МЕЖДУНАРОДНЫЙ СОЮЗ ЭЛЕКТРОСВЯЗИ

МККТТ X.800

МЕЖДУНАРОДНЫЙ
КОНСУЛЬТАТИВНЫЙ КОМИТЕТ
ПО ТЕЛЕГРАФИИ И ТЕЛЕФОНИИ

СЕТИ ПЕРЕДАЧИ ДАННЫХ: ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ (ВОС); БЕЗОПАСНОСТЬ, СТРУКТУРА И ПРИЛОЖЕНИЯ

АРХИТЕКТУРА БЕЗОПАСНОСТИ ДЛЯ ВЗАИМОСВЯЗИ ОТКРЫТЫХ СИСТЕМ ДЛЯ ПРИЛОЖЕНИЙ МККТТ

Рекомендация X.800

Женева, 1991 год

ПРЕДИСЛОВИЕ

МККТТ (Международный консультативный комитет по телеграфии и телефонии) – постоянный орган Международного союза электросвязи (МСЭ). МККТТ отвечает за изучение технических, эксплуатационных и тарифных вопросов и выпуск Рекомендаций по ним с целью стандартизации электросвязи на всемирной основе.

Пленарная ассамблея МККТТ, которая проводится каждые четыре года, определяет темы для исследования и утверждает Рекомендации, подготовленные ее исследовательскими комиссиями. Утверждение Рекомендаций членами МККТТ в период между пленарными ассамблеями осуществляется в соответствии с процедурой, изложенной в Резолюции 2 МККТТ (Мельбурн, 1988 г.).

Рекомендация X.800 подготовлена Исследовательской комиссией VII и утверждена 22 марта 1991 года в соответствии с Резолюцией 2.

_____

ПРИМЕЧАНИЕ МККТТ

В настоящей Рекомендации термин "администрация" используется для краткости и обозначает как администрацию электросвязи, так и признанную эксплуатационную организацию.

Рекомендация X.800

АРХИТЕКТУРА БЕЗОПАСНОСТИ ДЛЯ ВЗАИМОСВЯЗИ ОТКРЫТЫХ СИСТЕМ ДЛЯ ПРИЛОЖЕНИЙ МККТТ[1)]

0 Введение

В Рекомендации X.200 описана эталонная модель взаимосвязи открытых систем (ВОС). Определена основа для координации разработки существующих и будущих Рекомендаций взаимосвязи систем.

Задача ВОС заключается в обеспечении возможности взаимосвязи неоднородных компьютерных систем, с тем чтобы между прикладными процессами можно было установить используемую связь. Для защиты информации, участвующей в обмене между прикладными процессами, в разное время должны устанавливаться средства управления безопасностью. Такие средства управления должны увеличивать затраты в связи с ненадлежащим получением данных или получением измененных данных в такой степени, чтобы они значительно превышали потенциальную стоимость обеспечения этих средств, или же настолько увеличивать время ненадлежащего получения данных, чтобы утрачивалась ценность этих данных.

В настоящей Рекомендации определены общие элементы архитектуры, связанные с безопасностью, которые могут применяться соответствующим образом в условиях, когда требуется безопасность связи между открытыми системами. Рекомендация задает в рамках эталонной модели руководящие принципы и ограничения для совершенствования существующих Рекомендаций или разработки новых Рекомендаций в контексте ВОС, с тем чтобы обеспечить возможность безопасной связи и, таким образом, обеспечить единый подход к безопасности в рамках ВОС.

Для понимания настоящей Рекомендации полезно получить базовую информацию о безопасности. Читателям, не обладающим обширными знаниями в области безопасности, рекомендуется в первую очередь ознакомиться с Приложением A.

Данная Рекомендация расширяет эталонную модель (Рекомендация X.200) для охвата аспектов безопасности, которые в целом являются элементами архитектуры протоколов связи, но не рассматриваются в контексте эталонной модели.

1 Сфера и область применения

В настоящей Рекомендации:

a) представлено общее описание услуг и соответствующих механизмов безопасности, которые может обеспечивать эталонная модель; и

b) определены местоположения в эталонной модели, в которых могут обеспечиваться эти услуги и механизмы.

Настоящая Рекомендация расширяет области применения Рекомендации X.200 для охвата защищенной связи между открытыми системами.

Базовые услуги и механизмы безопасности и их соответствующее местоположение определены для всех уровней эталонной модели. Кроме того, определена архитектурная взаимосвязь услуг и механизмов безопасности и эталонной модели. В оконечных системах, установках и организациях могут потребоваться дополнительные меры безопасности. Эти меры применяются в различном прикладном контексте. Определение услуг безопасности, необходимых для обеспечения таких дополнительных мер безопасности, не входит в сферу применения настоящей Рекомендации.

---

1) Рекомендаия X.800 и стандарт ISO 7498-2 (Системы обработки информации – Взаимосвязь открытых систем – Базовая эталонная модель – Часть 2: Архитектура защиты) технически согласованы.

Функции безопасности ВОС связаны только с теми реальными аспектами тракта связи, которые обеспечивают оконечным системам возможность осуществления безопасной передачи информации между ними. Безопасность ВОС не связана с мерами безопасности, необходимыми в оконечных системах, установках и организациях, за исключением случаев, когда эти меры воздействуют на выбор и размещение услуг безопасности ВОС. Эти аспекты безопасности могут быть стандартизованы, но не в рамках сферы применения Рекомендаций ВОС.

Настоящая Рекомендация дополняет понятия и принципы, определенные в Рекомендации X.200, не изменяя их. Рекомендация не является спецификацией реализации или основой для оценки соответствия реальных реализаций.

2 Справочные документы

Рекомендация X.200 – Эталонная модель взаимосвязи открытых систем для применений МККТТ.

ISO 7498 – Information processing systems – Open systems interconnection – Basic Reference Model (1984).

ISO 7498-4 – Information processing systems – Open systems interconnection – Basic Reference Model – Part 4: Management framework (1989).

ISO 7498/AD1 – Information processing systems – Open systems interconnection – Basic Reference Model – Addendum 1: Connectionless-mode transmission (1987).

ISO 8648 – Information processing systems – Open systems interconnection – Internal organization of the network layer (1988).

3 Определения и аббревиатуры

3.1 В основе настоящей Рекомендации лежат понятия, выработанные в Рекомендации X.200, и для их определения используются следующие термины:

a) (N)-связь;

b) (N)-передача данных;

c) (N)-объект;

d) (N)-средство;

e) (N)-уровень;

f) открытая система;

g) одноранговые объекты;

h) (N)-протокол;

j) (N)-протокольный-блок-данных;

k) (N)-ретрансляция;

l) маршрутизация;

m) формирование последовательности;

n) (N)-услуга;

p) (N)-блок-служебных-данных;

q) (N)-данные-пользователя;

r) подсеть;

s) ресурс ВОС; и

t) синтаксис передачи.

3.2 В настоящей Рекомендации используются следующие термины из соответствующих Рекомендаций/Международных стандартов:

Передача в режиме без установления соединения (ISO 7498/AD1)

Оконечная система (Рек. X.200/ISO 7498)

Функция ретрансляции и маршрутизации (ISO 8648)

База информации управления (MIB) (ISO 7498-4)

Наряду с этим используются следующие аббревиатуры:

OSI	open systems interconnection	BOC	взаимосвязь открытых систем
SDU	service data unit		блок служебных данных
SMIB	security management information base		база информации управления безопасностью
MIB	management information base		база информации управления

3.3 Для целей настоящей Рекомендации применяются следующие определения:

3.3.1 **управление доступом (access control)**

Предотвращение несанкционированного использования ресурса, в том числе предотвращение использование ресурса несанкционированным способом.

3.3.2 **список управления доступом (access control list)**

Список объектов и их прав доступа, имеющих полномочия на получение доступа к ресурсу.

3.3.3 **подотчетность (accountability)**

Свойство, гарантирующее возможность прослеживания действий какого-либо объекта с однозначной привязкой к этому объекту.

3.3.4 **активная угроза (active threat)**

Угроза преднамеренного несанкционированного изменения состояния системы.

Примечание. – Примерами активных угроз безопасности могут служить: изменение сообщений, повторная передача сообщений, включение ложных сообщений, нелегальное проникновение под видом имеющего полномочия объекта и отказ в обслуживании.

3.3.5 **аудит (audit)**

См. Аудит безопасности.

3.3.6 **журнал аудита (audit trail)**

См. Журнал аудита безопасности.

3.3.7 **аутентификация (authentication)**

См. Аутентификация источника данных и Аутентификация однорангового объекта.

Примечание. – В настоящей Рекомендации термин "аутентификация" не используется применительно к целостности данных, вместо этого используется термин "целостность данных".

3.3.8 **информация аутентификации (authentication information)**

Информация, которая используется для установления верности предъявленной идентичности.

3.3.9 **аутентификационный обмен (authentication exchange)**

Механизм, предназначенный для удостоверения идентичности объекта путем обмена информацией.

3.3.10 **авторизация (authorization)**

Предоставление прав, которое включает предоставление доступа на основании прав доступа.

3.3.11 **готовность (availability)**

Свойство быть доступным и годным к использованию по запросу имеющего полномочия объекта.

3.3.12 **возможность (capability)**

Жетон, используемый в качестве идентификатора для ресурса, который означает, что владение им дает права доступа к данному ресурсу.

3.3.13 **канал (channel)**

Тракт передачи информации.

3.3.14 **зашифрованный текст (ciphertext)**

Данные, созданные с применением шифрования. Семантическое содержание результирующих данных недоступно.

Примечание. – Зашифрованный текст может пройти процедуру шифрования, в результате чего будут созданы супершифрованные данные.

3.3.15 **незашифрованный текст (cleartext)**

Открытые данные, семантический контент которых доступен.

3.3.16 **конфиденциальность (confidentiality)**

Свойство, защищающее информацию от доступа к ней или ее раскрытия неуполномоченными лицами, устройствами или процессами.

3.3.17 **регистрационные данные (credentials)**

Данные, которые передаются для установления предъявленной идентичности объекта.

3.3.18 **криптоанализ (cryptanalysis)**

Анализ криптографической системы и/или ее входных и выходных данных для извлечения секретных переменных и/или уязвимых данных, включая открытый текст.

3.3.19 **криптографическое контрольное значение (cryptographic checkvalue)**

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 (cryptography)**

Дисциплина, включающая принципы, средства и методы для преобразования данных, необходимого для того, чтобы скрыть содержащуюся в них информацию, предотвратить их скрытое изменение и/или предотвратить несанкционированное использование.

Примечание. – Криптография определяет методы, используемые при шифровании и дешифровании. Атака на криптографический принцип, средство или метод называется криптоанализом.

3.3.21 **целостность данных (data integrity)**

Показатель того, что данные не были изменены или разрушены несанкционированным способом.

3.3.22 **аутентификация источника данных (data origin authentication)**

Подтверждение того, что источник полученных данных соответствует объявленному.

3.3.23 **дешифрование (decipherment)**

Инверсия соответствующего обратимого шифрования.

3.3.24 **декодирование (decryption)**

См. Дешифрование.

3.3.25 **отказ в обслуживании (denial of service)**

Недопущение санкционированного доступа к ресурсам или задержка выполнения операций, критических во времени.

3.3.26 **цифровая подпись (digital signature)**

Данные, добавленные к блоку данных, или криптографическое преобразование (см. Криптография) блока данных, которые позволяют получателю блока данных удостоверить источник и целостность блока данных и обеспечить защиту от мошенничества, например получателем.

3.3.27 **шифрование (encipherment)**

Криптографическое преобразование данных (см. Криптография) для создания зашифрованного текста.

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

3.3.28 **кодирование (encryption)**

См. Шифрование.

3.3.29 **сквозное шифрование (end-to-end encipherment)**

Шифрование данных в пределах системы или на стороне источника с соответствующим дешифрованием, которое осуществляется только в пределах системы или на стороне назначения. (См. также Шифрование по участкам.)

3.3.30 **стратегия безопасности на основе идентичности (identity-based security policy)**

Стратегия безопасности, в основу которой положены идентичность и/или атрибуты пользователей, группы пользователей или объектов, действующих от имени пользователей, а также ресурсов/объектов, к которым осуществляется доступ.

3.3.31 **целостность (integrity)**

См. Целостность данных.

3.3.32 **ключ (key)**

Последовательность символов, которая управляет операциями шифрования и дешифрования.

3.3.33 **управление ключами (key management)**

Генерирование, хранение, распределение, удаление, архивирование и применение ключей в соответствии со стратегией безопасности.

3.3.34 **шифрование по участкам (link-by-link encipherment)**

Индивидуальное применение шифрования к данным на каждом участке системы связи. (См. также Сквозное шифрование.)

Примечание. – В результате шифрования по участкам данные на объектах ретрансляции будут находиться в формате открытого текста.

3.3.35 **обнаружение манипулирования данными (manipulation detection)**

Механизм, используемый для определения факта изменения данных (непредумышленно или намеренно).

3.3.36 **нелегальное проникновение (masquerade)**

Предпринимаемая объектом попытка представить себя другим объектом.

3.3.37 **заверение (notarization)**

Регистрация данных с участием доверенной третьей стороны, которая позволяет впоследствии гарантировать точность характеристик этих данных, таких как контент, источник, время и доставка.

3.3.38 **пассивная угроза (passive threat)**

Угроза несанкционированного раскрытия информации без изменения состояния системы.

3.3.39 **пароль (password)**

Конфиденциальная информация аутентификации, состоящая, как правило, из строки символов.

3.3.40 **аутентификация однорангового объекта (peer-entity authentication)**

Подтверждение того, что одноранговый объект в ассоциации является объявленным объектом.

3.3.41 **физическая безопасность (physical security)**

Меры, предпринимаемые для обеспечения физической защиты ресурсов от умышленных и непреднамеренных угроз.

3.3.42 **стратегия (policy)**

См. Стратегия безопасности.

3.3.43 **неприкосновенность частной жизни (privacy)**

Право частного лица контролировать или воздействовать на то, какая касающаяся его информация может быть собрана и сохранена, а также кем и кому эта информация может быть открыта.

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 требуемой безопасности.

3.3.44 **непризнание участия (repudiation)**

Отказ признания одним из участвующих в сеансе связи объектов участия во всем или в части сеанса связи.

3.3.45 **управление маршрутизацией (routing control)**

Применение правил в процессе маршрутизации для выбора или обхода конкретных сетей, каналов и ретрансляторов.

3.3.46 **стратегия безопасности на основе правил (rule-based security policy)**

Стратегия безопасности на основе глобальных правил, которые распространяются на всех пользователей. Эти правила обычно связаны со сравнением критичности ресурсов, к которым осуществляется доступ, и владением соответствующими атрибутами пользователей, группы пользователей или объектов, действующих от имени пользователей.

3.3.47 **аудит безопасности (security audit)**

Независимый анализ или ревизия системных записей и действий для проверки на адекватность управляющих функций системы, для обеспечения соответствия установленным стратегическим и эксплуатационным процедурам, для выявления нарушения безопасности и для предложения каких-либо изменений в управлении, стратегии или процедурах.

3.3.48 **журнал аудита безопасности (security audit trail)**

Данные, которые собраны и могут быть использованы для содействия проведению аудита безопасности.

3.3.49 **метка безопасности (security label)**

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

Примечание. – Маркировка и/или связывание может быть явным или неявным.

3.3.50 **стратегия безопасности (security policy)**

Набор критериев для предоставления услуг безопасности (см. также Стратегия безопасности на основе идентичности и на основе правил).

Примечание. – Полная стратегия безопасности неизбежно затрагивает многие вопросы, выходящие за рамки ВОС.

3.3.51 **услуга безопасности (security service)**

Услуга, предоставляемая каким-либо уровнем открытых систем связи, которая гарантирует достаточную защиту систем или процессов передачи данных.

3.3.52 **селективная защита полей (selective field protection)**

Защита конкретных полей в каком-либо сообщении, подлежащем передаче.

3.3.53 **критичность (sensitivity)**

Характеристика ресурса, которая заключает в себе его значение или важность и может также включать его уязвимость.

3.3.54 **подпись (signature)**

См. Цифровая подпись.

3.3.55 **угроза (threat)**

Потенциальное нарушение безопасности.

3.3.56 **анализ трафика (traffic analysis)**

Анализ информации на основе наблюдения за потоками трафика (наличие, отсутствие, объем, направление и частота).

3.3.57 **конфиденциальность потоков трафика (traffic flow confidentiality)**

Услуга обеспечения конфиденциальности для защиты от анализа трафика.

3.3.58 **подстановка трафика (traffic padding)**

Генерирование фальшивых экземпляров связи, фальшивых блоков данных и/или фальшивых данных в пределах блоков данных.

3.3.59 **доверенная функциональность (trusted functionality)**

Функциональность, воспринимаемая как корректная по определенным критериям, например как установленная стратегией безопасности.

4 Обозначение

Используется обозначение уровней, аналогичное принятому в Рекомендации X.200.

Термин "услуга" используется, если не указано иное, для обозначения услуги безопасности.

5 Общее описание услуг и механизмов безопасности

5.1 *Обзор*

В настоящем разделе рассматриваются услуги безопасности, включенные в архитектуру безопасности ВОС, и механизмы, которые реализуют эти услуги. Представленные ниже услуги безопасности являются базовыми услугами безопасности. На практике они будут задействованы на соответствующих уровнях и в соответствующих сочетаниях, как правило с не относящимися к ВОС услугами и механизмами, для обеспечения соответствия стратегии безопасности и/или требованиям пользователя. Для реализации сочетаний базовых услуг безопасности могут использоваться конкретные механизмы безопасности. В используемых на практике вариантах системы могут быть реализованы конкретные сочетания базовых услуг безопасности, которые вызываются напрямую.

5.2 *Услуги безопасности*

Нижеследующие услуги рассматриваются как услуги безопасности, которые могут быть факультативно обеспечены в рамках эталонной модели ВОС. Услуги аутентификации требуют информацию аутентификации, содержащую локально хранимую информацию и данные, которые передаются (регистрационные данные) для содействия аутентификации.

5.2.1 *Аутентификация*

Эти услуги обеспечивают аутентификацию осуществляющего связь однорангового объекта и источника данных, как описано ниже.

5.2.1.1 *Аутентификация однорангового объекта*

Эта услуга, если предоставляется (N)-уровнем, обеспечивает (N + 1)-объекту подтверждение того, что одноранговым объектом является объявленный (N + 1)-объект.

Эта услуга предоставляется для использования при установлении или в течение этапа передачи данных соединения для подтверждения идентичности одного или нескольких объектов, подсоединенных к одному или нескольким другим объектам. Услуга обеспечивает уверенность, но только в период использования, в том, что объект не предпринимает попыток нелегального проникновения или несанкционированного повторения предшествовавшего соединения. Возможны схемы односторонней и взаимной аутентификации одноранговых объектов – с проверкой и без проверки жизнеспособности, которые обеспечивают разную степень защиты.

5.2.1.2 *Аутентификация источника данных*

Эта услуга, если предоставляется (N)-уровнем, обеспечивает (N + 1)-объекту подтверждение того, что источником данных является объявленный (N + 1)-объект.

Услуга аутентификации источника данных обеспечивает подтверждение источника блока данных. Услуга не обеспечивает защиты от дублирования или изменения блоков данных.

5.2.2 *Управление доступом*

Эта услуга обеспечивает защиту от несанкционированного использования ресурсов, доступных через ВОС. Это могут быть ресурсы, относящиеся или не относящиеся к ВОС, доступные по протоколам ВОС. Данная услуга защиты может применяться к разным типам доступа к ресурсу (например, использование ресурса связи; чтение, запись или удаление информационного ресурса; выполнение функций ресурса обработки) или ко всем видам доступа к ресурсу.

Управление доступом будет осуществляться в соответствии с разными стратегиями безопасности (см. п. 6.2.1.1).

5.2.3 *Конфиденциальность данных*

Эти услуги обеспечивают защиту данных от несанкционированного раскрытия, как описано ниже.

5.2.3.1 Конфиденциальность в режиме установления соединения

Эта услуга обеспечивает конфиденциальность всех (N)-данных-пользователя в (N)-соединении.

Примечание. – В зависимости от использования и уровня защита всех данных может не требоваться, например сервисные данные или данные запроса соединения.

5.2.3.2 *Конфиденциальность в режиме без установления соединения*

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

5.2.3.3 *Селективная конфиденциальность полей*

Эта услуга обеспечивает конфиденциальность отдельных полей в пределах (N)-данных-пользователя в (N)-соединении или в одном (N)-SDU в режиме без установления соединения.

5.2.3.4 *Конфиденциальность потока трафика*

Эта услуга обеспечивает защиту информации, которая может быть извлечена из наблюдаемых потоков трафика.

5.2.4 *Целостность данных*

Эти услуги подсчитывают активные угрозы и могут выполняться в одной из описанных ниже форм.

Примечание. – Использование в соединении услуги аутентификации однорангового объекта в начале соединения и услуги целостности данных в течение срока существования этого соединения может – в сочетании – обеспечить подтверждение источника всех переданных по этому соединению блоков данных, целостность этих блоков данных и может также обеспечить обнаружение дублирования блоков данных, например путем использования порядковых номеров.

5.2.4.1 *Целостность в режиме установления соединения с восстановлением*

Эта услуга обеспечивает целостность всех (N)-данных пользователя в (N)-соединении и выявляет любое изменение, включение, удаление или повторную передачу любых данных в пределах всей последовательности SDU (предпринимается попытка восстановления).

5.2.4.2 *Целостность в режиме установления соединения без восстановления*

То же, что и в п. 5.2.4.1, но попытка восстановления не предпринимается.

5.2.4.3 *Селективная целостность полей в режиме установления соединения*

Эта услуга обеспечивает целостность отдельных полей в (N)-данных-пользователя блока (N)-SDU, передаваемого по соединению, и принимает форму определения факта внесения изменений, включения, удаления или повторной передачи отдельных полей.

5.2.4.4 *Целостность в режиме без установления соединения*

Эта услуга, если предоставляется (N)-уровнем, обеспечивает гарантию целостности для запрашивающего (N + 1)-объекта.

Эта услуга обеспечивает целостность одного SDU в режиме без установления соединения и принимает форму определения факта внесения изменений в принятый SDU. Наряду с этим может обеспечиваться ограниченная форма определения повторной передачи.

5.2.4.5 *Селективная целостность полей в режиме без установления соединения*

Эта услуга обеспечивает целостность отдельных полей в одном SDU в режиме без установления соединения и принимает форму определения факта внесения изменений в отдельные поля.

5.2.5 *Предотвращение отказа от авторства*

Эта услуга может принимать одну из двух форм или обе формы.

5.2.5.1 *Предотвращение отказа от авторства с подтверждением источника*

Получателю данных предоставляется подтверждение источника данных. Это защищает от любых попыток отправителя ложно отрицать отправление данных или их содержимое.

5.2.5.2 *Предотвращение отказа от авторства с подтверждением доставки*

Отправителю данных предоставляется подтверждение доставки данных. Это защищает от любых последующих попыток получателя ложно отрицать получение данных или их содержимого.

5.3 *Конкретные механизмы безопасности*

Представленные ниже механизмы могут включаться в соответствующий (N)-уровень с целью реализации ряда услуг, описанных в п. 5.2.

5.3.1 *Шифрование*

5.3.1.1 Шифрование может обеспечить конфиденциальность как данных, так и информации потока трафика, и может быть частью или дополнением ряда других механизмов безопасности, описанных в последующих разделах.

5.3.1.2 Алгоритмы шифрования могут быть алгоритмами обратимого или необратимого шифрования. Существуют две основные группы алгоритма обратимого шифрования:

a) симметричное (то есть с секретным ключом) шифрование, при котором знание ключа шифрования подразумевает знание ключа дешифрования и наоборот; и

b) асимметричное (то есть с открытым ключом) шифрование, при котором знание ключа шифрования не подразумевает знания ключа дешифрования и наоборот. Два ключа такой системы иногда называются "открытый ключ" и "личный ключ".

В алгоритмах необратимого шифрования может использоваться или не использоваться какой-либо ключ. Если ключ используется, этот ключ может быть открытым или секретным.

5.3.1.3 Существование механизма шифрования означает использование механизма управления ключом, кроме некоторых алгоритмов необратимого шифрования. В п. 8.4 приведен ряд руководящих указаний в отношении управления ключом.

5.3.2 *Механизмы цифровой подписи*

Эти механизмы определяют две процедуры:

a) подписание блока данных; и

b) проверка подписанного блока данных.

Первый процесс использует информацию, которая является личной (то есть уникальной и конфиденциальной) для подписывающего лица. Второй процесс использует процедуры и информацию, которые находятся в открытом доступе, но из которых невозможно вывести личную информацию подписывающего лица.

5.3.2.1 Процесс подписания включает либо шифрование блока данных или создание криптографического контрольного значения этого блока данных с использованием личной информации подписывающего лица в качестве личного ключа.

5.3.2.2 Процесс проверки включает использование открытых процедур и информации для определения факта создания подписи с использованием личной информации подписывающего лица.

5.3.2.3 Важной характеристикой механизма подписи является то, что подпись может быть создана только с использованием личной информации подписывающего лица. Следовательно, после выполнения проверки подписи далее в любой момент третьей стороне (например, судье или судье арбитражного суда) может быть предоставлено доказательство того, что данная подпись могла быть создана только единственным держателем личной информации.

5.3.3 *Механизмы управления доступом*

5.3.3.1 В этих механизмах может использоваться аутентифицированная идентичность объекта либо информация об этом объекте (например, член известной совокупности объектов) или возможностях этого объекта, с тем чтобы определить и осуществить права доступа данного объекта. Если объект пытается использовать неразрешенный ресурс или разрешенный ресурс с ненадлежащим типом доступа, то функция управления доступом отклонит эту попытку и, кроме того, может сообщить о происшествии с целью выработки аварийного сигнала и/или записи этого происшествия как части журнала аудита безопасности. Какое-либо уведомление отправителю об отказе в доступе в случае передачи данных в режиме без установления соединения может предоставляться только как результат функций управления доступом, заданных в источнике.

5.3.3.2 Механизмы управления доступом могут, например, основываться на использовании одного или нескольких следующих элементов.

a) Информационные базы управления доступом, в которых хранятся права доступа одноранговых объектов. Эта информация может поддерживаться центрами авторизации или объектом, к которому осуществляется доступ, и может иметь форму списка управления доступом или матрицы иерархической или распределенной структуры. Это предполагает, что была гарантирована аутентификация однорангового объекта.

b) Аутентификационная информация, например пароли, владение которой и последующее представление которой является доказательством авторизации осуществляющего доступ объекта.

c) Возможности, владение которыми и последующее представление которых является доказательством права доступа к объекту или ресурсу, определенному этими возможностями.

   Примечание. – Возможность должна быть непринудительной и передаваться безопасным способом.

d) Метки безопасности, которые, если связаны с объектом, могут быть использованы для предоставления доступа или отказа в доступе, обычно в соответствии со стратегией безопасности.

e) Время попытки доступа;

f) Маршрут попытки доступа, и

g) Продолжительность доступа.

5.3.3.3 Механизмы управления доступом могут применяться на любой стороне ассоциации связи и/или в любой промежуточной точке.

Функции управления доступом, участвующие в источнике или в любой промежуточной точке, используются для того, чтобы определить, разрешено ли отправителю осуществлять связь с получателем и/или использовать требуемые ресурсы связи.

Требования к механизмам управления доступом на уровне однорангового объекта на стороне получателя сеанса передачи данных в режиме без установления соединения должны быть известны в источнике априори и должны быть записаны в базе информации управления безопасностью (см. пп. 6.2 и 8.1).

5.3.4 *Механизмы обеспечения целостности данных*

5.3.4.1 Рассматриваются два аспекта целостности данных: целостность отдельного блока или поля данных и целостность потока блоков или полей данных. Для обеспечения этих двух типов услуги целостности обычно используются разные механизмы, хотя реализация второго типа без реализации первого типа нецелесообразна.

5.3.4.2 Определение целостности отдельного блока данных включает два процесса: один на передающем объекте и один на принимающем. Передающий объект добавляет к блоку данных величину, которая является функцией самих данных. Эта величина может нести дополнительную информацию, такую как проверочный код блока или криптографическое контрольное значение, и сама может быть зашифрована. Принимающий объект генерирует соответствующую величину и сравнивает ее с принятой величиной, для того чтобы определить, не были ли данные изменены при передаче. Этот механизм в отдельности не защитит от повторной передачи отдельного блока данных. На соответствующих уровнях архитектуры обнаружение манипулирования данными может привести к восстановительным действиям (например, путем повторной передачи или исправления ошибок) на данном или более высоком уровне.

5.3.4.3 В случае передачи данных в режиме с установлением соединения защита целостности последовательности блоков данных (то есть защита от нарушения порядка следования, потери, повторной передачи и включения и изменения данных) требует добавления некоторой формы явного упорядочивания, такой как нумерация последовательности, метки времени или криптографическое связывание.

5.3.4.4 В случае передачи данных в режиме без установления соединения для обеспечения ограниченной формы защиты от повторной передачи отдельных блоков данных могут использоваться метки времени.

5.3.5 *Механизм аутентификационного обмена*

5.3.5.1 В рамках аутентификационного обмена могут применяться следующие методы:

a) использование аутентификационной информации, такой как пароли, поставляемые передающим объектом и проверяемые принимающим объектом;

b) криптографические методы; и

c) использование характеристик объекта и/или владения объектом.

5.3.5.2 Эти механизмы могут быть включены в (N)-уровень для обеспечения аутентификации однорангового объекта. Если механизм не выполняет успешной аутентификации объекта, то это вызывает отклонение или завершение соединения, а также может вызвать запись в журнале аудита безопасности и/или представление отчета в центр управления безопасностью.

5.3.5.3 Если используются криптографические методы, они могут быть объединены с протоколами установления связи для защиты от повторной передачи (то есть для гарантирования жизнеспособности).

5.3.5.4 Выбор методов аутентификационного обмена зависит от условий, в которых необходимо их использование совместно с:

a) метками времени и синхронизированными часами;

b) двух- и трехступенчатым установлением связи (для односторонней и взаимной аутентификации соответственно); и

c) услугами предотвращения отказа от авторства на основе использования цифровой подписи и/или механизмов заверения.

5.3.6 *Механизм подстановки трафика*

Механизмы подстановки трафика могут использоваться для обеспечения разных уровней защиты от анализа трафика. Этот механизм может быть эффективен, только если подстановка трафика защищена услугой конфиденциальности.

5.3.7 *Механизм управления маршрутизацией*

5.3.7.1 Маршруты могут выбираться динамически или на основе предварительных договоренностей, так чтобы использовать только физически защищенные подсети, ретрансляторы или линии.

5.3.7.2 Оконечные системы могут, если определен факт постоянно предпринимаемых атак с целью манипуляции данными, дать поставщику услуг сети команду установить соединение через другой маршрут.

5.3.7.3 Для несущих определенные метки безопасности данных может быть запрещен проход через определенные подсети, ретрансляторы или линии. Кроме того, инициатор соединения (или отправитель блока данных в режиме без установления соединения) может определить конкретные предостережения в отношении маршрутизации, требующие избегать конкретные подсети, ретрансляторы и линии.

5.3.8 *Механизм заверения*

5.3.8.1 Свойства данных, передаваемых между двумя и более объектами, такие как целостность, источник, время и пункт назначения, могут гарантироваться путем обеспечения механизмов заверения. Гарантия предоставляется нотариусом третьей стороны, которому доверяют осуществляющие связь объекты и который располагает необходимой информацией для обеспечения требуемой гарантии, каковая может быть засвидетельствована. Каждый экземпляр связи может использовать цифровую подпись, шифрование и механизмы целостности, соответствующие услуге, предоставляемой нотариусом. Если используется механизм заверения, данные, передаваемые между осуществляющими связь объектами, передаются через защищенные экземпляры связи и нотариуса.

5.4 *Универсальные механизмы безопасности*

В данном подпункте описан ряд механизмов, которые не относятся к какой-либо конкретной услуге. Так, в разделе 7 они явно не описаны, поскольку находятся в любом конкретном уровне. Некоторые из этих универсальных механизмов безопасности могут рассматриваться как аспекты управления безопасностью (см. также раздел 8). Значение этих механизмов в целом определяется требуемым уровнем безопасности.

5.4.1 *Доверенная функциональность*

5.4.1.1 Доверенная функциональность может использоваться для расширения сферы охвата или определения эффективности других механизмов безопасности. Любая функциональность, которая обеспечивает напрямую механизмы безопасности или доступ к механизмам безопасности, должна быть надежной.

5.4.1.2 Процедуры, используемые для обеспечения возможности установления доверия к такому аппаратному и программному обеспечению, не входят в сферу применения настоящей Рекомендации и в ряде случаев меняются в зависимости от уровня воспринимаемых угроз и ценности подлежащей защите информации.

5.4.1.3 Эти процедуры, как правило, сопровождаются высокими затратами и сложны в реализации. Проблемы возможно сократить путем выбора архитектуры, позволяющей реализацию функций безопасности по модулям, которые могут быть отделены и обеспечиваться от не связанных с безопасностью функций.

5.4.1.4 Любая защита ассоциаций выше уровня, на котором применяется защита, должна обеспечиваться другими средствами, например соответствующей доверенной функциональностью.

5.4.2 *Метки безопасности*

5.4.2.1 Ресурсы, в том числе элементы данных, могут иметь связанные с ними метки безопасности, например для индикации уровня критичности. Часто необходимо перенести соответствующую метку безопасности вместе с передаваемыми данными. Метка безопасности может быть дополнительными данными, связанными с передаваемыми данными, или может быть неявной, например подразумеваемой в силу использования конкретного ключа для шифрования данных или в силу контекста данных, например источник или маршрут. Неявные метки безопасности должны быть однозначно идентифицируемыми, с тем чтобы было возможно провести их соответствующую проверку. Кроме того, они должны быть безопасным образом привязаны к данным, с которыми они связаны.

5.4.3 *Обнаружение событий*

5.4.3.1 Связанное с безопасностью обнаружение событий включает обнаружение очевидного нарушения безопасности и может также включать обнаружение "нормальных" событий, таких как успешный доступ (или регистрация). Связанные с безопасностью события могут обнаруживаться объектами в пределах ВОС, включая механизмы безопасности. Спецификация элементов события ведется в рамках управления обработкой событий (см. п. 8.3.1). Обнаружение различных связанных с безопасностью событий может, например, вызывать одно или несколько следующих действий:

a) сообщение о событии на локальном уровне;

b) дистанционное сообщение о событии;

c) регистрация события (см. п. 5.4.3); и

d) восстановительное действие (см. п. 5.4.4)

Примерами таких связанных с безопасностью событий могут служить:

a) конкретное нарушение безопасности;

b) конкретное выбранное событие; и

c) переполнение счетчика числа случаев.

5.4.3.2 Стандартизация в этой области будет учитывать передачу соответствующей информации для сообщения о событии и регистрации события, а также синтаксическое и семантическое определение, которое должно использоваться для передачи в рамках сообщения о событии и регистрации события.

5.4.4 *Журнал аудита безопасности*

5.4.4.1 Журналы аудита безопасности обеспечивают ценный механизм безопасности, поскольку потенциально они позволяют обнаруживать и расследовать случаи нарушения безопасности, допуская последующий аудит безопасности. Аудит безопасности – это независимый обзор и исследование системных записей и действий, проводимый для проверки адекватности средств управления системой, обеспечения соответствия установленным стратегиям и эксплуатационным процедурам, содействия в оценке ущерба и для выдачи рекомендаций по любым указанным изменениям в управлении, стратегиях и процедурах. Аудит безопасности требует занесения относящейся к безопасности информации в журнал аудита безопасности и анализа и сообщения информации из журнала аудита безопасности. Занесение в журнал или регистрация рассматривается как механизм безопасности и описан в данном разделе. Анализ и сообщение рассматривается как функция управления безопасностью (см. п. 8.3.2).

5.4.4.2 Собираемая в журнале аудита безопасности информация может быть адаптирована к различным требованиям путем определения типа(ов) относящихся к безопасности событий, которые подлежат регистрации (например, очевидные нарушения безопасности или успешное выполнение операций).

Информированность о существовании журнала аудита безопасности может служить сдерживающим фактором для потенциальных источников нацеленных на безопасность атак.

5.4.4.3 В отношении журнала аудита безопасности ВОС будет приниматься во внимание то, какая информация будет факультативно заноситься в журнал, при каких условиях эта информация будет заноситься в журнал, а также синтаксическое и семантическое определение, которое должно использоваться в обмене информацией журнала аудита безопасности.

5.4.5 *Восстановление безопасного состояния*

5.4.5.1 Восстановление безопасного состояния связано с запросами от таких механизмов, как функции обработки событий и управления обработкой, и заключается в выполнении восстановительных действий как результат применения набора правил. Такие восстановительные действия могут быть трех видов:

a) немедленные;

b) временные; и

c) долгосрочные.

Например:

Немедленные действия могут вызвать немедленное прерывание операций, например разъединение.

Временные действия могут вызывать временную недействительность объекта.

Долгосрочные действия могут заключаться во введении объекта в черный список или изменении ключа.

5.4.5.2 К объектам стандартизации относятся протоколы для восстановительных действий и для управления восстановлением безопасного состояния (см. п. 8.3.3).

5.5 *Иллюстрация взаимосвязи услуг и механизмов безопасности*

Таблица 1/X.800 служит иллюстрацией того, какие механизмы, самостоятельно или в сочетании с другими механизмами, рассматриваются как целесообразные для обеспечения каждой услуги. Таблица представляет обзор этих взаимосвязей и не является исчерпывающей. Услуги и механизмы, указанные в таблице, описаны в пп. 5.2 и 5.3. Взаимосвязи более подробно описаны в разделе 6.

ТАБЛИЦА 1/X.800

Иллюстрация взаимосвязи услуг и механизмов безопасности

Механизм / Услуга	Шифрование	Цифровая подпись	Управление доступом	Целостность данных	Аутентифика-ционный обмен	Подстановка трафика	Управление маршрути-зацией	Заверение
Аутентификация одноранговогo объекта	Д	Д	·	·	Д	·	·	·
Аутентификация источника данных	Д	Д	·	·	·	·	·	·
Услуга управления доступом	·	·	Д	·	·	·	·	·
Конфиденциальность в режиме установления соединения	Д	·	·	·	·	·	Д	·
Конфиденциальность в режиме без установления соединения	Д	·	·	·	·	·	Д	·
Селективная конфиденциальность полей	Д	·	·	·	·	·	·	·
Конфиденциальность потока трафика	Д	·	·	·	·	Д	Д	·
Целостность в режиме установления соединения с восстановлением	Д	·	·	Д	·	·	·	·
Целостность в режиме установления соединения без восстановления	Д	·	·	Д	·	·	·	·
Селективная целостность полей в режиме установления соединения	Д	·	·	Д	·	·	·	·
Целостность в режиме без установления соединения	Д	Д	·	Д	·	·	·	·
Селективная целостность полей в режиме без установления соединения	Д	Д	·	Д	·	·	·	·
Предотвращение отказа от авторства. Источник	·	Д	·	Д	·	·	·	Д
Предотвращение отказа от авторства. Доставка	·	Д	·	Д	·	·	·	Д

· Использование механизма представляется нецелесообразным.

Д Да: использование механизма представляется целесообразным либо самостоятельно, либо в сочетании с другими механизмами.

Примечание. – В ряде случаев механизмы обеспечивают результат, превосходящий необходимый для соответствующей услуги, но тем не менее могут использоваться.

6 Взаимосвязь услуг, механизмов и уровней

6.1 *Принципы разделения безопасности по уровням*

6.1.1 При организации распределения услуг безопасности по уровням и последующем размещении на этих уровнях механизмов безопасности использовались изложенные ниже принципы:

a) число альтернативных способов выполнения услуги следует сводить к минимуму;

b) допустимо строить защищенную систему, обеспечивая услуги безопасности на нескольких уровнях;

c) дополнительная функциональность, требуемая для обеспечения безопасности, не должна без необходимости дублировать существующие функции ВОС;

d) следует не допускать нарушения независимости уровней;

e) объем доверенной функциональности следует сводить к минимуму;

f) если объект зависит от механизма безопасности, обеспечиваемого объектом нижнего уровня, любые промежуточные уровни следует создавать таким образом, чтобы нарушение безопасности было невозможным;

g) по возможности дополнительные функции безопасности уровня следует определять таким образом, чтобы не препятствовать реализации в виде автономного(ых) модуля(ей); и

h) настоящая Рекомендация предполагается применимой к открытым системам, в состав которых входят оконечные системы, содержащие все семь уровней, и системам ретрансляции.

6.1.2 Определение услуг на каждом уровне может потребовать изменений в целях обеспечения запросов на услуги безопасности, независимо от того, предоставляются эти услуги на том же или более низком уровне.

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

Данный подраздел следует читать вместе с разделом 8, в котором рассматриваются вопросы управления безопасностью. Предусматривается, что услуги и механизмы безопасности могли активироваться объектом управления через интерфейс управления и/или путем вызова услуги.

6.2.1 *Определение функций защиты для экземпляра связи*

6.2.1.1 *Общее*

В данном подразделе описан процесс активизации защиты для экземпляров связи в режиме с установлением и без установления соединения. В случае связи с установлением соединения услуги защиты, как правило, запрашиваются/предоставляются в момент установления соединения. В случае активизации услуги в режиме без установления соединения защита запрашивается/предоставляется для каждого экземпляра запроса услуги в режиме без установления соединения.

Для упрощения последующего описания термин "запрос услуги" будет использоваться для обозначения установления соединения или вызова услуги в режиме без установления соединения. Активизация защиты для выбранных данных может обеспечиваться с помощью селективной защиты полей. Например, это может быть выполнено путем установления нескольких соединений, каждое из которых имеет разный тип или уровень защиты.

Такая архитектура безопасности допускает разнообразные стратегии безопасности, включая базирующиеся на правилах, на идентичности и их сочетание. Эта архитектура безопасности обеспечивает также защиту, вводимую административными средствами, динамически выбираемую или сочетающую в себе оба этих варианта.

6.2.1.2 *Запросы услуги*

Для каждого запроса (N)-услуги (N + 1)-объект может запрашивать необходимую целевую защиту безопасности. Запрос (N)-услуги определяет услуги безопасности и параметры и дополнительную соответствующую информацию (такую, как информация критичности и/или метки безопасности), необходимые для обеспечения целевой защиты безопасности.

Перед созданием каждого экземпляра связи (N)-уровень должен обратиться в базу информации управления безопасностью (SMIB) (см. п. 8.1). SMIB содержит информацию о требованиях к административно вводимой защите, связанных с (N + 1)-объектом. Для обеспечения выполнения этих требований к административно вводимой защите требуется доверенная функциональность.

Обеспечение функций безопасности в период существования экземпляра связи с установлением соединения может потребовать согласования требуемых услуг безопасности. Процедуры, необходимые для согласования механизмов и параметров, могут выполняться как отдельная процедуры или как составная часть обычной процедуры установления соединения.

Если согласование выполняется как отдельная процедура, согласованные результаты (то есть типы механизмов безопасности и параметры безопасности, необходимые для обеспечения данных услуг безопасности) вводятся в базу информации управления безопасностью (см. п. 8.1).

Если согласование выполняется как составная часть обычной процедуры установления соединения, результаты согласования между (N)-объектами будут временно сохранены в SMIB. Перед согласованием каждый (N)-объект обращается в SMIB с целью получения необходимой для согласования информации.

(N)-уровень отклонит запрос услуги, если он нарушает административно вводимые требования, занесенные в SMIB для (N + 1)-уровня.

(N)-уровень добавит также к запрошенным услугам защиты любые услуги безопасности, которые определены в SMIB как обязательные для достижения целевой защиты безопасности.

Если (N + 1)-объект не определяет целевую защиту безопасности, (N)-уровень будет следовать стратегии безопасности в соответствии с данными SMIB. Это может быть связь с использованием защиты безопасности по умолчанию в диапазоне, определенном для (N + 1)-объекта в SMIB.

6.2.2 *Предоставление услуг защиты*

После определения сочетания административно вводимых и динамически выбираемых требований к безопасности, согласно п. 6.2.1, (N)-уровень попытается обеспечить как минимум целевую защиту. Это достигается с помощью одного или обоих указанных ниже методов:

a) активизация механизмов безопасности непосредственно на (N)-уровне; и/или

b) запрос услуг защиты из (N – 1)-уровня. В этом случае область защиты должна быть расширена для включения (N)-услуги путем сочетания доверенной функциональности и/или конкретных механизмов безопасности на (N)-уровне.

   Примечание. – Это не обязательно подразумевает, что вся функциональность на (N)-уровне должна быть доверенной.

Таким образом, (N)-уровень определяет возможность достижения запрошенной целевой защиты. Если достичь ее невозможно, экземпляр связи не появляется.

6.2.2.1 *Установление защищенного (N)-соединения*

Ниже рассматривается предоставление услуг в пределах (N)-уровня (в противоположность использованию (N – 1)-услуг).

В некоторых протоколах для достижения удовлетворительной целевой защиты решающее значение имеет последовательность операций.

a) *Постоянное управление доступом*

   (N)-уровень может вводить постоянные операции управление доступом, то есть он может локально (из SMIB) определять, допустима или запрещена попытка установления защищенного (N)-соединения.

b) *Аутентификация однорангового объекта*

   Если целевая защита включает аутентификацию однорангового объекта или если известно (из SMIB), что (N)-объект в пункте назначения потребует аутентификацию однорангового объекта, то должен выполняться аутентификационный обмен. Это может повлечь использование двух- или трехсторонней процедуры установления соединения для выполнения односторонней или взаимной аутентификации, в зависимости от требований.

   Иногда аутентификационный обмен может быть составной частью обычных процедур установления (N)-соединения. В других условиях аутентификационный обмен может выполняться отдельно от установления (N)-соединения.

c) *Услуга управления доступом*

(N)-объект назначения или промежуточные объекты могут вводить ограничения управления доступом. Если механизм дистанционного управления доступом запрашивает конкретную информацию, то являющийся инициатором (N)-объект предоставляет эту информацию в рамках протокола (N)-уровня или по каналам управления.

d) *Конфиденциальность*

Если выбрана полная или селективная конфиденциальность, должно быть установлено защищенное (N)-соединение. Это должно включать установление надлежащего(их) рабочего(их) ключа(ей) и согласование криптографических параметров соединения. Это может выполняться на основе предварительных договоренностей, в рамках аутентификационного обмена или с помощью специального протокола.

e) *Целостность данных*

Если выбрана целостность всех (N)-данных-пользователя, с восстановлением или без него, или целостность отдельных полей, должно быть установлено защищенное (N)-соединение. Это может быть то же соединение, что и установленное для обеспечения услуги конфиденциальности и может обеспечивать аутентификацию. В отношении защищенного (N)-соединения применяются те же соображения, что и в отношении услуги конфиденциальности.

f) *Услуги "предотвращения отказа от авторства"*

Если выбрано "предотвращение отказа от авторства" с подтверждением источника, должны быть установлены надлежащие криптографические параметры или должно быть установлено защищенное соединение с объектом заверения.

Если выбрано "предотвращение отказа от авторства" с подтверждением доставки, должны быть установлены надлежащие параметры (отличные от параметров, требуемых для "предотвращения отказа от авторства" с подтверждением источника) или должно быть установлено защищенное соединение с объектом заверения.

Примечание. – Установление защищенного (N)-соединения может оказаться невыполненным в связи с отсутствием соглашения относительно криптографических параметров (возможно включая отсутствие владения надлежащими ключами) или в силу его отклонения механизмом управления доступом.

6.2.3 *Работа защищенного (N)-соединения*

6.2.3.1 На этапе передачи данных защищенного (N)-соединения должны обеспечиваться согласованные услуги защиты.

На границе (N)-услуги очевидно будет выполняться следующее:

a) аутентификация однорангового объекта (с интервалами);

b) селективная защита полей; и

c) сообщение об активных атаках (например, в случае манипуляции данными и в случае услуги, предоставляемой как "целостность в режиме установления соединения без восстановления" – см. п. 5.2.4.2).

Наряду с этим может потребоваться следующее:

a) ведение журнала аудита безопасности; и

b) обнаружение и обработка событий.

6.2.3.2 *Следующие услуги могут применяться в селективном режиме*:

a) конфиденциальность;

b) целостность данных (возможно с аутентификацией); и

c) предотвращение отказа от авторства (получателя или отправителя).

Примечание 1. – Для отметки элементов данных, выбранных для применения той или иной услуги, предлагаются два метода. Первый предусматривает строгую типизацию. Предполагается, что уровень представления распознает определенные типы как типы, требующие применения конкретных услуг защиты. Второй способ предусматривает определенную форму установления флагов в отдельных элементах данных, к которым следует применять конкретные услуги защиты.

Примечание 2. – Предполагается, что одна из причин осуществления селективного применения услуг "предотвращения отказа от авторства" может возникать в результате следующего сценария. До того как оба (N)-объекта придут к соглашению о взаимной приемлемости окончательной версии элемента данных, в рамках ассоциации происходит определенный диалог согласования. На этом этапе целевой получатель может просить отправителя применить к окончательно согласованной версии элемента данных услуги "предотвращения отказа от авторства" (в отношении и источника и доставки). Отправитель запрашивает и получает эти услуги, передает элемент данных и далее получает извещение о том, что элемент данных был получен и получатель подтвердил получение. Услуги "предотвращения отказа от авторства" гарантируют и отправителю и получателю элемента данных успешную передачу этого элемента данных.

Примечание 3. – Обе услуги "предотвращения отказа от авторства" (то есть в отношении источника и доставки) вызываются отправителем.

6.2.4 *Обеспечение защищенной передачи данных в режиме без установления соединения*

Не все услуги безопасности, доступные в протоколах с установлением соединения, доступны в протоколах в режиме без установления соединения. В частности, защита от атак, предпринимаемых в целях удаления, включения и повторной передачи данных, если необходимо, должна предоставляться на более высоких уровнях с установлением соединения. Ограниченная защита от атак с целью повторной передачи может обеспечиваться с помощью механизма установления отметок. Кроме того, ряд других услуг безопасности не могут обеспечить тот же уровень применения мер безопасности, который может быть достигнут протоколами с установлением соединения.

Для передачи данных в режиме без установления соединения могут использоваться следующие услуги защиты:

a) аутентификация однорангового объекта (см. п. 5.2.1.1);

b) аутентификация источника данных (см. п. 5.2.1.2);

c) услуга управления доступом (см. п. 5.2.2);

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

e) селективная конфиденциальность полей (см. п. 5.2.3.3);

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

g) селективная целостность полей в режиме без установления соединения (см. п. 5.2.4.5); и

h) предотвращение отказа от авторства, источник (см. п. 5.2.5.1).

Эти услуги предоставляются с помощью механизмов шифрования, подписи, управления доступом, маршрутизации, обеспечения целостности данных и/или механизмов заверения (см. п. 5.3).

Инициатор передачи данных в режиме без установления соединения должен обеспечить, чтобы его отдельный SDU содержал всю информацию, которая необходима для приемлемости его SDU в пункте назначения.

7 Размещение услуг и механизмов безопасности

В данном разделе определяются услуги безопасности, которые должны обеспечиваться в рамках базовой эталонной модели ВОС, и описывается способ предоставления этих услуг. Обеспечение любой услуги безопасности является необязательным и определяется требованиями.

Если конкретная услуга безопасности определяется в данном разделе как не обязательно обеспечиваемая конкретным уровнем, то эта услуга безопасности обеспечивается механизмами безопасности, функционирующими на данном уровне, если не указано иное. Как показано в разделе 6, многие уровни будут предлагать конкретные услуги безопасности. Эти уровни не всегда предоставляют услуги безопасности в рамках своего уровня, но могут использовать соответствующие услуги безопасности, обеспечиваемые нижними уровнями. Даже если какой-либо уровень не обеспечивает услуг безопасности, может потребоваться изменение определения услуг этого уровня, с тем чтобы сделать возможными запросы услуг безопасности, направляемые в какой-либо нижний уровень.

Примечание 1. – Универсальные механизмы безопасности (см. п. 5.4) в данном разделе не рассматриваются.

Примечание 2. – Выбор местоположения механизмов шифрования для приложений рассматривается в Приложении C.

7.1 *Физический уровень*

7.1.1 *Услуги*

На физическом уровне обеспечиваются только следующие услуги, по отдельности или в сочетании:

a) конфиденциальность в режиме установления соединения; и

b) конфиденциальность потока трафика.

Услуга конфиденциальности потока трафика имеет две формы:

1) полная конфиденциальность потока трафика, которая может обеспечиваться только в определенных условиях, например двусторонняя, одновременная, синхронная передача из пункта в пункт; и

2) ограниченная конфиденциальность потока трафика, которая может обеспечиваться для других типов передачи, например для асинхронной передачи.

Эти услуги безопасности ограничиваются пассивными угрозами и могут применяться в случае связи из пункта в пункт или многопунктовой одноранговой связи.

7.1.2 *Механизмы*

На физическом уровне основной механизм безопасности составляет полное шифрование потока данных.

Конкретной формой шифрования, применяемой только на физическом уровне, является безопасность передачи (то есть безопасность распределенного спектра).

Защита физического уровня обеспечивается с помощью устройства шифрования, которое функционирует прозрачно. Задачей защиты физического уровня является защита всего физического битового потока данных услуги и обеспечение конфиденциальности потока трафика.

7.2 *Канальный уровень*

7.2.1 *Услуги*

На канальном уровне обеспечиваются только следующие услуги:

a) конфиденциальность в режиме установления соединения; и

b) конфиденциальность в режиме без установления соединения.

7.2.2 *Механизмы*

На канальном уровне для обеспечения услуг безопасности используется механизм шифрования (см. Приложение C).

Дополнительная функциональность защиты безопасности канального уровня выполняется до обычных функций уровня, предназначенных для передачи, и после обычных функций уровня, предназначенных для приема, то есть механизмы безопасности базируются на обычных функциях уровня и используют все обычные функции уровня.

Механизмы шифрования на канальном уровне критичны к протоколу канального уровня.

7.3 *Сетевой уровень*

Сетевой уровень по сути организован для обеспечения протокола(ов), предназначенных для выполнения следующих операций:

a) доступ к подсети;

b) зависящая от подсети конвергенция;

c) не зависящая от подсети конвергенция; и

d) ретрансляция и маршрутизация.

7.3.1 *Услуги*

Протокол, выполняющий функции доступа к подсети, которые связаны с обеспечением сетевых услуг ВОС, может обеспечивать следующие услуги безопасности:

a) аутентификация однорангового объекта;

b) аутентификация источника данных;

c) услуга управления доступом;

d) конфиденциальность в режиме установления соединения;

e) конфиденциальность в режиме без установления соединения;

f) конфиденциальность потока трафика;

g) целостность в режиме установления соединения без восстановления; и

h) целостность в режиме без установления соединения.

Эти услуги безопасности могут обеспечиваться по отдельности или в сочетании. Услуги безопасности, которые могут быть обеспечены протоколом, выполняющим операции ретрансляции и маршрутизации, связанные с обеспечением сетевых услуг ВОС от оконечной системы к оконечной системе, те же, что и услуги, обеспечиваемые протоколом, выполняющим операции доступа к подсети.

7.3.2 *Механизмы*

7.3.2.1 Протокол(ы), выполняющий(е) операции доступа к подсети и операции ретрансляции и маршрутизации, связанные с обеспечением сетевых услуг ВОС от оконечной системы к оконечной системе, использует(ют) идентичные механизмы безопасности. На этом уровне выполняется маршрутизация и, следовательно, управление маршрутизацией находится на этом же уровне. Указанные услуги безопасности обеспечиваются следующим образом:

a) услуга аутентификации однорангового объекта обеспечивается надлежащим сочетанием имеющих криптографическую основу или защиту аутентификационных обменов, защищенного обмена паролями и механизмами подписи;

b) услуга аутентификации источника данных может обеспечиваться с помощью механизмов шифрования и подписи;

c) услуга управления доступом обеспечивается путем надлежащего использования определенных механизмов управления доступом;

d) услуга конфиденциальности в режиме установления соединения обеспечивается с помощью механизма шифрования и/или управления маршрутизацией;

e) услуга конфиденциальности в режиме без установления соединения обеспечивается с помощью механизмов шифрования и/или управления маршрутизацией;

f) услуга конфиденциальности потока трафика обеспечивается с помощью механизма подстановки трафика в сочетании с услугой конфиденциальности на сетевом уровне или ниже и/или управления маршрутизации;

g) услуга целостности в режиме установления соединения без восстановления обеспечивается с помощью использования механизма целостности данных, иногда в увязке с механизмом шифрования; и

h) услуга целостности в режиме без установления соединения обеспечивается с помощью использования механизма целостности данных, иногда в увязке с механизмом шифрования.

7.3.2.2 Механизмы в протоколе, который выполняет операции доступа к подсети, связанные с обеспечением сетевых услуг ВОС от оконечной системы к оконечной системе, предоставляют услуги в одной подсети.

Защита подсети, введенная администрацией подсети, будет применяться в соответствии с предписаниями протоколов доступа к подсети, но, как правило, будет применяться до обычных функций подсети при передаче и после обычных функций подсети при получении.

7.3.2.3 Механизмы, обеспечиваемые протоколом, который выполняет операции ретрансляции и маршрутизации, связанные с обеспечением сетевых услуг ВОС от оконечной системы к оконечной системе, предоставляют услуги в одной или нескольких присоединенных сетях.

Эти механизмы будут активироваться до выполнения функций ретрансляции и маршрутизации после передачи и после функций ретрансляции и маршрутизации после получения. В случае механизма управления маршрутизацией соответствующие ограничения маршрутизации получают из SMIB до того, как данные вместе с необходимыми ограничениями маршрутизации поступят к функциям ретрансляции и маршрутизации.

7.3.2.4 Управление доступом на сетевом уровне может выполнять много задач. Например, оно дает оконечной системе возможность управлять установлением сетевых соединений и отклонять нежелательные вызовы. Оно также обеспечивает возможность одной или нескольким подсетям управлять использованием ресурсов сетевого уровня. В некоторых случаях эта последняя задача связана с начислением платы за использование сети.

Примечание. – Установление сетевого соединения зачастую приводит к начислению платы администрацией подсети. Снизить затраты можно путем управления доступом и выбора начисления платы на вызываемого абонента или других определяемых сетью параметров.

7.3.2.5 Требование какой-либо конкретной подсети может вводить механизмы управления доступом в протокол, который выполняет операции доступа к подсети, связанные с обеспечением сетевых услуг ВОС от оконечной системы к оконечной системе. Если механизмы управления доступом обеспечиваются протоколом, который выполняет операции ретрансляции и маршрутизации, связанные с обеспечением сетевых услуг ВОС от оконечной системы к оконечной системе, они могут использоваться объектами ретрансляции для управления доступом к подсетям, и использоваться для управления доступом к оконечным системам. Очевидно, что область обособления управления доступом определяется достаточно широко, различая только объекты сетевого уровня.

7.3.2.6 Если подстановка трафика используется в сочетании с механизмом шифрования на сетевом уровне (или услугой конфиденциальности из сетевого уровня), то возможно достижение приемлемого уровня конфиденциальности потока трафика.

7.4 *Транспортный уровень*

7.4.1 *Услуги*

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

a) аутентификация однорангового объекта;

b) аутентификация источника данных;

c) услуга управления доступом;

d) конфиденциальность в режиме установления соединения;

e) конфиденциальность в режиме без установления соединения;

f) целостность в режиме установления соединения с восстановлением;

g) целостность в режиме установления соединения без восстановления; и

h) целостность в режиме без установления соединения.

7.4.2 *Механизмы*

Указанные услуги безопасности обеспечиваются следующим образом:

a) услуга аутентификации однорангового объекта обеспечивается надлежащим сочетанием имеющих криптографическую основу или защиту аутентификационных обменов, защищенного обмена паролями и механизмами подписи;

b) услуга аутентификации источника данных может обеспечиваться с помощью механизмов шифрования и подписи;

c) услуга управления доступом обеспечивается путем надлежащего использования определенных механизмов управления доступом;

d) услуга конфиденциальности в режиме установления соединения обеспечивается с помощью механизма шифрования;

e) услуга конфиденциальности в режиме без установления соединения обеспечивается с помощью механизма шифрования;

f) услуга целостности в режиме установления соединения с восстановлением обеспечивается с помощью использования механизма целостности данных, иногда в увязке с механизмом шифрования;

g) услуга целостности в режиме установления соединения без восстановления обеспечивается с помощью использования механизма целостности данных, иногда в увязке с механизмом шифрования; и

h) услуга целостности в режиме без установления соединения обеспечивается с помощью использования механизма целостности данных, иногда в увязке с механизмом шифрования.

Механизмы защиты будут работать таким образом, чтобы обеспечивать возможность вызова услуг безопасности для отдельного транспортного соединения. Защита будет такой, что отдельное транспортное соединение может быть изолированным от всех других транспортных соединений.

7.5 *Сеансовый уровень*

7.5.1 *Услуги*

На сеансовом уровне услуги безопасности не обеспечиваются.

7.6 *Уровень представления*

7.6.1 *Услуги*

Уровень представления будет обеспечивать средства в поддержку обеспечения следующих услуг безопасности прикладным уровнем для прикладного процесса:

a) конфиденциальность в режиме установления соединения;

b) конфиденциальность в режиме без установления соединения; и

c) селективная конфиденциальность полей.

Средства уровня представления могут также поддерживать обеспечение следующих услуг безопасности прикладным уровнем для прикладного процесса:

d) конфиденциальность потока трафика;

e) аутентификация однорангового объекта;

f) аутентификация источника данных;

g) целостность в режиме установления соединения с восстановлением;

h) целостность в режиме установления соединения без восстановления;

j) селективная целостность полей в режиме установления соединения;

k) целостность в режиме без установления соединения;

m) селективная защита полей в режиме без установления соединения;

n) предотвращение отказа от авторства с подтверждением источника; и

p) предотвращение отказа от авторства с подтверждением доставки.

Примечание. – Обеспечиваемые уровнем представления средства – это средства, базирующиеся на механизмах, которые могут функционировать только при кодировании синтаксиса передачи данных и будут включать, например, средства, базирующиеся на криптографических методах.

7.6.2 *Механизмы*

Поддерживающие механизмы для следующих услуг безопасности могут размещаться на уровне представления и в таком случае могут использоваться в сочетании с механизмами безопасности прикладного уровня для обеспечения услуг безопасности прикладного уровня:

a) услуга аутентификации однорангового объекта может поддерживаться механизмами синтаксического преобразования (например, шифрование);

b) услуга аутентификации источника данных может поддерживаться механизмами шифрования или подписи;

c) услуга конфиденциальности в режиме установления соединения может поддерживаться механизмом шифрования;

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

e) услуга селективной конфиденциальности полей может поддерживаться механизм шифрования;

f) услуга конфиденциальности потока трафика может поддерживаться механизмом шифрования;

g) услуга целостности в режиме установления соединения с восстановлением может поддерживаться механизмом целостности данных, иногда в сочетании с механизмом шифрования;

h) услуга целостности в режиме установления соединения без восстановления может поддерживаться механизмом целостности данных, иногда в сочетании с механизмом шифрования;

j) услуга селективной целостности полей в режиме установления соединения может поддерживаться механизмом целостность данных, иногда в сочетании с механизмом шифрования;

k) услуга целостности в режиме без установления соединения может поддерживаться механизмом целостности данных, иногда в сочетании с механизмом шифрования;

m) услуга селективной защиты полей в режиме без установления соединения может поддерживаться механизмом целостности данных, иногда в сочетании с механизмом шифрования;

n) услуга "предотвращения отказа от авторства" с подтверждением источника может поддерживаться надлежащей комбинацией механизмов целостности данных, подписи и заверения; и

p) услуга "предотвращения отказа от авторства" с подтверждением доставки может поддерживаться надлежащей комбинацией механизмов целостности данных, подписи и заверения.

Механизмы шифрования, применяемые в отношении передачи данных, если они размещены на верхних уровнях, будут содержаться на уровне представления.

Некоторые из перечисленных выше услуг безопасности могут альтернативно обеспечиваться механизмами безопасности, полностью содержащимися на прикладном уровне.

Только услуги конфиденциальности могут целиком обеспечиваться механизмами безопасности, содержащимися на уровне представления.

Механизмы безопасности на уровне представления функционируют в качестве завершающего этапа преобразования в синтаксис передачи при передаче и в качестве начального этапа процесса преобразования при получении.

7.7 *Прикладной уровень*

7.7.1 *Услуги*

Прикладной уровень может обеспечивать одну или несколько следующих базовых услуг безопасности по отдельности или в комбинации:

a) аутентификация однорангового объекта;

b) аутентификация источника данных;

c) услуга управления доступом;

d) конфиденциальность в режиме установления соединения;

e) конфиденциальность в режиме без установления соединения;

f) селективная конфиденциальность полей;

g) конфиденциальность потока трафика;

h) целостность в режиме установления соединения с восстановлением;

j) целостность в режиме установления соединения без восстановления;

k) селективная целостность полей в режиме установления соединения;

m) целостность в режиме без установления соединения;

n) селективная защита полей в режиме без установления соединения;

p) предотвращение отказа от авторства с подтверждением источника; и

q) предотвращение отказа от авторства с подтверждением доставки.

Аутентификация предопределенных партнеров по связи обеспечивает поддержку управления доступом к ресурсам, как относящимся, так и не относящимся к ВОС (например, файлы, программное обеспечение, терминалы, принтеры), в реальных открытых системах.

Определение конкретных требований безопасности в экземпляре связи, включая конфиденциальность, целостность и аутентификацию данных, может выполняться управлением безопасностью ВОС или управлением прикладного уровня на основании информации SMIB наряду с запросами, осуществляемыми прикладным процессом.

7.7.2 *Механизмы*

Услуги безопасности на прикладном уровне обеспечиваются с помощью следующих механизмов:

a) услуга аутентификации однорангового объекта может обеспечиваться с использованием аутентификационной информации, передаваемой между прикладными объектами, защищенными механизмами шифрования уровня представления или более низкого уровня;

b) услуга аутентификации источника данных может поддерживаться путем использования механизмов подписи или механизмами шифрования более низкого уровня;

c) услуга управления доступом к тем аспектам реальной открытой системы, которые относятся к ВОС, такие как способность связи с определенными системами или дистанционными прикладными объектами, может обеспечиваться с помощью сочетания механизмов управления доступом на прикладном уровне или на более низких уровнях;

d) услуга конфиденциальности в режиме установления соединения может поддерживаться путем использования механизма шифрования более низкого уровня;

e) услуга конфиденциальности в режиме без установления соединения может поддерживаться путем использования механизма шифрования более низкого уровня;

f) услуга селективной конфиденциальности полей может поддерживаться путем использования механизма шифрования уровня представления;

g) услуга ограниченной конфиденциальности потока трафика может поддерживаться путем использования механизма подстановки трафика на прикладном уровне в сочетании с услугой конфиденциальности на более низком уровне;

h) услуга целостности в режиме установления соединения с восстановлением может поддерживаться путем использования механизмов целостности данных более низкого уровня (иногда в сочетании с механизмом шифрования);

j) услуга целостности в режиме установления соединения без восстановления может поддерживаться путем использования механизма целостности данных более низкого уровня (иногда в сочетании с механизмом шифрования);

k) услуга селективной целостности полей в режиме установления соединения может поддерживаться путем использования механизма целостности данных (иногда в сочетании с механизмом шифрования) на уровне представления;

m) услуга целостности в режиме без установления соединения может поддерживаться путем использования механизма целостности данных более низкого уровня (иногда в сочетании с механизмом шифрования);

n) услуга селективной защиты полей в режиме без установления соединения может поддерживаться путем использования механизма целостности данных (иногда в сочетании с механизмом шифрования) на уровне представления;

p) услуга "предотвращения отказа от авторства" с подтверждением источника может поддерживаться соответствующим сочетанием механизмов подписи и механизмов обеспечения целостности данных более низкого уровня, вероятно, совместно с нотариусами третьей стороны; и

q) услуга "предотвращения отказа от авторства" с подтверждением доставки может поддерживаться соответствующим сочетанием механизмов подписи и механизмов обеспечения целостности данных более низкого уровня, вероятно, совместно с нотариусами третьей стороны.

Если для обеспечения услуги "предотвращения отказа от авторства" используется механизм заверения, он будет функционировать в качестве доверенной третьей стороны. Он может располагать записью блоков данных, ретранслируемых в их форме передачи (например, синтаксис передачи), для целей разрешения споров. Он может использовать услуги защиты из более низких уровней.

7.7.3 *Услуги безопасности, не относящиеся к ВОС*

Прикладные процессы сами могут обеспечивать практически все услуги и использовать те же типы механизмов, что и описанные в настоящей Рекомендации, так как они соответствующим образом размещены на разных уровнях архитектуры. Такое использование механизмов не входит в сферу определения услуг и протоколов ВОС и архитектуры ВОС, но и не противоречит им.

7.8 *Иллюстрация взаимосвязи услуг безопасности и уровней*

В таблице 2/X.800 показаны уровни эталонной модели, на которых могут обеспечиваться конкретные услуги безопасности. Описание услуг безопасности приведено в п. 5.2. Обоснования размещения услуг на конкретных уровнях приведены в Приложении B.

ТАБЛИЦА 2/X.800

Иллюстрация взаимосвязи услуг безопасности и уровней

Услуга	Уровень						
	1	2	3	4	5	6	7*
Аутентификация однорангового объекта	·	·	Д	Д	·	·	Д
Аутентификация источника данных	·	·	Д	Д	·	·	Д
Услуга управления доступом	·	·	Д	Д	·	·	Д
Конфиденциальность в режиме установления соединения	Д	Д	Д	Д	·	Д	Д
Конфиденциальность в режиме без установления соединения	·	Д	Д	Д	·	Д	Д
Селективная конфиденциальность полей	·	·	·	·	·	Д	Д
Конфиденциальность потока трафика	Д	·	Д	·	·	·	Д
Целостность в режиме установления соединения с восстановлением	·	·	·	Д	·	·	Д
Целостность в режиме установления соединения без восстановления	·	·	Д	Д	·	·	Д
Селективная целостность полей в режиме установления соединения	·	·	·	·	·	·	Д
Целостность в режиме без установления соединения	·	·	Д	Д	·	·	Д
Селективная защита полей в режиме без установления соединения	·	·	·	·	·	·	Д
Предотвращение отказа от авторства, источник	·	·	·	·	·	·	Д
Предотвращение отказа от авторства, доставка	·	·	·	·	·	·	Д

Д Да, услугу следует включить в стандарты для данного уровня как вариант поставщика.

· Не обеспечивается.

* Следует заметить в отношении уровня 7, что прикладные процессы могут сами обеспечивать услуги безопасности.

Примечание 1. – В таблице 2/X.800 не предполагается указания на то, что элементы имеют равное значение или важность, напротив, элементы таблицы существенно различаются по масштабу.

Примечание 2. – Размещение услуг безопасности по уровням сети описано в п. 7.3.2. Местоположение услуг безопасности в рамках уровня сети имеет значительное воздействие на характер и сферу действия услуг, которые будут предоставляться.

Примечание 3. – Уровень представления содержит ряд средств безопасности, которые поддерживают предоставление услуг безопасности прикладным уровнем.

8 Управление безопасностью

8.1 *Общее*

8.1.1 Управление безопасностью ВОС связано с аспектами управления безопасностью, относящимися к ВОС и безопасности управления ВОС. Аспекты управления безопасностью ВОС связаны с операциями, не входящими в рамки обычных экземпляров связи, но необходимыми для поддержки и управления аспектами безопасности этой связи.

Примечание. – Доступность услуги связи определяется проектным решением сети и/или протоколами управления сетью. Надлежащий выбор этого необходим для защиты от отказа в обслуживании.

8.1.2 Администрация(и) распределенных открытых систем может(гут) вводить большое число стратегий безопасности, и рекомендации по управлению безопасностью ВОС должны поддерживать эти стратегии. Объекты, которые являются предметом одной стратегии безопасности и управляются одним полномочным органом, иногда собираются в так называемый домен безопасности. Домены безопасности и их взаимодействие составляют важную область будущего расширения.

8.1.3 Управление безопасностью ВОС связано с управлением услугами и механизмами безопасности ВОС. Такое управление требует распределения информации управления между этими услугами и механизмами, а также сбора информации, касающейся функционирования этих услуг и механизмов. Примерами являются распределение криптографических ключей, установление параметров выбора услуги, вводимых административно, представление отчета о штатных и нештатных событиях безопасности (журналы аудита) и активация и деактивация услуг. Управление безопасностью не затрагивает прохождение связанной с безопасностью информации в протоколах, которые вызывают конкретные услуги (например, в параметрах запроса соединения).

8.1.4 База информации управления безопасностью (SMIB) – это концептуальный репозиторий всей относящейся к безопасности информации, необходимой для открытых систем. Эта концепция не предполагает какой-либо формы для хранения информации или ее реализации. Вместе с тем каждая оконечная система должна содержать необходимую местную информацию, которая обеспечит ей возможность реализации надлежащей стратегии безопасности. SMIB является распределенной базой информации в такой степени, каковая необходима для реализации последовательной стратегии безопасности в (логической или физической) группировке оконечных систем. На практике части SMIB могут быть интегрированы или не интегрированы в MIB.

Примечание. – Возможны разнообразные формы реализации SMIB, например:

a) таблица данных;

b) файл;

c) данные или правила, встроенные в программное или аппаратное обеспечение реальных открытых систем.

8.1.5 Протоколы управления, в частности протоколы управления безопасностью, и каналы связи, по которым передается информация управления, потенциально уязвимы. Следовательно, необходимо уделять особое внимание обеспечению защиты протоколов и информации управления, с тем чтобы не ослабить защиту безопасности, обеспечиваемую для обычных экземпляров связи.

8.1.6 Управление безопасностью может требовать обмена информацией, касающейся безопасности, между различными системными администрациями в целях установления или расширения SMIB. В некоторых случаях относящаяся к безопасности информация будет проходить через тракты связи, не входящие в ВОС, и администраторы местных систем будут обновлять SMIB с помощью методов, не стандартизованных ВОС. В других случаях может оказаться желательным провести обмен такой информацией через тракт связи ВОС, и тогда информация будет проходить между двумя приложениями управления безопасностью, выполняемыми в реальных открытых системах. Приложение управления безопасностью будет использовать передаваемую для обновления SMIB. Такое обновление SMIB может потребовать предварительной авторизации соответствующего администратора безопасности.

8.1.7 Для обмена относящейся к безопасности информацией по каналам связи ВОС будут определяться прикладные протоколы.

8.2 *Категории управления безопасностью*

Существует три категории операций управления безопасностью ВОС:

a) управление безопасностью системы;

b) управление услугой безопасности; и

c) управление механизмом безопасности.

Наряду с этим следует учитывать безопасность самого управления ВОС (см. п. 8.2.4). Ниже кратко представлены ключевые функции, выполняемые этими категориями управления безопасностью.

8.2.1 *Управление безопасностью системы*

Управление безопасностью системы связано с управлением аспектами безопасности всей среды ВОС. Ниже перечислены типовые операции, входящие в категорию управления безопасностью:

a) общее управление стратегией безопасности, включая обновления и поддержание согласованности;

b) взаимодействие с другими функциями управления ВОС;

c) взаимодействие с управлением услугами безопасности и управлением механизмами безопасности;

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

e) управление аудитом безопасности (см. п. 8.3.2); и

f) управление восстановлением безопасного состояния (см. п. 8.3.3).

8.2.2 *Управление услугами безопасности*

Управление услугами безопасности связано с управлением конкретными услугами безопасности. Ниже перечислены типовые операции, которые могут выполняться в рамках управления конкретной услугой безопасности:

a) определение и присвоение целевой защиты безопасности для услуги;

b) присвоение и актуализация правил выбора (в случае существования альтернативы) конкретных механизмов безопасности, которые должны использоваться для обеспечения запрошенной услуги безопасности;

c) согласование (местное и дистанционное) доступных механизмов безопасности, которые требуют предварительного соглашения об управлении;

d) вызов конкретных механизмов безопасности через соответствующую функцию управления механизмом безопасности, например для обеспечения административно вводимых услуг безопасности; и

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

8.2.3 *Управление механизмами безопасности*

Управление механизмами безопасности связано с управлением конкретными механизмами безопасности. Представленный ниже перечень функций управления механизмами безопасности является типовым, но не исчерпывающим:

a) управление ключами;

b) управление шифрованием;

c) управление цифровыми подписями;

d) управление управлением доступом;

e) управление целостностью данных;

f) управление аутентификацией;

g) управление подстановкой трафика;

h) управление управлением маршрутизации; и

j) управление заверением.

Каждая из перечисленных функций управления механизмами безопасности подробно рассматривается в п. 8.4.

8.2.4 *Управление безопасностью ВОС*

Безопасность всех функций управления и передачи информации управления ВОС является важной составляющей безопасности ВОС. Эта категория управления безопасностью предполагает надлежащий выбор перечисленных услуг и механизмов безопасности ВОС (см. п. 8.1.5), с тем чтобы обеспечить необходимую защиту протоколов и информации управления ВОС. Например, связь между объектами управления, в которой участвует база информации управления, будет требовать, как правило, определенной формы защиты.

8.3 *Конкретные операции управления безопасностью системы*

8.3.1 *Управление обработкой событий*

Аспекты управления обработкой событий, очевидные в ВОС, это дистанционное сообщение о явных попытках нарушения безопасности системы и изменение пороговых значений, используемых для включения операции сообщения о событии.

8.3.2 *Управление аудитом безопасности*

Управление аудитом безопасности может включать:

a) выбор событий, подлежащих регистрации и/или дистанционному сбору;

b) разрешение и запрещение регистрации в журнале аудита выбранных событий;

c) дистанционный сбор выбранных записей аудита; и

d) составление отчетов об аудите безопасности.

8.3.3 *Управление восстановлением безопасного состояния*

Управление восстановлением безопасного состояния может включать:

a) актуализацию правил, используемых для реагирования на реальные или подозреваемые нарушения безопасности;

b) дистанционное сообщение о явных нарушениях безопасности системы;

c) взаимодействие, осуществляемое администратором безопасности.

8.4 *Функции управления механизмами безопасности*

8.4.1 *Управление ключами*

Управление ключами может включать следующие операции:

a) генерация соответствующих ключей с интервалами, соразмерных требуемому уровню безопасности;

b) определение в соответствии с требованиями управления доступом тех объектов, которые должны получить копию каждого ключа; и

c) предоставление экземплярам объекта в реальных открытых системах или распределение между ними ключей безопасным образом.

Известно, что некоторые функции управления ключами будут выполняться за пределами среды ВОС. Это включает физическое распределение ключей безопасными средствами.

Обмен рабочими ключами для их использования в течение ассоциации – это обычная функция протокола уровня. Выбор рабочих ключей может также выполняться путем доступа к центру распределения ключей или путем предварительного распределения через протоколы управления.

8.4.2 *Управление шифрованием*

Управление шифрованием может включать:

a) взаимодействие с управлением ключами;

b) установление криптографических параметров;

c) криптографическую синхронизацию.

Существование механизма шифрования обусловливает использование управления ключами и общих способов ссылки на криптографические алгоритмы.

Приемлемая для шифрования степень подавления защиты определяется тем, какие объекты в среде ВОС имеют независимые ключи. Это в свою очередь определяется в целом архитектурой безопасности и конкретно – механизмом управления ключами.

Общую ссылку на криптографические алгоритмы можно получить путем использования реестра криптографических алгоритмов или путем предварительных соглашений между объектами.

8.4.3 *Управление цифровыми подписями*

Управление цифровыми подписями может включать:

a) взаимодействие с управлением ключами;

b) установление криптографических параметров и алгоритмов; и

c) использование протокола между взаимодействующими объектами и, возможно, третьей стороной.

Примечание. – В целом между управлением цифровыми подписями и управлением шифрованием много общего.

8.4.4 *Управление управлением доступом*

Управление управлением доступом может включать распределение атрибутов безопасности (в том числе пароли) или обновление списков управления доступом или списков возможностей. Оно может также включать использование протокола между взаимодействующими объектами и другими объектами, обеспечивающими услуги управления доступом.

8.4.5 *Управление целостностью данных*

Управление целостностью данных может включать:

a) взаимодействие с управлением ключами;

b) установление криптографических параметров и алгоритмов; и

c) использование протокола между взаимодействующими объектами.

Примечание. – При использовании криптографических методов для обеспечения целостности данных управление целостностью данных и управление шифрованием весьма схожи.

8.4.6 *Управление аутентификацией*

Управление аутентификацией может включать описательную информацию, пароли или ключи (используя управление ключами) для объектов, требуемых для выполнения аутентификации. Это может также включать использование протокола между взаимодействующими объектами и другими объектами, обеспечивающими услуги аутентификации.

8.4.7 *Управление подстановкой трафика*

Управление подстановкой трафика может включать актуализацию правил, которые должны использоваться для подстановки трафика. Например:

a) предварительно определенная скорость передачи данных;

b) определение скорости произвольных данных;

c) определение характеристик сообщений, таких как длина; и

d) изменение спецификации, вероятно, в соответствии с временем суток и/или по календарю.

8.4.8 *Управление управлением маршрутизацией*

Управление управлением маршрутизацией может включать определение линий или подсетей, которые по определенным критериям рассматриваются как безопасные или доверенные.

8.4.9 *Управление заверением*

Управление заверением может включать:

a) распределение информации о нотариусах;

b) использование протокола между нотариусом и взаимодействующими объектами; и

c) взаимодействие с нотариусами.

ПРИЛОЖЕНИЕ A

Базовая информация о безопасности в ВОС

(Данное приложение не является неотъемлемой частью настоящей Рекомендации.)

A.1 *Базовая информация*

В данном Приложении содержится:

a) информация о безопасности ВОС, которая представлена в качестве введения в настоящую Рекомендацию; и

b) базовая информация о влиянии на архитектуру различных средств и требований безопасности.

Безопасность в среде ВОС – это лишь один аспект безопасности обработки данных/передачи данных. Для обеспечения эффективности защитных мер, используемых в среде ВОС, требуются поддерживающие средства, которые находятся за пределами ВОС. Например, информация, проходящая между системами, может быть зашифрована, но если в отношении доступа к самим системам не применяются физические ограничения для безопасности, шифрование может оказаться бесполезным. Кроме того, ВОС рассматривается только в аспекте присоединения систем. Для того чтобы меры безопасности ВОС были эффективными, они должны применяться в сочетании с мерами, которые не входят в сферу ВОС.

A.2 *Требование безопасности*

A.2.1 *Что означает безопасность?*

Термин "безопасность" используется в смысле минимизации уязвимости активов и ресурсов. Активом является что-либо, представляющее ценность. Уязвимость – это любое слабое место, которое возможно использовать для нарушения системы или содержащейся в ней информации. Потенциальным нарушением безопасности является угроза.

A.2.2 *Актуальность безопасности в открытых системах*

МККТТ определил необходимость в разработке серии Рекомендаций для укрепления безопасности архитектуры взаимосвязи открытых систем. Это было обусловлено следующим:

a) возрастает зависимость общества от компьютеров, доступ к которым или связь с которыми осуществляется в рамках передачи данных и которые требуют защиты от различных угроз;

b) появление в ряде стран законодательства в области "защиты данных", которое обязывает поставщиков подтверждать целостность системы и неприкосновенность личных данных; и

c) желание различных организаций использовать рекомендации ВОС, усовершенствованные при необходимости в отношении существующих и будущих защищенных систем.

А.2.3 *Что следует защищать?*

В целом защита может потребоваться для:

a) информации и данных (включая программное обеспечение и пассивные данные, относящиеся к мерам безопасности, такие как пароли);

b) услуг связи и обработки данных; и

c) оборудования и средств.

А.2.4 *Угрозы*

К угрозам для систем передачи данных относятся:

a) разрушение информации и/или других ресурсов;

b) повреждение или изменение информации;

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

d) раскрытие информации; и

e) прерывание предоставления услуги.

Угрозы можно разделить на случайные и намеренные, а также на активные и пассивные.

А.2.4.1 *Случайные угрозы*

Случайные угрозы – это угрозы непреднамеренного характера. К существующим на практике примерам таких угроз относятся нарушение работы системы, грубые эксплуатационные ошибки и ошибки в программном обеспечении.

А.2.4.2 *Намеренные угрозы*

Диапазон намеренных угроз составляют угрозы случайного просмотра с использованием легкодоступных средств мониторинга до атак с применением новейших средств нападения на основе специальных знаний системы. Намеренная угроза, если она реализована, может считаться "атакой".

А.2.4.3 *Пассивные угрозы*

Пассивные угрозы – это угрозы, реализация которых не приводит к какому-либо изменению какой-либо информации, содержащейся в система(ах), и не вызывает изменения функционирования или состояния системы. Одним из вариантов реализации пассивной угрозы является использование пассивного подслушивающего оборудования для наблюдения за информацией, передаваемой по линии связи.

А.2.4.4 *Активные угрозы*

Активные угрозы системе включают изменение информации, содержащейся в системе, или изменение состояния или функционирования системы. Одним из примеров активной угрозы служит злонамеренное изменение таблиц маршрутизации системы неавторизованным пользователем.

А.2.5 *Некоторые особые типы атак*

Далее приведен краткий обзор атак, представляющих опасность конкретно для среды обработки данных/передачи данных. В следующих ниже разделах появляются термины "авторизованный" и "неавторизованный". Авторизация означает предоставление прав. Это определение обусловливает два аспекта: права – это права на выполнение определенный деятельности (например, доступ к данным), и эти права предоставляются определенному объекту, агенту-человеку или процессу. Таким образом, авторизованное поведение – это выполнение той деятельности, права на которую были предоставлены (и не отозваны). Более подробно о понятии "авторизация" см. в п. А.3.3.1.

A.2.5.1 *Нелегальное проникновение*

Нелегальное проникновение – это стремление объекта выдать себя за другой объект. Нелегальное проникновение используется, как правило, с другими формами активных атак, в особенности с повторной передачей и изменением сообщений. Например, последовательности аутентификации могут перехватываться и передаваться повторно после осуществления действительной последовательности аутентификации. Имеющий ряд привилегий авторизованный объект может использовать нелегальное проникновение для получения дополнительных привилегий, выдавая себя за объект, имеющий эти привилегии.

A.2.5.2 *Повторная передача*

Повторная передача происходит при повторении сообщения или части сообщения для получения неавторизованного результата. Например, действительное сообщение, содержащее аутентификационную информацию, может быть повторно передано другим объектом, для того чтобы аутентифицировать самого себя (в качестве объекта, каковым он не является).

A.2.5.3 *Изменение сообщений*

Изменение сообщения происходит при необнаруженном изменении содержимого передачи данных и получении неавторизованного результата, например сообщение "Разрешить «Джону Смиту» чтение конфиденциального файла «Счета»" изменяется на "Разрешить «Фреду Брауну» чтение конфиденциального файла «Счета»".

A.2.5.4 *Отказ в обслуживании*

Отказ в обслуживании происходит при невыполнении объектом своих надлежащих функций или в случае действий объекта, препятствующих другим объектам выполнять свои надлежащие функции. Эта атака может иметь общий характер, когда объект подавляет все сообщения, или может существовать конкретная цель, когда объект подавляет все сообщения, направляемые в определенный пункт назначения, например к услуге аудита безопасности. Такая атака может включать подавление трафика, как описано в приведенном выше примере, или может создавать дополнительный трафик. Также возможна генерация сообщений, предназначенных для нарушения функционирования сети, в частности если сеть содержит объекты ретрансляции, принимающие решения о маршрутизации на основе отчетов о состоянии, получаемых от других объектов ретрансляции.

A.2.5.5 *Внутренние атаки*

Внутренние атаки происходят при непредусмотренном или неавторизованном поведении законных пользователей системы. Большинство известных компьютерных преступлений связаны с внутренними атаками, которые нарушают безопасность системы. Против внутренних атак могут применяться следующие защитные методы:

a) тщательная проверка персонала;

b) тщательный контроль аппаратной части, программного обеспечения, стратегии безопасности и конфигурации системы, с тем чтобы обеспечить определенную степень гарантии их надлежащего функционирования (доверенная функциональность); и

c) журналы аудита для повышения вероятности обнаружения таких атак.

A.2.5.6 *Внешние атаки*

При внешних атаках могут использоваться нижеперечисленные методы:

a) прослушивание линии (активное и пассивное);

b) перехват передачи;

c) нелегальное проникновение под видом авторизованных пользователей системы или компонентов системы; и

d) обход аутентификации или механизмов управления доступом.

A.2.5.7 *Путь обхода системы защиты*

Если объект системы изменен таким образом, чтобы позволить злоумышленнику добиться неавторизованного воздействия по команде или при предопределенном событии или последовательности событий, то результат называется "путь обхода системы защиты". Например, валидация пароля может быть изменена таким образом, что наряду со штатным результатом будет также подтверждена подлинность пароля злоумышленника.

A.2.5.8 "*Троянский конь"*

При введении в систему "троянский конь" наряду со своими авторизованными функциями обладает неавторизованной функцией. Примером "троянского коня" является ретрансляция, которая копирует также сообщения в неавторизованный канал.

A.2.6 *Оценка угроз, рисков и мер противодействия*

Функции безопасности, как правило, увеличивают стоимость системы и могут сделать ее использование более сложным. Таким образом, перед началом проектирования защищенной системы следует определить конкретные угрозы, от которых требуется защита. Этот процесс называется оценкой угроз. Система уязвима во многих направлениях, но использоваться могут только некоторые из них, потому что злоумышленник не имеет соответствующей возможности или потому что результат не оправдывает усилий и риска обнаружения. Конкретные вопросы оценки угроз не входят в сферу настоящего Приложения, но в широком значении оценка включает следующие элементы:

a) выявление уязвимостей системы;

b) анализ вероятности угроз, направленных на использование этих уязвимостей;

c) оценка последствий каждой угрозы в случае ее успешной реализации;

d) оценка затрат в связи с каждой атакой;

e) оценка стоимости потенциальных мер противодействия; и

f) выбор обоснованных механизмов безопасности (возможно, путем анализа рентабельности).

Рентабельной альтернативой техническим мерам безопасности могут быть меры нетехнического характера, например страховое обеспечение. Идеальная техническая безопасность, также как и идеальная физическая безопасность, невозможна. Следовательно, задача должна заключаться в том, чтобы сделать стоимость атаки достаточно высокой для снижения рисков до приемлемых уровней.

A.3 *Стратегия безопасности*

В данном разделе рассматривается стратегия безопасности – необходимость адекватного определения стратегии безопасности, ее роль, используемые в рамках этой стратегии подходы, и уточнения для применения в конкретных ситуациях. Эти понятия применяются к системам связи.

A.3.1 *Необходимость и задачи стратегии безопасности*

Сфера безопасности во всей полноте и сложна и обширна. Любой в разумных пределах полный анализ повлечет устрашающее количество деталей. Удовлетворительная стратегия безопасности должна быть направлена на такие аспекты ситуации, чтобы наивысший уровень полномочий рассматривался как заслуживающий внимания. По существу, стратегия безопасности определяет, в общих понятиях, что именно разрешено и не разрешено в области безопасности при штатной эксплуатации рассматриваемой системы. Как правило, стратегия не является конкретной, она определяет, что именно имеет первостепенное значение, не указывая конкретно на то, как достичь желаемых результатов. Стратегия устанавливает верхний уровень спецификации безопасности.

A.3.2 *Последствия определения стратегии: процесс уточнения*

Столь общий характер стратегии делает непонятным на начальном этапе то, каким образом обеспечить соответствие стратегии конкретной ситуации. Зачастую оптимальным способом достижения этого является последовательное уточнение стратегии при включении большего объема подробной информации о приложении на каждом этапе. Для того чтобы узнать, какой должна быть эта подробная информация, необходимо детальное исследование области применения в свете общей стратегии. Это исследование должно определить проблемы, возникающие в результате применения условий стратегии к данному приложению. Процесс уточнения приведет к изменению изложения стратегии в общих терминах в изложение стратегии в очень точных терминах, непосредственно взятых из приложения. Изменение изложения стратегии упрощает определение детальной реализации.

A.3.3 *Компоненты стратегий безопасности*

Существующие стратегии безопасности характеризуются двумя аспектами. Оба зависят от понятия авторизованного поведения.

A.3.3.1 *Авторизация*

Угрозы, которые рассматривались выше, все включают понятие авторизованного и неавторизованного поведения. Декларация содержания авторизации включена в стратегию безопасности. Общая стратегия безопасности может включать заявление "лицо, не авторизованное надлежащим образом, не может ни получать информацию, ни иметь к ней доступ или интерпретировать эту информацию, ни использовать какой-либо ресурс". Характер авторизации – это то, что различает стратегии безопасности. Стратегии можно разделить на две отдельные группы по характеру применяемой авторизации: стратегии на основе правил и стратегии на основе идентичности. В первой используются правила, основанные на небольшом числе общих атрибутов или классов критичности, которые могут быть реализованы универсальным образом. Вторая включает критерий авторизации на основе конкретных индивидуализированных атрибутов. Некоторые атрибуты предполагаются как имеющие постоянную ассоциацию с объектом, к которому они применяются, другие могут быть правами владения (например, возможности), которые могут передаваться другим объектам. Также можно различать административно вводимые и динамично выбираемые услуги авторизации. Стратегия безопасности определяет те элементы безопасности системы, которые всегда применяются и остаются в силе (например, компоненты стратегии безопасности, базирующиеся на правилах и базирующиеся на идентичности, если таковые имеются), и те, которые пользователь может выбрать для использования и которые представляются ему подходящими.

A.3.3.2 *Стратегия безопасности на основе идентичности*

Базирующийся на идентичности аспект стратегий безопасности частично соответствует концепции безопасности, называемой "необходимо знать". Цель такой стратегии заключается в фильтровании доступа к данным и ресурсам. Существуют два основных способа реализации стратегий на основе идентичности – в зависимости от того, хранится ли информации о правах доступа лицом, осуществляющим доступ, или эта информация является частью данных, к которым осуществляется доступ. Первый вариант поясняется идеей привилегий или возможностей, которые даются пользователям и используются процессами, действующими от их имени. Примером второго случая являются списки управления доступом (ACL). В обоих случаях размер элемента данных (от полного файла до элемента данных), который может иметь имя и возможности или который несет собственный ACL, может сильно различаться.

A.3.3.3 *Стратегия безопасности на основе правил*

Авторизация в стратегии на основе правил размещается, как правило, в критичности. В системе безопасности данные и/или ресурсы должны маркироваться метками безопасности. Процессы, действующие от имени пользователей-людей, могут получать метку безопасности в соответствии со своими создателями.

A.3.4 *Стратегия безопасности, связь и метки*

Концепция меток важна в среде передачи данных. Метки, переносящие атрибуты, выполняют большое число функций. Существуют элементы данных, которые перемещаются в процессе связи; существуют процессы и объекты, которые инициируют связь и которые отвечают; и существуют каналы и другие ресурсы самой системы, которые используются в процессе связи. Все они могут быть помечены тем или иным образом в соответствии со своими атрибутами. Стратегии безопасности должны указывать, как атрибуты каждого могут использоваться для обеспечения предусмотренной безопасности. Для установления соответствующей важности в аспекте безопасности каждого помеченного атрибута может потребоваться согласование. Если метки безопасности прикрепляются и к процессам доступа и к данным, к которым осуществляется доступ, в соответствующих метках должна содержаться дополнительная информация для применения управления доступом на основе идентичности. Если стратегия безопасности базируется на идентичности пользователя, осуществляющего доступ к данным, непосредственно или через процесс, то метки безопасности должны

включать информацию об идентичности пользователя. Функции конкретных меток должны быть определены в стратегии безопасности в базе информации управления безопасностью (SMIB) и/или согласованы с оконечными системами, в зависимости от требований. Метка может сопровождаться атрибутами, которые квалифицируют ее критичность, определяют предостережения в отношении обработки и распределения, вводят ограничения по времени и расположению и в которых точно определены конкретные для оконечной системы требования.

A.3.4.1 *Метки процессов*

В рамках аутентификации полная идентификация тех процессов или объектов, которые инициируют экземпляр связи и отвечают на этот экземпляр связи, а также всех соответствующих атрибутов имеет, как правило, принципиальное значение. Следовательно, SMIB будет содержать достаточную информацию об тех атрибутах, которые важны для любой административно вводимой стратегии.

A.3.4.2 *Метки элементов данных*

Поскольку элементы данных перемещаются в течение существования экземпляров связи, каждый будет жестко связан со своей меткой. (Такое связывание имеет существенное значение, и в некоторых стратегиях на основе правил предусмотрено требование о том, чтобы метка стала особой частью элемента данных до их представления приложению.) Методы сохранения целостности элемента данных будут также поддерживать точность и увязку метки. Эти атрибуты могут использоваться функциями управления маршрутизацией на канальном уровне базовой эталонной модели ВОС.

A.4 *Механизмы безопасности*

Стратегия безопасности может быть реализована с использованием различных механизмов по отдельности или в сочетании, в зависимости от целей стратегии и используемых механизмов. В целом механизм может относиться к одному из трех (пересекающихся) классов:

a) предупреждение;

b) обнаружение; и

c) восстановление.

Ниже представлены механизмы безопасности, соответствующие среде передачи данных.

A.4.1 *Криптографические методы и шифрование*

Криптография лежит в основе многих услуг и механизмов безопасности. Криптографические функции могут использоваться как часть шифрования, дешифрования, целостности данных, аутентификационных обменов, хранения и проверки паролей и т. д., с тем чтобы обеспечивать конфиденциальность, целостность и/или аутентификацию. Шифрование, используемое для обеспечения конфиденциальности, преобразует критические данные (то есть данные, подлежащие защите) в менее критические форматы. При использовании для обеспечения целостности и аутентификации криптографические методы применяются для расчета непринудительных функций.

Первоначально выполняется шифрование открытого текста для создания зашифрованного текста. Результатом дешифрования является либо открытый текст или зашифрованный текст с какой-либо защитой. В вычислительном отношении возможно использование открытого текста для обработки общего характера, так как семантическое содержимое этого текста доступно. За исключением конкретных методов (например, первичное дешифрование или точное совпадение), в вычислительном отношении обработка зашифрованного текста невозможна, поскольку его семантическое содержимое скрыто. Шифрование иногда намеренно является необратимым (например, путем усечения или путем потери данных), если абсолютно нежелательно выведение оригинального открытого текста, например паролей.

Криптографические функции используют криптографические переменные и осуществляют действия с полями, блоками данных и/или потоками блоков данных. Двумя криптографическими переменными являются ключ, который направляет конкретные преобразования, и переменная инициализации, которая требуется в определенных криптографических протоколах для сохранения кажущейся хаотичности зашифрованного текста. Ключ должен, как правило, оставаться конфиденциальным, а криптографическая функция и переменная инициализации могут увеличивать задержку и потребление ширины полосы. Это усложняет "прозрачное" или "прозрачное" и "ложное" криптографическое добавление к существующим системам.

Криптографические переменные могут быть симметричными и асимметричными при шифровании и дешифровании. Используемые в асимметричных алгоритмах ключи математически связаны; один ключ не может быть вычислен на основании другого. Эти алгоритмы иногда называются алгоритмами "открытых ключей", так как один из ключей может быть открытым, а другой – секретным.

Если в вычислительном отношении возможно восстановить открытый текст без знания ключа, зашифрованный текст может быть подвергнут криптографическому анализу. Это может случиться при использовании слабой или поврежденной криптографической функции. Перехваты и анализ трафика могут привести к атакам на криптосистему, включая введение, удаление и изменение сообщений/полей, повторную передачу ранее действительного зашифрованного текста и нелегальное проникновение.

Таким образом, криптографические протоколы разработаны с учетом устойчивости к атакам и также, иногда, к анализу трафика. Специальное средство противодействия анализу трафика – "конфиденциальность потока трафика" – предназначено для сокрытия наличия или отсутствия данных и их характеристик. Если зашифрованный текст ретранслируется, адреса должны быть открытыми в точках ретрансляции и в шлюзах. Если данные зашифровываются только в каждой линии и дешифруются (и, следовательно, становятся уязвимыми) в точках ретрансляции и шлюзах, такая архитектура называется "шифрование по участкам". Если в точках ретрансляции и шлюзах открытыми являются только адреса (и аналогичные данные управления), такая архитектура называется "сквозное шифрование". В аспекте безопасности более предпочтительно сквозное шифрование, но оно существенно сложнее в архитектурном аспекте, особенно если предполагается внутриполосное распределение электронных ключей (функция управления ключами). Для достижения нескольких целей безопасности шифрование по участкам и сквозное шифрование могут быть объединены. Целостность данных зачастую обеспечивается путем расчета криптографического контрольного значения. Контрольное значение может быть выведено за один или несколько шагов и является математической функцией криптографических переменных и данных. Эти контрольные значения связаны с данными, подлежащими защите. Криптографические контрольные значения иногда называют кодами обнаружения манипулирования данными.

Криптографические методы могут обеспечить или содействовать обеспечению защиты от следующих действий:

a) наблюдение и/или изменение потока сообщений;

b) анализ трафика;

c) непризнание участия;

d) подлог;

e) неавторизованное соединение; и

f) изменение сообщений.

A.4.2 *Аспекты управления ключами*

Управление ключами обусловливается использованием криптографических алгоритмов. Управление ключами охватывает создание, распределение криптографических ключей и управление ими. Выбор метода управления ключами основывается на оценке участниками среды, в которой этот метод будет использоваться. В оценке среды рассматриваются такие соображения, как угрозы, от которых следует обеспечить защиту (внутренние и внешние по отношению к организации), используемые технологии, структура архитектуры и местоположение предоставляемых криптографических услуг, а также физическая структура и местоположение поставщиков криптографических услуг.

В отношении управления ключами следует рассматривать следующие аспекты:

a) использование "времени жизни" основано на времени, использовании и других критериях для каждого определенного ключа в явной и неявной форме;

b) надлежащая идентификация ключей в соответствии с их функцией, так чтобы их использование могло резервироваться только для их функции, например ключи, предназначенные в целях использования для услуги конфиденциальности, не должны использоваться для услуги целостности, и наоборот; и

c) факторы, не связанные с ВОС, такие как физическое распределение ключей и архивирование ключей.

В отношении управления ключами для симметричных алгоритмов ключей следует рассматривать следующие аспекты:

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

b) использование иерархии ключей. Должны предусматриваться различные ситуации, такие как:

   1) "горизонтальная" иерархия с использование только ключей шифрования данных, явно или неявно выбранных из набора по идентичности или индексу ключа;

   2) многоуровневые иерархии ключей; и

   3) никогда не следует использовать ключи шифрования ключей для защиты данных, а ключи шифрования данных никогда не следует использовать для защиты ключей шифрования ключей;

c) распределение ответственности, так чтобы ни одно лицо не имело полной копии важного ключа.

В отношении управления ключами для симметричных алгоритмов ключей следует рассматривать следующие аспекты:

a) использование услуги конфиденциальности в протоколе управления ключами для переноса секретных ключей; и

b) использование услуги целостности или услуги предотвращения отказа от авторства с подтверждением источника в протоколе управления ключами для переноса открытых ключей. Эти услуги могут обеспечиваться путем использования симметричных и/или асимметричных криптографических алгоритмов.

A.4.3 *Механизмы цифровой подписи*

Термин "цифровая подпись" используется для указания конкретного метода, который может использоваться для обеспечения услуг безопасности, таких как предотвращение отказа от авторства и аутентификация. Механизмы цифровой подписи требуют использования асимметричных криптографических алгоритмов. Важной характеристикой механизма цифровой подписи является невозможность создания подписанных данных без использования личного ключа. Это означает, что:

a) подписанный блок данных не может быть создан никаким иным лицом, кроме владельца личного ключа; и

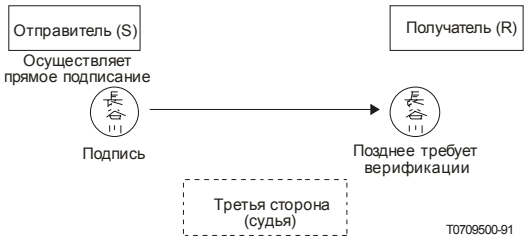
b) получатель не может создать подписанный блок данных.

Следовательно, используя только общедоступную информацию, возможно однозначно определить лицо, подписавшее блок данных, как владельца личного ключа. В случае последующего конфликта между участниками можно будет доказать идентичность лица, подписавшего блок данных, надежной третьей стороне, призванной сделать заключение об аутентичности подписанного блока данных. Такой тип цифровой подписи называется схемой прямой подписи (см. рис. A-1/X.800). В других случаях может потребоваться дополнительное свойство c):

c) отправитель не может отрицать отправления подписанного блока данных.

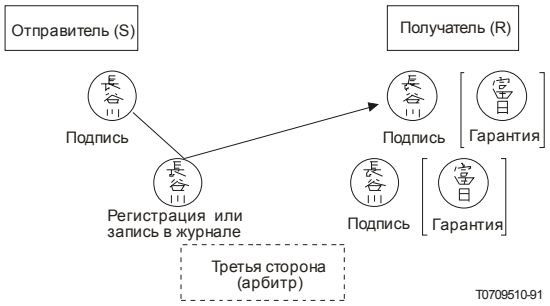
В этом случае надежная третья сторона (арбитр) предъявляет получателю доказательства источника и целостности информации. Этот тип цифровой подписи иногда называется схемой арбитражной подписи (см. рис. A-2/X.800).

Примечание. – Отправитель может потребовать, чтобы получатель не мог позднее отрицать получение подписанного блока данных. Это может быть выполнено с помощью услуги предотвращения отказа от авторства с подтверждением доставки с использованием соответствующей комбинации механизмов цифровой подписи, целостности данных и заверения.



Примечание. – Верифицирует подпись в случае возникновения конфликта между участниками (S или R может быть лжесвидетелем)

РИСУНОК A-1/X.800
Схема прямой подписи



Примечание. – Третья сторона осуществляет аутентификацию источника и выдает гарантию (то есть положительный результат) получателю. Информация, необходимая для доказательства источника и целостности данных, записывается в журнал третьей стороной. В этом случае S не сможет позднее успешно отрицать отправку подписанного блока данных.

РИСУНОК A-2/X.800
Схема арбитражной подписи

A.4.4 *Механизмы управления доступом*

Механизмы управления доступом – это механизмы, которые используются для осуществления стратегии ограничения доступа к ресурсу только авторизованными пользователями. Методы включают использование списков или матриц управления доступом (которые, как правило, содержат идентичности управляемых элементов и авторизованных пользователей, например лиц или процессов), паролей и возможностей, меток и жетонов, владение которыми может использоваться для указания прав доступа. Если используются возможности, они должны быть непринудительными и должны переноситься надежным образом.

A.4.5 *Механизмы обеспечения целостности данных*

Механизмы обеспечения целостности данных бывают двух типов: используемые для защиты целостности одного блока данных и используемые для защиты и целостности одного блока данных и последовательности целого потока блока данных в данном соединении.

A.4.5.1 *Обнаружение изменения потока сообщений*

Для обнаружения изменения потока сообщений могут также использоваться методы обнаружения искажения, связанные обычно с обнаружением битовых ошибок, вносимых линиями и сетями связи. Однако, если не предусмотрена защита заголовков и трейлеров протокола с помощью механизмов целостности, информированный злоумышленник может успешно обойти эти проверки. Надежное обнаружение изменения потока сообщений может быть обеспечено, таким образом, только путем использования методов обнаружения искажения в сочетании с информацией последовательности. Это не предотвратит изменение потока сообщений, но обеспечит извещение об атаках.

A.4.6 *Механизмы аутентификационного обмена*

A.4.6.1 *Выбор механизма*

Существует большое число вариантов и сочетаний механизмов аутентификационного обмена, соответствующих различным условиям. Ниже приведен ряд примеров.

a) Если одноранговые объекты и средства связи являются доверенными, идентификация одноранговых объектов может быть подтверждена паролем. Пароль защищает от ошибки, но не является средством защиты от злого умысла (особенно от повторной передачи). Может выполняться взаимная аутентификация с использованием разных паролей в каждом направлении.

b) Если объект доверяет своим одноранговым объектам, но не доверяет средству связи, защита от активных атак может быть обеспечена сочетанием паролей и шифрования или с помощью криптографических средств. Защита от атак с целью повторной передачи требует двухступенчатого установления соединения (с параметрами защиты) или установки меток времени (с использованием доверенных часов). Взаимная аутентификация с защитой от повторной передачи может обеспечиваться с помощью трехступенчатого установления соединения.

c) Если объекты не доверяют (или понимают, что могут не доверять в будущем) своим одноранговым объектам или средствам связи, могут использоваться услуги предотвращения отказа от авторства. Услуга предотвращения отказа от авторства может выполняться с использованием механизмов цифровой подписи и/или заверения. Эти механизмы могут использоваться с механизмами, описанными в п. b) выше.

A.4.7 *Механизмы подстановки трафика*

Ограниченную защиту от анализа трафика может обеспечить генерирование ложного трафика и подстановка блоков протокольных данных постоянной длины. Для того чтобы эта мера была успешной, уровень ложного трафика должен приближаться к наивысшему ожидаемому уровню реального трафика. Наряду с этим содержимое блоков протокольных данных должно быть зашифровано или замаскировано таким образом, чтобы не допустить возможности идентификации ложного трафика и его отделения от реального трафика.

A.4.8 *Механизм управления маршрутизацией*

Для обеспечения переноса данных только по тем маршрутам, которые являются физически безопасными, или для обеспечения переноса критической информации только по тем маршрутам, которые имеют соответствующий уровень защиты, может использоваться спецификация предостережений маршрутизации для передачи данных (включая спецификацию полного маршрута).

A.4.9 *Механизм заверения*

Механизм заверения основан на концепции доверенной третьей стороны (нотариус) для гарантирования определенных свойств информации, которой обмениваются два объекта, таких как отправитель, целостность информации или время отправки и получения информации.

A.4.10 *Физическая и личная безопасность*

Для обеспечения полной защиты всегда необходимы меры физической безопасности. Физическая безопасность требует значительных затрат, и необходимость в ней, как правило, стремятся уменьшить, применяя другие (менее затратные) методы. Аспекты физической и личной безопасности не входят в сферу применения ВОС, однако во всех системах в конце концов применяется какая-либо форма физической безопасности и предполагается доверие к персоналу, эксплуатирующему эту систему. Для обеспечения надлежащей эксплуатации и определения ответственности персонала следует определять эксплуатационные процедуры.

A.4.11 *Доверенное аппаратное оборудование/программное обеспечение*

Методы, используемые для формирования уверенности в надлежащем функционировании объекта, включают формальные методы доказательства, верификацию и валидацию, обнаружение и регистрацию известных предпринятых попыток атак и создание объекта доверенным персоналом в безопасной среде. Также необходимо принимать меры предосторожности, для того чтобы не допустить случайного или намеренного изменения объекта в целях нарушения безопасности в течение его эксплуатационного срока существования, например в течение технического обслуживания или обновления. Для поддержания уровня безопасности некоторые объекты в системе для корректного функционирования также должны быть доверенными. Методы, используемые для установления доверия, не входят в сферу применения ВОС.

ПРИЛОЖЕНИЕ B

Обоснование представленного в разделе 7 размещения услуг и механизмов

(Данное приложение не является неотъемлемой частью настоящей Рекомендации.)

B.1 *Общее*

В данном Приложении приведены некоторые обоснования обеспечения конкретных услуг безопасности на разных уровнях, как указано в разделе 7. Этот процесс выбора обусловлен принципами разделения безопасности по уровням, приведенными в п. 6.1.1 настоящего стандарта.

Конкретная услуга безопасности обеспечивается несколькими уровнями, если воздействие на общий уровень безопасности связи может рассматриваться как неодинаковый (например, конфиденциальность в режиме установления соединения на уровнях 1 и 4). Вместе с тем, рассматривая существующие функциональные возможности передачи данных ВОС (например, процедуры с несколькими линиями, функция мультиплексирования, различные способы усиления услуги в режиме без установления соединения до режима с установлением соединения), а также в целях обеспечения возможности функционирования этих механизмов передачи, может потребоваться конкретная услуга, предоставляемая на другом уровне, хотя последствия для уровня безопасности не могут рассматриваться как неодинаковые.

B.2 *Аутентификация однорангового объекта*

- *Уровни 1 и 2*: Нет, аутентификация однорангового объекта не представляется целесообразной на этих уровнях.
- *Уровень 3*: Да, в отдельных подсетях и для маршрутизации и/или в интерсети.
- *Уровень 4*: Да, аутентификация оконечной системы к оконечной системе на уровне 4 может служить для взаимной аутентификации двух и более объектов сеанса до начала соединения и в течение существования этого соединения.
- *Уровень 5*: Нет, отсутствуют преимущества обеспечения этой услуги на уровне 4 и/или более высоких уровнях.
- *Уровень 6*: Нет, но механизмы шифрования могут поддерживать эту услугу на прикладном уровне.
- *Уровень 7*: Да, аутентификация однорангового объекта должна обеспечиваться прикладным уровнем.

B.3 *Аутентификация источника данных*

– *Уровни 1 и 2*: Нет, аутентификация источника данных не представляется целесообразной на этих уровнях.

– *Уровни 3 и 4*: Может обеспечиваться сквозная аутентификация источника данных в функции ретрансляции или маршрутизации уровня 3 и/или на уровне 4 следующим образом:

  a) выполнение аутентификации однорангового объекта во время установления соединения в совокупности с непрерывной аутентификацией на основе шифрования в течение срока существования соединения обеспечивает де-факто услугу аутентификации источника данных; и

  b) даже если a) не выполняется, аутентификация источника данных на основе шифрования может выполняться с весьма незначительной дополнительной служебной нагрузкой на механизмы обеспечения целостности данных, уже размещенные на этих уровнях.

– *Уровень 5*: Нет, отсутствуют преимущества обеспечения этой услуги на уровне 4 или на уровне 7.

– *Уровень 6*: Нет, но механизмы шифрования могут поддерживать эту услугу на прикладном уровне.

– *Уровень 7*: Да, вероятно, в сочетании с механизмами уровня представления.

B.4 *Управление доступом*

– *Уровни 1 и 2*: Механизмы управления доступом не могут обеспечиваться на уровне 1 или уровне 2 в системе, соответствующей полным протоколам ВОС, поскольку отсутствуют оконечные средства, доступные для такого механизма.

– *Уровень 3*: Механизмы управления доступом могут быть включены в функцию доступа подсети посредством требований к конкретной подсети. При выполнении функций ретрансляции и маршрутизации механизмы доступа на сетевом уровне могут использоваться для управления доступом к подсетям объектами ретрансляции и для управления доступом к оконечным системам. Очевидно, что гранулярность доступа является весьма грубой, обеспечивающей разделение только между объектами сетевого уровня.

  Установление сетевого соединения зачастую приводит к начислению платы администрацией подсети. Снизить затраты можно путем управления доступом и выбора начисления платы на вызываемого абонента или других определяемых сетью параметров.

– *Уровень 4*: Да, механизмы управления доступом могут использоваться на основе сквозного транспортного соединения.

– *Уровень 5*: Нет, отсутствуют преимущества обеспечения этой услуги на уровне 4 и/или уровне 7.

– *Уровень 6*: Нет, это нецелесообразно на уровне 6.

– *Уровень 7*: Да, прикладные протоколы и/или прикладные процессы могут обеспечивать средства управления доступом, ориентированного на приложение.

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

– *Уровень 1*: Да, должна обеспечиваться, поскольку электрическое включение открытых пар устройств преобразования может привести к полной конфиденциальности в физическом соединении.

– *Уровень 2*: Да, но это не обеспечивает дополнительных преимуществ безопасности по сравнению с обеспечением конфиденциальности на уровне 1 или уровне 3.

– *Уровень 3*: Да, для функции доступа к подсети в отдельных подсетях и функций ретрансляции и маршрутизации в интерсети.

– *Уровень 4*: Да, поскольку отдельное транспортное соединение предоставляет сквозной транспортный механизм и может обеспечить изолирование соединений сеанса.

– *Уровень 5*: Нет, поскольку это не обеспечивает дополнительных преимуществ безопасности по сравнению с обеспечением конфиденциальности на уровнях 3, 4 и 7. Не представляется целесообразным обеспечивать эту услугу на данном уровне.

– *Уровень 6*: Да, поскольку механизмы шифрования обеспечивают чисто синтаксические преобразования.

– *Уровень 7*: Да, в сочетании с механизмами нижних уровней.

B.6 *Конфиденциальность всех (N)-данных-пользователя в одном (N)-SDU в режиме без установления соединения*

Обоснование, аналогичное обоснованию в отношении конфиденциальности всех (N)-данных-пользователя, за исключением уровня 1, на котором отсутствует услуга в режиме без установления соединения.

B.7 *Избирательная конфиденциальность полей в (N)-данных-пользователя SDU*

Эта услуга конфиденциальности обеспечивается шифрованием на уровне представления и активируется на прикладном уровне в соответствии с семантикой данных.

B.8 *Конфиденциальность потока трафика*

Полная конфиденциальность потока трафика может достигаться только на уровне 1. Это возможно путем физического включения пары устройств шифрования в физический тракт передачи. Предполагается, что тракт передачи будет трактом двунаправленной одновременной и синхронной передачи, так чтобы включение устройств делало все передачи (и даже их наличие) в физическом носителе нераспознаваемыми.

Выше физического уровня полная безопасность потока трафика невозможна. Некоторые ее эффекты могут быть частично созданы путем использования услуги полной конфиденциальности SDU на одном уровне и включения ложного трафика на более высоком уровне. Такой механизм связан с большими затратами и потенциально потребляет существенный объем несущей и коммутационной емкости.

Если конфиденциальность потока трафика обеспечивается на уровне 3, будет использоваться подстановка трафика и/или управление маршрутизацией. Управление маршрутизацией может обеспечивать ограниченную конфиденциальность потока трафика путем направления сообщений в обход небезопасных линий или подсетей. Однако введение подстановки трафика в уровень 3 позволит более эффективно использовать сеть, например не допуская нецелесообразной подстановки и перегрузки сети.

Ограниченная конфиденциальность потока трафика может обеспечиваться на прикладном уровне путем генерации ложного трафика в сочетании с конфиденциальностью, с тем чтобы предотвращать идентификацию ложного трафика.

B.9 *Целостность всех (N)-данных-пользователя в (N)-соединении (с восстановлением после ошибок)*

– *Уровни 1 и 2*: На уровнях 1 и 2 обеспечение этой услуги невозможно. На уровне 1 отсутствуют механизмы обнаружения и восстановления, а механизм уровня 2 работает только в режиме связи пункта с пунктом, а не в режиме сквозной связи и, следовательно, не представляется подходящим для обеспечения этой услуги.

– *Уровень 3*: Нет, поскольку восстановление после ошибки не является универсально доступным.

– *Уровень 4*: Да, поскольку обеспечивается действительно сквозное транспортное соединение.

– *Уровень 5*: Нет, поскольку восстановление после ошибки не является функцией уровня 5.

– *Уровень 6*: Нет, но механизмы шифрования могут поддерживать эту услугу на прикладном уровне.

– *Уровень 7*: Да, в сочетании с механизмами на уровне представления.

B.10 *Целостность всех (N)-данных-пользователя в (N)-соединении (без восстановления после ошибки)*

– *Уровни 1 и 2*: На уровнях 1 и 2 обеспечение этой услуги невозможно. На уровне 1 отсутствуют механизмы обнаружения и восстановления, а механизм уровня 2 работает только в режиме связи пункта с пунктом, а не в режиме сквозной связи и, следовательно, не представляется подходящим для обеспечения этой услуги.

– *Уровень 3*: Да, для функции доступа к подсети в отдельных подсетях и для функций маршрутизации и ретрансляции в интерсети.

– *Уровень 4*: Да, для тех случаев использования, когда допустимо прекращение связи после обнаружения активной атаки.

– *Уровень 5*: Нет, поскольку это не обеспечивает дополнительных преимуществ безопасности по сравнению с обеспечением конфиденциальности на уровнях 3, 4 или 7.

– *Уровень 6*: Нет, но механизмы шифрования могут поддерживать эту услугу на прикладном уровне.

– *Уровень 7*: Да, в сочетании с механизмами на уровне представления.

B.11 *Селективная целостность полей в (N)-данных-пользователя (N)-SDU, передаваемого по (N)-соединению (без восстановления)*

Селективная целостность полей может обеспечиваться механизмами шифрования на уровне представления в сочетании с механизмами вызова и проверки на прикладном уровне.

B.12 *Целостность всех (N)-данных-пользователя в одном (N)-SDU в режиме без установления соединения*

В целях сокращения дублирования функций целостность передачи в режиме без установления соединения должна обеспечиваться только теми же уровнями, которые обеспечивают целостность без восстановления, то есть сетевым, транспортным и прикладным уровнями. Эти механизмы целостности могут обеспечивать весьма ограниченную эффективность, и это следует понимать.

B.13 *Селективная целостность полей в одном (N)-SDU в режиме без установления соединения*

Селективная целостность полей может обеспечиваться механизмами шифрования на уровне представления в сочетании с механизмами вызова и проверки на прикладном уровне.

B.14 *Предотвращение отказа от авторства*

Услуги "предотвращения отказа от авторства" с подтверждением источника и доставки могут обеспечиваться механизмом заверения, который будет участвовать в ретрансляции на уровне 7.

Использование механизмов цифровой подписи для предотвращения отказа от авторства требует тесного взаимодействия уровней 6 и 7.

ПРИЛОЖЕНИЕ C

Выбор местоположения шифрования для приложений

(Данное приложение не является неотъемлемой частью настоящей Рекомендации.)

C.1 Для большинства приложений шифрование более чем на одном уровне не потребуется. Выбор уровня зависит от принятого решения по основным вопросам, перечисленным ниже.

1) Если требуется полная конфиденциальность потока трафика, выбирается шифрование или безопасность передачи (например, подходящие методы распределенного спектра). Все требования конфиденциальности могут быть удовлетворены с помощью соответствующей физической безопасности и доверенной маршрутизации и аналогичной функциональности на уровне ретрансляции.

2) Если требуется высокая гранулярность защиты (то есть потенциально отдельный ключ для каждой ассоциации приложений) и предотвращение отказа от авторства или селективная защита полей, то выбирается шифрование на уровне представления. Большое значение может иметь селективная защита полей, так как алгоритмы шифрования потребляют большой объем мощности обработки. Шифрование на уровне представления может обеспечить целостность без восстановления, предотвращение отказа от авторства и полную конфиденциальность.

3) Если желательна массовая защита всей связи между оконечной системой и оконечной системой и/или внешнее устройство шифрования (например, для введения физической защиты от неисправных программных средств), то выбирается шифрование на сетевом уровне. Это может обеспечить конфиденциальность и целостность без восстановления.

   Примечание. – Притом что на сетевом уровне восстановление не обеспечивается, для восстановления после обнаружения атак сетевым уровнем могут использоваться обычные механизмы восстановления транспортного уровня.

4) Если требуется целостность вместе с высокой гранулярностью защиты, то выбирается шифрование на транспортном уровне. Это может обеспечить конфиденциальность и целостность с восстановлением и без восстановления.

5) Для будущих реализаций шифрование на канальном уровне не рекомендуется.

C.2 Если рассматриваются два и более из этих вопросов, может потребоваться обеспечение шифрования на нескольких уровнях.