виде. Если данные шифруются только в каждом звене данных, а дешифруются (и таким образом уязвимы) в ретрансляторе или шлюзе, говорят, что используется архитектура «канального шифрования». Если в ретрансляторе или шлюзе в открытом виде находится только адрес (и аналогичные данные управления), то использованная архитектура определяется как «сквозное шифрование». Сквозное шифрование более желательно с точки зрения безопасности, но с точки зрения архитектуры оно значительно более сложно, особенно, если обеспечивается внутриполосное распределение электронных ключей (функция управления ключами). Комбинация сквозного и канального шифрования может использоваться для достижения различных целей безопасности. Целостность данных часто обеспечивается путем подсчета криптографического контрольного значения. Контрольное значение может быть получено за один или несколько шагов и является математической функцией криптографических переменных и данных. Эти контрольные значения связаны с данными, безопасность которых необходимо обеспечить. Криптографические контрольные значения иногда называются кодами обнаружения манипуляции.

Криптографические методы могут обеспечить или помочь обеспечить защиту от:

a) наблюдения потока сообщения и/или его модификации;
b) анализа трафика;
c) непризнания участия;
d) подделки;
e) несанкционированного соединения;
f) модификации сообщений.

A.4.2 Аспекты управления ключами

Управление ключами обеспечивается с помощью криптографических алгоритмов. Управление ключами включает генерацию, распределение и управление. Выбор метода управления ключами основан на экспертной оценке среды, в которой он будет использоваться. К вопросам, касающимся этой среды, относятся угрозы (как внутренние, так и внешние по отношению к организации), от которых необходима защита, используемые технологии, архитектурная структура и расположение предоставляемых криптографиче-

ских услуг, а также физическая структура и размещение провайдеров криптографических услуг.

Управление ключами включает следующее:

a) использование понятия «жизненный цикл», основанного на времени использования или другом критерии, который явно или неявно определен для каждого ключа;

b) соответствующую идентификацию ключей согласно их функции таким образом, чтобы они использовались только для этих функций, например, ключи, предназначенные для услуги конфиденциальности не должны использоваться для услуги целостности и наоборот;

c) вопросы, не относящиеся к функциям ВОС, например, физическое распределение и архивация ключей.

К вопросам управления ключами симметричных алгоритмов относятся:

a) использование услуги конфиденциальности в протоколе управления ключами при их передаче;

b) использование иерархии ключей. Допускаются различные ситуации, например:

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

2) многоуровневые иерархии ключей;

3) мастер-ключи (главные ключи) никогда не следует использовать для безопасности данных и ключи шифрования данных никогда не следует использовать для безопасности мастер-ключей;

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

К вопросам управления ключами асимметричных алгоритмов относятся:

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

b) использование услуги целостности или неотказуемости с подтверждением источника в протоколе управления ключами для передачи открытого ключа. Эти услуги могут быть обеспечены с помощью симметричных и/или асимметричных криптографических алгоритмов.

A.4.3 Механизмы цифровой подписи

Понятие цифровой подписи используется для указания конкретного метода, который может быть применен для обеспечения таких услуг безопасности, как «неотказуемость» и аутентификация. 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 владельца личного ключа;

b) получатель не может создать подписанный блок данных.

Из этого следует, что использование информации общего пользования возможно только для идентификации лица, подписавшего блок данных, в качестве владельца личного ключа. В случае возникновения в дальнейшем конфликта между участниками обмена данными, возможность проверки идентификации лица, подписавшего блок данных, предоставляется надежной третьей стороне, которая привлекается при анализе подлинности подписанного блока данных. Этот тип цифровой подписи называется схемой прямой подписи (рисунок А.1). В других случаях может потребоваться дополнительное свойство (c);

c) отправитель не может отрицать передачу подписанного блока данных.

В этом случае надежная третья сторона (арбитр) обеспечивает получателю регистрацию источника и целостность информации. Этот тип цифровой подписи иногда называют схемой арбитражной подписи (рисунок А.2).

Примечание - Отправитель может потребовать, чтобы получатель не смог позже отказаться от приема подписанного блока данных. Это может быть достигнуто с помощью услуги неотказуемость с подтверждением доставки соответствующей комбинации цифровой подписи, целостности данных и механизмов нотаризации.

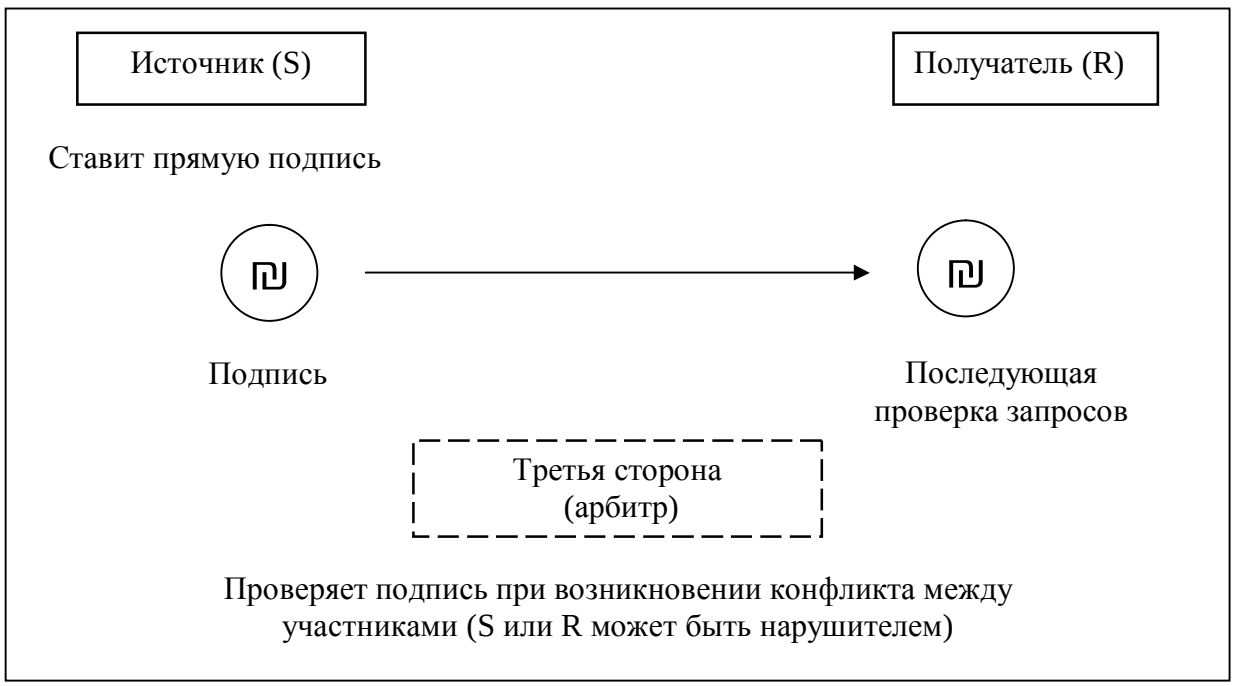

Рисунок А.1 – Схема прямой подписи

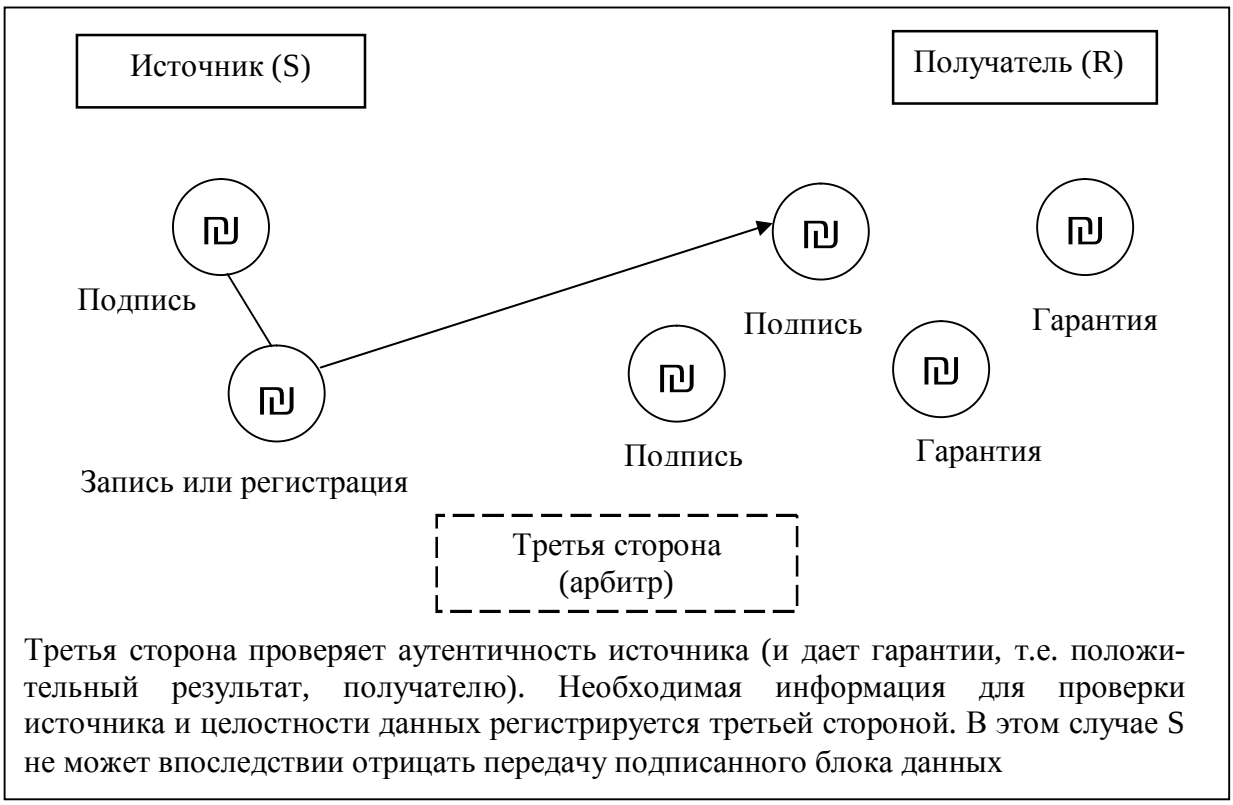

Рисунок А.2 – Схема арбитражной подписи

А.4.4 Механизмы управления доступом

К механизмам управления доступом относятся механизмы, используемые для реализации политики ограниченного доступа к ресурсам только авторизованных пользователей.

К таким механизмам относятся использование списков или таблиц управления доступом (которые обычно содержат идентификаторы конкретных объектов управления и авторизованных пользователей, например, персонала или процессов), паролей, полномочий, меток или токенов, обладание которыми может быть использовано для указания права доступа. При использовании полномочий должна быть исключена возможность подделки и обеспечена достоверная передача.

А.4.5 Механизмы целостности данных

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

A.4.5.1 Обнаружение модификации потока сообщений

Методы обнаружения нарушений целостности, обычно связанные с обнаружением ошибок битов, блоков и последовательностей, вносимые линиями и сетями телекоммуникаций, могут быть также использованы для обнаружения модификации потока сообщений. Однако, если заголовки и окончания протоколов не защищены механизмами целостности, то осведомленный злоумышленник может успешно обойти такой контроль. Таким образом, успешно обнаружить модификацию потока сообщений можно только с помощью средств обнаружения нарушений целостности в сочетании с последующей информацией об этом событии. Все это не сможет предотвратить модификацию потока сообщений, но обеспечит уведомление об атаках.

A.4.6 Механизмы обмена информацией аутентификации

A.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 телекоммуникаций надежны, то идентификация равноправного логического объекта может быть подтверждена паролем. Пароль защищает от ошибки, но не гарантирует защиту от злоумышленных действий (особенно от повторного использования информации). Взаимная аутентификация может быть выполнена путем использования разных паролей для каждого направления;

b) если каждый логический объект доверяет соответствующему равноправному логическому объекту, но не доверяет средствам телекоммуникаций, то защита от активных атак может быть обеспечена с помощью различных комбинаций паролей и шифрования или с помощью криптографических методов. Защита от атак повторного использования информации требует дуплексного квитирования (с параметрами защиты) или установки временных меток (с точными часами). Взаимная аутентификация с защитой от повторного использования информации может быть достигнута с помощью трехстороннего квитирования;

c) если логические объекты не доверяют (или чувствуют, что они не смогут доверять в будущем) соответствующим равноправным логическим объектам или средствам телекоммуникаций, то можно использовать услугу «неотказуемость». Услуга «неотказуемость» может быть реализована с помощью механизмов цифровой подписи и/или нотаризации. Эти механизмы могут использоваться вместе с вышеописанными в b) механизмами.

A.4.7 Механизмы заполнения трафика

С помощью генерации ложного трафика и протокола заполнения блоками данных постоянной длины можно обеспечить ограниченную защиту от анализа трафика. Для успешного выполнения этой задачи уровень

ложного трафика должен приблизительно равняться максимальному 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.

A.4.8 Механизм управления маршрутизацией

Спецификация запретов на использование маршрутов для передачи данных (включая спецификацию всего маршрута) может применяться для передачи данных только по маршрутам, гарантированно обеспечивающим физическую безопасность, а также для обеспечения передачи чувствительной информации только по маршрутам с соответствующим уровнем защиты.

A.4.9 Механизм нотаризации

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

A.4.10 Физическая безопасность и безопасность персонала

При обеспечении комплексной защиты всегда будут необходимы физические средства защиты. Организация физической безопасности требует больших финансовых затрат, и поэтому часто пытаются минимизировать необходимость в ней с помощью других (более дешевых) методов. Вопросы физической безопасности и безопасности персонала не входят в область рассмотрения ВОС, хотя, в конечном счете, все системы должны полагаться на некоторые формы физической безопасности и на надежность персонала, обслуживающего системы. Чтобы гарантировать выполнение надлежащих действий и определить ответственность персонала должны быть разработаны правила технической эксплуатации.

A.4.11 Надежное аппаратное/программное обеспечение

К методам, используемым для получения уверенности в правильном функционировании логического объекта, относятся методы формального доказательства, верификации и проверки корректности, обнаружения и регистрации попыток известных атак, а также построения модели надежного персонала логического объекта в безопасной среде. Необходимо также соблюдать меры предосторожности от преднамеренной или умышленной модификации логического объекта, которая компрометирует безопасность его ресурса, например, в процессе эксплуатации или модернизации. Некоторые логические объекты системы также должны быть надежными, т.е. обеспечивающими правильное функционирование и поддерживающими необходимую безопасность. Методы, использующиеся для повышения доверия, не входят в область рассмотрения ВОС.

Приложение В
(справочное)

Обоснование размещения услуг и механизмов безопасности в разделе 7

В.1 Общие положения

В данном приложении рассмотрены некоторые соображения относительно распределения определенных услуг безопасности по различным уровням, описанным в разделе 7. Управление этим процессом выбора осуществляется по принципу иерархического распределения безопасности, указанному в 6.1.1 настоящего стандарта.

Конкретная услуга безопасности обеспечивается на нескольких уровнях, если ее влияние на общую безопасность процесса передачи информации может считаться различным (например, конфиденциальность соединения на уровнях 1 и 4).

Тем не менее, учитывая существующие функциональные возможности обмена данными ВОС (например, многозвенные процедуры, функции мультиплексирования, различные методы расширения услуг как в режиме без установления соединения, так и в режиме с установлением соединения), а также для обеспечения работоспособности механизмов передачи может возникнуть необходимость обеспечения конкретной услугой на другом уровне, хотя влияние этой услуги на безопасность будет не менее эффективным.

В.2 Аутентификация равноправного логического объекта

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

Уровень 3. Используется в отдельных подсетях и для маршрутизации и/или во внутренней сети.

Уровень 4. Используется для взаимной аутентификации двух или более логических объектов сеансового уровня от одной оконечной системы до другой до установления соединения, а также во время этого соединения.

Уровень 5. Отсутствует, нет никаких преимуществ относительно обеспечения этой услугой на уровне 4 и/или более высоких уровнях.

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

Уровень 7. Используется, аутентификация равноправных логических объектов должна обеспечиваться на прикладном уровне.

B.3 Аутентификация источника данных

Уровни 1 и 2. Отсутствует, так как считается, что аутентификация источника данных на этих уровнях нецелесообразна.

Уровни 3 и 4. Предусмотрена сквозная аутентификация источника данных с целью ретрансляции и маршрутизации на этих уровнях следующим образом:

a) 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 источника данных;

b) даже там, где способ a) не предусмотрен, аутентификация источника данных на основе шифрования может быть предусмотрена с очень небольшими дополнительными затратами в механизмах целостности данных, уже размещенных на этих уровнях.

Уровень 5. Отсутствует, нет преимуществ относительно обеспечения этой услугой на уровне 4 или 7.

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

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

B.4 Управление доступом

Уровни 1 и 2. В системе, соответствующей всем протоколам ВОС, механизмы управления доступом на этих уровнях не могут быть предоставлены, поскольку в существующем оконечном оборудовании такие механизмы отсутствуют.

Уровень 3. Механизмы управления доступом, по требованиям конкретной подсети, могут использоваться с протоколами, выполняющими операции доступа к подсети. При выполнении протоколами операций 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 такая степень детализации доступа довольно груба, она различается только между логическими объектами сетевого уровня.

Установление сетевого соединения часто может производиться на платной основе, что требует от администрации подсети определенных финансовых затрат. Минимизировать эти затраты можно с помощью контроля доступа и с помощью взаиморасчетов с другой сетью или выбора конкретных параметров подсети.

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

Уровень 5. Отсутствует, нет преимуществ относительно обеспечения этой услугой на уровне 4 и/или уровне 7.

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

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

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

Уровень 1. Используется, полная конфиденциальность физического соединения может быть обеспечена после того, как электрический ввод устройств преобразования будет проложен скрытым способом.

Уровень 2. Используется, но не предоставляет никаких дополнительных преимуществ по сравнению с конфиденциальностью на уровне 1 или уровне 3.

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

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

Уровень 5. Отсутствует, поскольку не предоставляет никаких дополнительных преимуществ по сравнению с конфиденциальностью на уровнях 3, 4 и 7. Предоставление этой услуги на данном уровне нецелесообразно.

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

Уровень 7. Используется в сочетании с механизмами нижерасположенных уровней.

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

Соображения аналогичны конфиденциальности всех (N)-данных пользователя за исключением уровня 1, на котором отсутствует эта услуга в режиме без установления соединения.

B.7 Конфиденциальность выбранных полей внутри (N)-данных пользователя некоторого СБД

Эта услуга конфиденциальности обеспечивается с помощью шифрования на уровне представления данных и применения механизмов прикладного уровня в соответствии с семантикой данных.

B.8 Конфиденциальность потока трафика

Конфиденциальность всего потока трафика можно обеспечить только на уровне 1 путем подключения к линии передачи двух устройств шифрования. Предполагается, что режим передачи одновременно должен быть и дуплексным, и синхронным, а включение этих устройств будет способствовать тому, что в физической среде будет невозможно провести анализ трафика (и даже его наличия).

На уровнях выше физического безопасность всего потока трафика невозможна. Конфиденциальность ограниченного потока трафика может быть обеспечена путем использования услуги конфиденциальности всех СБД на одном уровне и введения фиктивного трафика на смежном верхнем уровне. Такой механизм стоит дорого и потенциально предполагает большую пропускную способность каналов и средств коммутации.

Если конфиденциальность потока трафика обеспечивается на уровне 3, то должны использоваться заполнение трафика и/или управление маршрутизацией. Управление маршрутизацией может обеспечить конфиденциальность ограниченного потока трафика путем передачи сообщений маршрутизации по незащищенным звеньям данных или подсетям. Тем не менее, добавление в состав уровня 3 функции заполнения трафика позволяет достичь более эффективного использования сети, например, путем предотвращения излишнего заполнения и перегрузки сети.

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

B.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 на сквозной основе, поэтому здесь данная услуга неприемлема.

Уровень 3. Отсутствует, поскольку восстановление при ошибках не везде доступно.

Уровень 4. Используется, поскольку на транспортном уровне это действительно обеспечивает сквозное соединение.

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

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

Уровень 7. Используется в сочетании с механизмами уровня представления данных.

B.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 на сквозной основе, поэтому здесь данная услуга 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, когда необходимо прекратить обмен данными после обнаружения активной атаки.

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

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

Уровень 7. Используется в сочетании с механизмами уровня представления данных.

B.11 Целостность отдельных полей внутри (N)-данных пользователя (N)-СБД, передаваемого по (N)-соединению (без восстановления)

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

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

Для минимизации дублирования функций, целостность данных, передаваемых в режиме без установления соединения, должна обеспечиваться только на тех уровнях, где и целостность без восстановления, т.е. на сетевом,

транспортном и прикладном уровнях. Такие механизмы целостности имеют очень ограниченную эффективность, и они должны быть реализованы.

B.13 Целостность отдельных полей в отдельном (N)-СБД, передаваемом в режиме без установления соединения

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

B.14 Услуга «неотказуемость»

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

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

Приложение С
(справочное)

Выбор позиций шифрования для приложений

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

1) если необходимо обеспечить конфиденциальность всего потока трафика, то должно быть выбрано шифрование на физическом уровне или обеспечена безопасность передачи (например, используя подходящие методы расширения спектра). Адекватная физическая безопасность и надежная маршрутизация, а также аналогичные функциональные возможности ретрансляторов могут удовлетворить все требования конфиденциальности;

2) если требуется высокая степень детализации безопасности (возможно, отдельный ключ для каждой прикладной ассоциации) и услуги «неотказуемость» или «избирательная защита поля», то должно быть выбрано шифрование на уровне представления данных. Избирательная защита поля может оказаться важной, потому что алгоритмы шифрования потребляют большую вычислительную мощность. Шифрование на уровне представления данных может обеспечить целостность без восстановления, услугу «безотказность» и полную конфиденциальность;

3) если необходимо обеспечить общую безопасность всех обменов данными между оконечными системами и/или внешних устройств шифрования (например, для обеспечения физической безопасности алгоритмов и ключей или безопасности от сбоев программного обеспечения), то 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 после атак, обнаруженных сетевым уровнем;

4) если требуется обеспечить целостность с восстановлением совместно с высокой степенью детализации безопасности, то должно быть выбрано шифрование на транспортном уровне. Это может обеспечить конфиденциальность и целостность с восстановлением или без него;

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

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

Приложение D
(обязательное)

Сведения о соответствии государственного стандарта Узбекистана ссылочному международному стандарту

Таблица D.1

Обозначение и наименование международного стандарта	Степень соответствия	Обозначение и наименование государственного стандарта Узбекистана
ISO/IEC 7498-1:1994 Информационная технология – Взаимосвязь открытых систем – Базовая эталонная модель: Базовая модель (Information technology – Open System Interconnection – Base Reference Model: The Basic Model).	IDT	O‘z DSt ISO/IEC 7498-1:2009 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель
Примечание – В настоящей таблице использовано следующее условное обозначение степени соответствия стандартов: IDT – идентичные стандарты.		

УДК 681.324:006.354 ОКС 35.100

Ключевые слова: архитектура безопасности, взаимосвязь открытых систем, эталонная модель, аутентификация равноправного логического объекта, нотаризация, инструкционная политика безопасности.

Заместитель директора
ГУП «UNICON.UZ» _____ Х. Хасанов

Начальник отдела
Криптографии _____ О. Ахмедова

Ведущий инженер _____ С.И. Абрамова

Нормоконтроль _____ Л. Шаймарданова

СОГЛАСОВАНО

Заместитель
генерального директора
Узбекского агентства связи
и информатизации
М. Сангилов
письмом от 20.12.2010 г.
№ 14-8/4965