



МЕЖДУНАРОДНЫЙ СОЮЗ ЭЛЕКТРОСВЯЗИ

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

X.1121

(04/2004)

СЕРИЯ X: СЕТИ ПЕРЕДАЧИ ДАННЫХ
И ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ

Безопасность электросвязи

**Структура технологий безопасности для
подвижной передачи данных от конца
до конца**

Рекомендация МСЭ-Т X.1121

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ X
СЕТИ ПЕРЕДАЧИ ДАННЫХ И ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ

СЕТИ ПЕРЕДАЧИ ДАННЫХ ОБЩЕГО ПОЛЬЗОВАНИЯ	
Службы и услуги	X.1–X.19
Интерфейсы	X.20–X.49
Передача, сигнализация и коммутация	X.50–X.89
Сетевые аспекты	X.90–X.149
Техническое обслуживание	X.150–X.179
Административные предписания	X.180–X.199
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ	
Модель и обозначение	X.200–X.209
Определения служб	X.210–X.219
Спецификации протоколов с установлением соединений	X.220–X.229
Спецификации протоколов без установления соединений	X.230–X.239
Формы PICS	X.240–X.259
Идентификация протоколов	X.260–X.269
Протоколы обеспечения безопасности	X.270–X.279
Управляемые объекты уровня	X.280–X.289
Испытание на соответствие	X.290–X.299
ВЗАИМОДЕЙСТВИЕ МЕЖДУ СЕТЯМИ	
Общие положения	X.300–X.349
Спутниковые системы передачи данных	X.350–X.369
IP-сети	X.370–X.399
СИСТЕМЫ ОБРАБОТКИ СООБЩЕНИЙ	X.400–X.499
СПРАВОЧНИК	X.500–X.599
ОРГАНИЗАЦИЯ СЕТИ ВОС И СИСТЕМНЫЕ АСПЕКТЫ	
Организация сети	X.600–X.629
Эффективность	X.630–X.639
Качество обслуживания	X.640–X.649
Наименование, адресация и регистрация	X.650–X.679
Абстрактно-синтаксическая нотация 1 (ASN.1)	X.680–X.699
УПРАВЛЕНИЕ В ВОС	
Структура и архитектура управления системами	X.700–X.709
Служба и протокол связи для общего управления	X.710–X.719
Структура управляющей информации	X.720–X.729
Функции общего управления и функции ODMA	X.730–X.799
БЕЗОПАСНОСТЬ	X.800–X.849
ПРИЛОЖЕНИЯ ВОС	
Фиксация, параллельность и восстановление	X.850–X.859
Обработка транзакций	X.860–X.879
Удаленные операции	X.880–X.899
ОТКРЫТАЯ РАСПРЕДЕЛЕННАЯ ОБРАБОТКА	X.900–X.999
БЕЗОПАСНОСТЬ ЭЛЕКТРОСВЯЗИ	X.1000–

Для получения более подробной информации просьба обращаться к перечню Рекомендаций МСЭ-Т.

Рекомендация МСЭ-Т X.1121

Структура технологий безопасности для подвижной передачи данных от конца до конца

Аннотация

В настоящей Рекомендации описываются угрозы безопасности подвижной передачи данных и требования безопасности с точки зрения подвижных пользователей и поставщиков прикладных услуг (ASP). Кроме того, в настоящей Рекомендации показывается, где в моделях подвижной передачи данных от конца до конца появляются технологии безопасности, которые реализуют некоторые функции безопасности.

Источник

Рекомендация МСЭ-Т X.1121 утверждена 29 апреля 2004 года 17-й Исследовательской комиссией МСЭ-Т (2001–2004 гг.) в соответствии с процедурой, изложенной в Рекомендации МСЭ-Т A.8.

ПРЕДИСЛОВИЕ

Международный союз электросвязи (МСЭ) является специализированным учреждением Организации Объединенных Наций в области электросвязи. Сектор стандартизации электросвязи МСЭ (МСЭ-Т) – постоянный орган МСЭ. МСЭ-Т отвечает за изучение технических, эксплуатационных и тарифных вопросов и за выпуск Рекомендаций по ним с целью стандартизации электросвязи на всемирной основе.

Всемирная ассамблея по стандартизации электросвязи (ВАСЭ), которая проводится каждые четыре года, определяет темы для изучения Исследовательскими комиссиями МСЭ-Т, которые, в свою очередь, вырабатывают Рекомендации по этим темам.

Утверждение Рекомендаций МСЭ-Т осуществляется в соответствии с процедурой, изложенной в Резолюции 1 ВАСЭ.

В некоторых областях информационных технологий, которые входят в компетенцию МСЭ-Т, необходимые стандарты разрабатываются на основе сотрудничества с ИСО и МЭК.

ПРИМЕЧАНИЕ

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

Соблюдение положений данной Рекомендации носит добровольный характер. Однако в Рекомендации могут содержаться определенные обязательные положения (например, для обеспечения возможности взаимодействия или применимости), и соответствие данной Рекомендации достигается в случае выполнения всех этих обязательных положений. Для выражения необходимости выполнения требований используется синтаксис долженствования и соответствующие слова (такие, как "должен" и т.п.), а также их отрицательные эквиваленты. Использование этих слов не предполагает, что соблюдение положений данной Рекомендации является обязательным для какой-либо из сторон.

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

МСЭ обращает внимание на то, что практическое применение или реализация этой может включать использование заявленного права интеллектуальной собственности. МСЭ не занимает какую бы то ни было позицию относительно подтверждения, обоснованности или применимости заявленных прав интеллектуальной собственности, независимо от того, отстаиваются ли они членами МСЭ или другими сторонами вне процесса подготовки Рекомендации.

На момент утверждения настоящей Рекомендации МСЭ не получил извещение об интеллектуальной собственности, защищенной патентами, которые могут потребоваться для реализации этой Рекомендации. Однако те, кто будет применять Рекомендацию, должны иметь в виду, что это может не отражать самую последнюю информацию, и поэтому им настоятельно рекомендуется обращаться к патентной базе данных БСЭ.

© ITU 2005

Все права сохранены. Никакая часть данной публикации не может быть воспроизведена с помощью каких-либо средств без письменного разрешения МСЭ.

СОДЕРЖАНИЕ

	Стр.
1 Область применения	1
2 Нормативные ссылки	1
3 Определения	1
3.1 Определения архитектуры безопасности эталонной модели ВОО	1
3.2 Дополнительные определения	2
4 Сокращения	3
5 Обзор	3
6 Модели подвижной передачи данных от конца до конца	3
6.1 Обобщенная модель подвижной передачи данных от конца до конца между подвижным пользователем и поставщиком ASP	3
6.2 Модель подвижной передачи данных от конца до конца между подвижным пользователем и поставщиком ASP со шлюзом	4
7 Характеристики подвижной передачи данных от конца до конца	4
8 Угрозы безопасности в подвижной среде	5
8.1 Общие угрозы безопасности	5
8.2 Угрозы безопасности, ориентированные на подвижную связь	6
8.3 Отношения угроз безопасности к моделям связи от конца до конца	7
9 Требования к безопасности для подвижной передачи данных от конца до конца	8
9.1 Требования к безопасности с точки зрения подвижного пользователя	8
9.2 Требования к безопасности с точки зрения поставщика ASP	11
9.3 Взаимоотношения между требованиями безопасности и угрозами безопасности	14
10 Функции безопасности для удовлетворения требований безопасности подвижной связи	15
11 Технологии безопасности для подвижной передачи данных от конца до конца	18

Рекомендация МСЭ-Т X.1121

Структура технологий безопасности для подвижной передачи данных от конца до конца

1 Область применения

В настоящей Рекомендации представлены требования к безопасности с точки зрения подвижного пользователя и поставщика прикладных услуг на верхнем уровне эталонной модели ВОС для подвижной передачи данных от конца до конца, между подвижным терминалом в подвижной сети и сервером приложений в открытой сети.

В настоящей Рекомендации представлена структура технологий безопасности для подвижной передачи данных от конца до конца.

В настоящей Рекомендации не представлены детали элементов подвижной сети, за исключением доступа к беспроводной сети подвижного терминала, подключенного к открытой сети.

2 Нормативные ссылки

Нижеследующие Рекомендации МСЭ-Т и другие ссылки содержат положения, которые путем ссылки на них в этом тексте образуют положения настоящей Рекомендации. В момент публикации указанные издания были действительны. Все Рекомендации и другие ссылки подвергаются пересмотру; поэтому всем пользователям настоящей Рекомендации следует изыскивать возможность применения самых последних редакций перечисленных ниже Рекомендаций и других ссылок. Список текущих действующих Рекомендаций МСЭ-Т регулярно публикуется. Ссылка в этой Рекомендации на какой-либо документ не придает ему, как отдельному документу, статуса Рекомендации.

- ITU-T Recommendation Q.1701 (1999), *Framework for IMT-2000 networks*.
- ITU-T Recommendation Q.1711 (1999), *Network functional model for IMT-2000*.
- ITU-T Recommendation Q.1761 (2004), *Principles and requirements for convergence of fixed and existing IMT-2000 systems*.
- ITU-T Recommendation X.800 (1991), *Security Architecture for Open Systems Interconnection for CCITT applications*.
- ITU-T Recommendation X.803 (1994) | ISO/IEC 10745:1995, *Information technology – Open Systems Interconnection – Upper layers security model*.
- ITU-T Recommendation X.810 (1995) | ISO/IEC 10181-1:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Overview*.

3 Определения

3.1 Определения архитектуры безопасности эталонной модели ВОС

В Рекомендации МСЭ-Т X.800:

- a) управление доступом;
- b) аутентификация;
- c) информация аутентификации;
- d) обмен данными аутентификации;
- e) авторизация;
- f) готовность;
- g) конфиденциальность;

- h) криптография;
- i) целостность данных;
- j) аутентификация источника данных;
- k) шифрование;
- l) целостность;
- m) ключ;
- n) обмен ключами;
- o) управление ключами;
- p) фиксация авторства;
- q) заверение;
- r) пароль;
- s) секретность.

3.2 Дополнительные определения

В настоящей Рекомендации определяются следующие термины:

3.2.1 анонимность: Способность обеспечивать анонимный доступ к услугам, при которой избегается отслеживание персональной информации о пользователе и о поведении пользователя, такой как местоположение пользователя, частота пользования услугой и т. д.

3.2.2 блуждание с подглядыванием: Угроза безопасности, которая собирает информацию в местах с интенсивной деятельностью путем наблюдения за нажатием клавиш, чтения с экрана подвижного терминала или прослушивания звуков, исходящих от подвижного терминала.

3.2.3 подвижный терминал: Объект, который имеет функцию доступа к беспроводной сети и соединяет подвижную сеть передачи данных с серверами приложений или другими подвижными терминалами.

3.2.4 сеть подвижной связи: Сеть, которая предоставляет мобильным терминалам пункты беспроводного доступа к сети.

3.2.5 подвижный пользователь: Объект (лицо), которое применяет и эксплуатирует подвижный терминал для получения различных услуг от поставщиков прикладных услуг.

3.2.6 прикладная услуга: Услуга типа подвижного банка, подвижной коммерции и т. д.

3.2.7 сервер приложений: Объект, который соединяет открытую сеть передачи данных с подвижными терминалами.

3.2.8 поставщик (провайдер) прикладной услуги (ASP): Объект (лицо или группа лиц), который предоставляет подвижным пользователям прикладную(ые) услугу(и) через сервер приложений.

3.2.9 шлюз безопасности подвижной связи: Объект, который служит ретранслятором данных между подвижным терминалом и сервером приложений, изменяет параметры безопасности или протокол связи между сетью подвижной связи и открытой сетью или, наоборот, может выполнять функции управления стратегией безопасности для подвижной передачи данных от конца до конца.

3.2.10 управление стратегией безопасности: Функция управления или согласования свода правил для предоставления классифицированных услуг безопасности, которые могут быть реализованы в шлюзе безопасности подвижной связи или другом сервере.

4 Сокращения

В настоящей Рекомендации используются следующие сокращения:

ВОС	Взаимодействие открытых систем
КПК	Карманный персональный компьютер
ЛВС	Локальная вычислительная сеть
ПК	Персональный компьютер
ASP	Поставщик прикладной услуги
DoS	Отказ в обслуживании
ИМТ-2000	Международная подвижная электросвязь-2000
PIN	Номер персональной идентификации

5 Обзор

Широко распространены подвижные терминалы с возможностями передачи данных (такие как подвижные телефоны ИМТ-2000, портативные ПК или КПК с радиокартой), а через сеть подвижной связи подвижным терминалам могут быть предоставлены различные прикладные услуги (например, подвижная коммерция). Для приложений е-коммерции необходима и обязательна безопасность.

Существует множество областей, исследования которых ведутся с точки зрения операторов подвижной связи (например, архитектура безопасности в сети подвижной телефонной связи ИМТ-2000). Однако важно проводить исследования также с точки зрения подвижного пользователя и с точки зрения поставщиков ASP.

При исследовании безопасности в подвижной связи, с точки зрения подвижного пользователя или с точки зрения поставщика ASP, одним из наиболее важных вопросов является безопасность подвижной передачи данных от конца до конца между подвижным терминалом и сервером приложений.

Кроме того, для системы подвижной связи, которая соединяет сеть подвижной связи с открытой сетью, необходимы исследования безопасности на верхних уровнях (прикладном, представительском и сеансовом уровнях) эталонной модели ВОС, потому что существуют различные варианты построения сетей подвижной связи (например, сеть подвижной телефонной связи ИМТ-2000, беспроводные ЛВС, Bluetooth) или открытых сетей.

В настоящей Рекомендации описываются угрозы безопасности подвижной передачи данных от конца до конца и требования к безопасности с точки зрения подвижного пользователя и поставщика ASP. Кроме того, в настоящей Рекомендации показывается, где в моделях подвижной передачи данных от конца до конца появляются технологии безопасности, которые реализуют определенные функции безопасности.

6 Модели подвижной передачи данных от конца до конца

Прежде чем приступить к описанию технологий безопасной подвижной связи, следует определить модели подвижной передачи данных от конца до конца. Модели подвижной передачи данных от конца до конца разъясняют взаимоотношения между объектами в моделях и точками, в которых следует применять технологии безопасной подвижной связи.

6.1 Обобщенная модель подвижной передачи данных от конца до конца между подвижным пользователем и поставщиком ASP

Обобщенная модель подвижной передачи данных от конца до конца между подвижным пользователем и поставщиком ASP показана на рисунке 1.

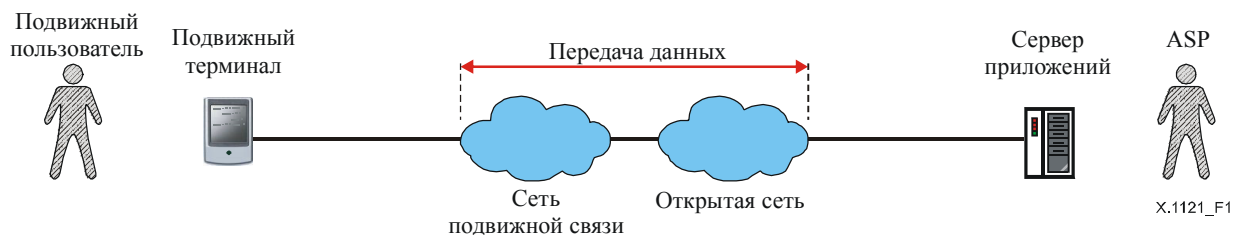


Рисунок 1/X.1121 – Обобщенная модель подвижной передачи данных от конца до конца между подвижным пользователем и поставщиком ASP

В настоящую модель входят шесть объектов: подвижный пользователь, подвижный терминал, сеть подвижной связи, открытая сеть, сервер приложений и ASP.

В настоящей модели существуют пять взаимосвязей между: подвижным пользователем и подвижным терминалом, подвижным терминалом и сетью подвижной связи, сетью подвижной связи и открытой сетью, открытой сетью и сервером приложений и подвижным терминалом и сервером приложений.

6.2 Модель подвижной передачи данных от конца до конца между подвижным пользователем и поставщиком ASP со шлюзом

Другая модель (модель со шлюзом) подвижной передачи данных от конца до конца между подвижным пользователем и ASP показана на рисунке 2.

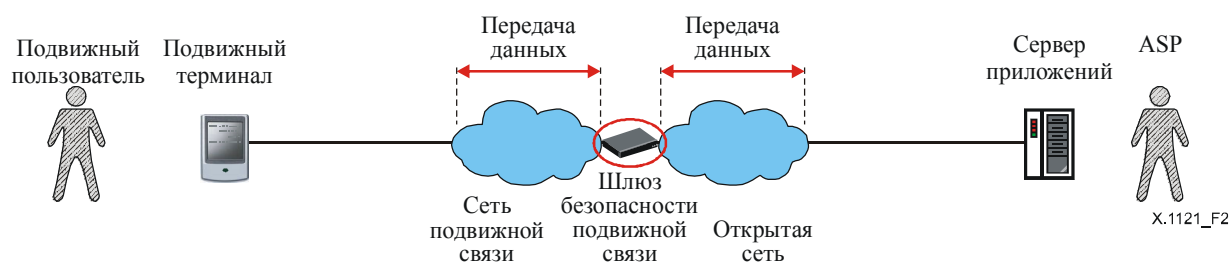


Рисунок 2/X.1121 – Модель подвижной передачи данных от конца до конца между подвижным пользователем и поставщиком ASP со шлюзом

В настоящую модель входят семь объектов: подвижный пользователь, подвижный терминал, сеть подвижной связи, открытая сеть, сервер приложений, ASP и шлюз безопасности подвижной связи.

В настоящей модели существуют шесть взаимосвязей между: подвижным пользователем и подвижным терминалом, подвижным терминалом и сетью подвижной связи, сетью подвижной связи и шлюзом безопасности подвижной связи, шлюзом безопасности подвижной связи и открытой сетью, открытой сетью и сервером приложений, подвижным терминалом и шлюзом безопасности подвижной связи и шлюзом безопасности подвижной связи и сервером приложений.

7 Характеристики подвижной передачи данных от конца до конца

Подвижная передача данных от конца до конца имеет более разнообразные характеристики по сравнению с обобщенной передачей данных от конца до конца в открытой сети. Эти характеристики перечислены ниже.

Подвижная связь основана на беспроводной связи

Поскольку подвижная передача данных от конца до конца основана на беспроводной связи, она более нестабильна, чем проводная передача данных от конца до конца в открытой сети. Кроме того, поскольку подвижный пользователь во время подвижной передачи данных от конца до конца может перемещаться с места на место, это также добавляет нестабильности.

Беспроводная связь может быть основана на широкополосной связи между подвижным терминалом и сетью подвижной связи.

Подвижные терминалы обычно бывают малыми терминалами

Обычно подвижные терминалы, которые используются для подвижной передачи данных от конца до конца, меньше, чем типичные существующие терминалы (например, настольные ПК), которые используются для передачи данных от конца до конца в открытой сети. Следствиями этого являются:

- трудности с вводом или выводом данных.
Трудно вводить данные с клавиатуры или специализированной клавиатуры и видеть много данных на экране из-за ограниченного пространства экрана (в особенности в случае маломерного ручного терминала);
- меньшая производительность, чем у настольного ПК;
- ограничение соответствующих возможностей применения (объем памяти, электропитание и т. д.).

Подвижные терминалы перемещаются подвижными пользователями с места на место

8 Угрозы безопасности в подвижной среде

Существуют два типа угроз безопасности. К одному из них относятся общие угрозы безопасности, которые могут существовать в любой открытой сети. Другие относятся к угрозам безопасности, ориентированным на подвижную связь, которые могут существовать вследствие особенностей подвижной связи.

8.1 Общие угрозы безопасности

Являясь подмножеством передачи данных от конца до конца, подвижная передача данных от конца до конца уязвима со стороны общих угроз безопасности, существующих в открытых сетях.

8.1.1 Подслушивание

Наиболее часто выявляемой проблемой в открытых сетях является подверженность подслушиванию при анонимных атаках. Анонимные атакующие могут активно перехватывать передаваемые данные, вызывая утечку данных.

8.1.2 Создание помех средствам связи

Оно имеет место, когда преднамеренная или непреднамеренная помеха подавляет передатчик или приемник звена связи, вследствие чего эффективное использование звена связи становится невозможным. Итогом этого может быть атака типа DoS.

8.1.3 Вставка и изменение данных

Это случается, когда неуполномоченный объект вводит, изменяет или удаляет информацию, передаваемую между подвижным терминалом и сервером приложений. Неуполномоченным объектом может быть лицо, программа или компьютер. Эти атаки происходят, когда атакующий добавляет данные к существующему соединению с целью разрушения соединения или злонамеренной передачи данных. Итогом этого может быть атака типа DoS или атака типа посредника (man-in-the-middle).

8.1.4 Прерывание

Результатом атаки этого типа является разрушение компонента подвижного терминала или сетевого элемента, примерами являются разрушения части аппаратного обеспечения, такого как жесткий диск; разрыв линии связи или неработоспособность системы управления файлами в подвижном терминале или сетевого элемента в инфраструктуре сети подвижной связи.

8.1.5 Несанкционированный доступ

Под управлением доступом понимается способность ограничивать и управлять доступом к серверу приложений через звено связи. Эта угроза возникает, когда незаконный объект получает доступ к серверу приложений, маскируясь под действительного подвижного пользователя. Объект, пытающийся получить несанкционированный доступ, должен быть выявлен или аутентифицирован.

8.1.6 Непризнание авторства

Эта атака возникает, когда передатчик или приемник отрицает факт передачи или приема сообщения, соответственно.

8.2 Угрозы безопасности, ориентированные на подвижную связь

Существуют угрозы безопасности, ориентированные на подвижную связь, которые являются следствием особенностей беспроводной связи и широковещательной связи между подвижным терминалом и сетью подвижной связи. Наиболее широко выявляемой проблемой в беспроводной сети является подверженность анонимным атакующим.

Ниже перечислены угрозы безопасности, ориентированные на подвижную связь.

8.2.1 Подслушивание

В подвижной связи оно может быть выполнено наиболее просто путем активного перехвата радиосигналов и декодирования переданных данных, вызывающего утечку данных.

8.2.2 Создание помех средствам связи

В подвижной связи это также может быть выполнено наиболее просто между подвижным терминалом и подвижной сетью. Существуют два типа атак: создание помех подвижному терминалу и создание помех элементу сети. Первая позволяет подвижному терминалу-мошеннику выдавать себя за законный подвижный терминал. Последняя играет роль законного элемента сети, взаимодействующего с подвижным терминалом через беспроводной стык.

8.2.3 Блуждание с подглядыванием

Это происходит, когда атакующий собирает информацию в местах с интенсивной деятельностью путем наблюдения за нажатием клавиш, чтением с экрана подвижного терминала или прослушивания звуков, исходящих от подвижного терминала. Это приводит к утечке информации.

8.2.4 Потерянный подвижный терминал

Эта угроза безопасности может произойти с подвижным терминалом, перемещаемым с места на место подвижным пользователем. Она может привести к потере или разрушению информации, хранящейся в подвижном терминале.

8.2.5 Похищенный подвижный терминал

Эта угроза также может произойти с подвижным терминалом, перемещаемым с места на место подвижным пользователем. Она может привести к утечке информации, хранящейся в подвижном терминале, стиранию данных, вызванному несанкционированным доступом похищенного подвижного терминала, в дополнение к потерям информации, хранящейся в подвижном терминале.

8.2.6 Неподготовленное завершение связи

Эта угроза безопасности является следствием неустойчивой связи или ограничения электропитания. Она может привести к стиранию данных.

8.2.7 Ошибочное чтение

Эта угроза безопасности вызывается малым размером дисплеев подвижных терминалов. Она может привести к стиранию данных за счет маскарда ASP.

8.2.8 Ошибка ввода

Эта угроза безопасности вызвана трудностью ввода данных с малой клавиатуры или специализированной клавиатуры подвижного терминала. Она может привести к ошибке в аутентификации пользователя.

8.3 Отношения угроз безопасности к моделям связи от конца до конца

Угрозы безопасности возникают в отдельных местах моделей. Отношения угроз безопасности и функциональных объектов показаны в таблицах 1 и 2.

В этих таблицах показывается, что в сервере приложений и в шлюзе безопасности подвижной связи существуют одни и те же угрозы безопасности. В этих таблицах также показывается, что существуют схожие угрозы безопасности в отношениях между подвижным терминалом и сервером приложений, подвижным терминалом и шлюзом безопасности подвижной связи, сервером приложений и шлюзом безопасности подвижной связи.

Таблица 1/X.1121 – Отношения общих угроз безопасности к моделям

Объекты, Отношения \ Угрозы	Подслушивание	Создание помех средствам связи	Вставка/ Изменение	Прерывание	Несанкциониро- ванный доступ	Непризнание авторства
Подвижный терминал				X	X	
Сервер приложений		X		X	X	
Отношения между подвижным пользователем и подвижным терминалом						
Отношения между подвижным терминалом и сервером приложений	X	X	X	X		X
Шлюз безопасности подвижной связи				X	X	
Отношения между подвижным терминалом и шлюзом безопасности подвижной связи	X	X	X	X		X
Отношения между сервером приложений и шлюзом безопасности подвижной связи	X	X	X	X		X

Таблица 2/X.1121 – Отношения к моделям угроз безопасности, ориентированных на подвижную связь

Объекты, Отношения \ Угрозы	Подслушивание	Создание помех средствам связи	Блуждание с подглядыванием	Потерянный/ Похищенный терминал	Неподготовленное завершение связи	Ошибочное чтение/Ошибка ввода
Подвижный терминал		X		X		
Сервер приложений						
Отношения между подвижным пользователем и подвижным терминалом			X			X
Отношения между подвижным терминалом и сервером приложений	X	X			X	
Шлюз безопасности подвижной связи		X				
Отношения между подвижным терминалом и шлюзом безопасности подвижной связи	X	X			X	
Отношения между сервером приложений и шлюзом безопасности подвижной связи	X	X			X	

9 Требования к безопасности для подвижной передачи данных от конца до конца

Существуют два типа требований к безопасности для подвижной передачи данных от конца до конца. Один из них представляет точку зрения подвижного пользователя. Другой – точку зрения поставщика ASP.

9.1 Требования к безопасности с точки зрения подвижного пользователя

Существуют много различных ожиданий и потребностей пользователей, когда они поступают в приложения. Общим для большинства подвижных пользователей является их надежда просто на то, что приложение работоспособно и дружелюбно по отношению к пользователю. Большинство людей надеются, что приложения и поставщики услуг обрабатывают их персональные данные безопасным и учитывающим секретность образом. Для удовлетворения этих ожиданий подвижный пользователь устанавливает условия в следующих зонах безопасности информации:

- управление идентификацией;
- конфиденциальность данных;
- целостность данных;
- аутентификация;
- управление доступом;
- фиксация авторства;
- анонимность;
- секретность;
- применимость;
- готовность.

9.1.1 Управление идентификацией

Управление идентификацией обычно относится к защите информации об идентификации пользователя. Поэтому управление идентификацией является очень важным аспектом обеспечения секретности пользователя. Во время связи могут использоваться псевдонимы. Требования подвижного пользователя к управлению идентификацией относятся к генерированию (или запросу на генерирование), поддержке, удалению (или запросу на удаление) и применению ключей в соответствии со стратегией безопасности подвижного пользователя.

9.1.2 Конфиденциальность данных

В требованиях подвижного пользователя к конфиденциальности данных содержится следующее:

Конфиденциальность данных, передаваемых между подвижным терминалом и сервером приложений

Это обеспечивает конфиденциальность всех или чувствительных данных, передаваемых между подвижным терминалом и сервером приложений.

Конфиденциальность данных, хранящихся в подвижном терминале

Это обеспечивает конфиденциальность всех или чувствительных данных, хранящихся в подвижном терминале.

Конфиденциальность данных, хранящихся в сервере приложений

Это обеспечивает конфиденциальность всех или чувствительных данных в сервере приложений, которые связаны с подвижным пользователем.

В "модели шлюза" требования подвижного пользователя к конфиденциальности данных охватывают также:

Конфиденциальность данных, передаваемых между подвижным терминалом и шлюзом безопасности подвижной связи

Это обеспечивает конфиденциальность всех или чувствительных данных, передаваемых между подвижным терминалом и шлюзом безопасности подвижной связи.

Конфиденциальность данных, передаваемых между сервером приложений и шлюзом безопасности подвижной связи

Это обеспечивает конфиденциальность всех или чувствительных данных, передаваемых между сервером приложений и шлюзом безопасности подвижной связи.

Конфиденциальность данных, хранящихся в шлюзе безопасности подвижной связи

Это обеспечивает конфиденциальность всех или чувствительных данных, хранящихся в шлюзе безопасности подвижной связи.

9.1.3 Целостность данных

В требованиях подвижного пользователя к целостности данных содержится следующее:

Целостность данных, передаваемых между подвижным терминалом и сервером приложений

Это обеспечивает целостность всех или чувствительных данных, передаваемых между подвижным терминалом и сервером приложений.

Целостность данных, хранящихся в подвижном терминале

Это обеспечивает целостность всех или чувствительных данных, хранящихся в подвижном терминале.

Целостность данных, хранящихся в сервере приложений

Это обеспечивает целостность всех данных, хранящихся в сервере приложений, которые связаны с подвижным пользователем.

В "модели шлюза" требования подвижного пользователя к целостности данных охватывают также:

Целостность данных, передаваемых между подвижным терминалом и шлюзом безопасности подвижной связи

Это обеспечивает целостность всех или чувствительных данных, передаваемых между подвижным терминалом и шлюзом безопасности подвижной связи.

Целостность данных, передаваемых между сервером приложений и шлюзом безопасности подвижной связи

Это обеспечивает целостность всех или чувствительных данных, передаваемых между сервером приложений и шлюзом безопасности подвижной связи.

Целостность данных, хранящихся в шлюзе безопасности подвижной связи

Это обеспечивает целостность всех или чувствительных данных, хранящихся в шлюзе безопасности подвижной связи.

9.1.4 Аутентификация

Существуют два типа аутентификации: аутентификация объекта и аутентификация сообщения. Аутентификация объекта предназначена для подтверждения идентичности объекта соответствующему объекту. Аутентификация сообщения предназначена для подтверждения источника или получателя данных. В требованиях аутентификации подвижного пользователя содержится следующее:

Аутентификация ASP

Этот тип аутентификации объекта используется для подтверждения идентичности ASP, чтобы удостовериться, что ASP не предпринимает попыток нелегального проникновения или несанкционированного повторения предшествовавшего соединения.

Аутентификация подвижного пользователя

Этот тип аутентификации объекта используется для подтверждения идентичности пользователя подвижного терминала путем реализации различных схем аутентификации пользователя, таких как отпечатки пальцев, пароль или PIN-код, для обеспечения защиты от несанкционированного доступа с потерянного или похищенного подвижного терминала.

Аутентификация принятых данных

Этот тип аутентификации сообщений используется для подтверждения источника передаваемых данных. Он не требует защиты от дублирования или изменения данных.

9.1.5 Управление доступом

В требованиях подвижного пользователя к управлению доступом содержится следующее:

Управление доступом на подвижном терминале

Это обеспечивает защиту от несанкционированного доступа к подвижному терминалу или от несанкционированного использования его.

Управление доступом должно производиться в соответствии со стратегией безопасности подвижного пользователя.

Управление доступом на сервере приложений

Это обеспечивает защиту от несанкционированного доступа сервера приложений к данным, переданным подвижным пользователем, таким как персональная информация пользователя.

Управление доступом должно производиться в соответствии со стратегией безопасности подвижного пользователя.

В "модели шлюза" требования подвижного пользователя к управлению доступом охватывают также:

Управление доступом на шлюзе безопасности подвижной связи

Это обеспечивает защиту на шлюзе безопасности подвижной связи от несанкционированного доступа к данным, переданным подвижным пользователем, таким как персональная информация пользователя.

Управление доступом должно производиться в соответствии со стратегией безопасности подвижного пользователя.

9.1.6 Фиксация авторства

Это существует в одном или обоих из двух вариантов, описанных ниже:

Фиксация авторства с подтверждением источника

Это используется, чтобы удостовериться, что источником принятых данных является отдельный поставщик ASP. Это необходимо для защиты от любой попытки ASP ложно отказаться от передачи этих данных.

Фиксация авторства с подтверждением доставки

Это используется, чтобы удостовериться доставку данных поставщику ASP. Это необходимо для защиты от любой последующей попытки ASP ложно отказаться от приема этих данных.

Требования фиксации авторства связаны со следующими требованиями: конфиденциальности данных, передаваемых между подвижным терминалом и сервером приложений; целостности данных, передаваемых между подвижным терминалом и сервером приложений; целостности данных, хранящихся на подвижном терминале; аутентификации подвижного пользователя и управления доступом на подвижном терминале.

"Модель шлюза" связана со следующими требованиями: конфиденциальности данных, передаваемых между подвижным терминалом и шлюзом безопасности подвижной связи; конфиденциальности данных, передаваемых между шлюзом безопасности подвижной связи и сервером приложений; целостности данных, передаваемых между подвижным терминалом и шлюзом безопасности подвижной связи; целостности данных, передаваемых между шлюзом безопасности подвижной связи и сервером приложений; целостности данных, хранящихся в шлюзе безопасности подвижной связи.

9.1.7 Анонимность

Это позволяет передавать сообщение так, что поставщик ASP не может идентифицировать подвижного пользователя (и подвижный терминал).

9.1.8 Секретность

Это используется во избежание утечки информации и для предотвращения получения информации неуполномоченными лицами.

Требования секретности связаны со следующими требованиями: конфиденциальности данных, передаваемых между подвижным терминалом и сервером приложений; конфиденциальности данных, хранящихся в подвижном терминале; конфиденциальности данных, хранящихся на сервере приложений; управления доступом на подвижном терминале и управления доступом на сервере приложений.

"Модель шлюза" связана со следующими требованиями: конфиденциальности данных, передаваемых между подвижным терминалом и шлюзом безопасности подвижной связи; конфиденциальности данных, передаваемых между шлюзом безопасности подвижной связи и сервером приложений; конфиденциальности данных, хранящихся на шлюзе безопасности подвижной связи и управления доступом на шлюзе безопасности подвижной связи.

9.1.9 Применимость

Это обеспечивает простое использование приложения и позволяет избежать ошибочного считывания или ошибок ввода.

9.1.10 Готовность

Это предоставляет подвижному пользователю возможность получать прикладную услугу откуда угодно и в любое время.

9.2 Требования к безопасности с точки зрения поставщика ASP

Бизнес, который предлагает свои услуги подвижным пользователям, должен защищать свои системы от мошенничества. Вследствие специфики подвижного оборудования аутентификация абонента и механизмы платежей должны управляться с большой осторожностью. Кроме того, если услуга доставляется подвижным пользователям, не могут быть обойдены фиксация авторства и отслеживание трассы. Вследствие этого у поставщика ASP имеются требования в следующих областях:

- конфиденциальности данных;
- целостности данных;
- аутентификации;
- управления доступом;
- фиксации авторства;
- готовности.

9.2.1 Конфиденциальность данных

В требованиях поставщика ASP к конфиденциальности данных содержится следующее:

Конфиденциальность данных, передаваемых между подвижным терминалом и сервером приложений

Это обеспечивает конфиденциальность всех или чувствительных данных, передаваемых между подвижным терминалом и сервером приложений.

Конфиденциальность данных, хранящихся в подвижном терминале

Это обеспечивает конфиденциальность всех или чувствительных данных или контентов, переданных поставщиком ASP и хранящихся в подвижном терминале.

Конфиденциальность данных, хранящихся в сервере приложений

Это обеспечивает конфиденциальность всех данных, хранящихся в сервере приложений.

В "модели шлюза" требования поставщика ASP к конфиденциальности данных охватывают также:

Конфиденциальность данных, передаваемых между подвижным терминалом и шлюзом безопасности подвижной связи

Это обеспечивает конфиденциальность всех или чувствительных данных, передаваемых между подвижным терминалом и шлюзом безопасности подвижной связи.

Конфиденциальность данных, передаваемых между сервером приложений и шлюзом безопасности подвижной связи

Это обеспечивает конфиденциальность всех или чувствительных данных, передаваемых между сервером приложений и шлюзом безопасности подвижной связи.

Конфиденциальность данных, хранящихся в шлюзе безопасности подвижной связи

Это обеспечивает конфиденциальность всех или чувствительных данных (или контентов), которые передаются поставщиком ASP и хранятся в шлюзе безопасности подвижной связи.

9.2.2 Целостность данных

В требованиях поставщика ASP к целостности данных содержится следующее:

Целостность данных, передаваемых между подвижным терминалом и сервером приложений

Это обеспечивает целостность всех данных, передаваемых между подвижным терминалом и сервером приложений.

Целостность данных, хранящихся в подвижном терминале

Это обеспечивает целостность всех данных или контентов, которые передаются поставщиком ASP и хранятся в подвижном терминале.

Целостность данных, хранящихся в сервере приложений

Это обеспечивает целостность всех данных, хранящихся в сервере приложений, которые связаны с подвижным пользователем (например, персональная информация о подвижном пользователе).

В "модели шлюза" требования поставщика ASP к целостности данных охватывают также:

Целостность данных, передаваемых между подвижным терминалом и шлюзом безопасности подвижной связи

Это обеспечивает целостность всех или (или части) данных, передаваемых между подвижным терминалом и шлюзом безопасности подвижной связи.

Целостность данных, передаваемых между сервером приложений и шлюзом безопасности подвижной связи

Это обеспечивает целостность всех данных, передаваемых между сервером приложений и шлюзом безопасности подвижной связи.

Целостность данных, хранящихся в шлюзе безопасности подвижной связи

Это обеспечивает целостность всех данных или контентов, которые передаются поставщиком ASP и хранятся в шлюзе безопасности подвижной связи.

9.2.3 Аутентификация

Требования к аутентификации со стороны поставщика ASP также касаются аутентификации объекта (подвижный пользователь и подвижный терминал) и аутентификации сообщения (принятые данные).

Аутентификация подвижного пользователя

Этот тип аутентификации объекта используется для подтверждения идентичности подвижного пользователя терминала, чтобы удостовериться, что подвижный пользователь не предпринимает попыток нелегального проникновения или несанкционированного повторения предшествовавшего соединения.

Аутентификация подвижного терминала

Этот тип аутентификации объекта используется для подтверждения идентичности подвижного терминала, чтобы гарантировать, что подвижный терминал имеет функциональность, необходимую для доступа к прикладной услуге.

Аутентификация принятых данных

Этот тип аутентификации сообщений используется для подтверждения источника передаваемых данных. Он не требует обеспечения защиты от дублирования или изменения данных.

9.2.4 Управление доступом

В требованиях поставщика ASP к управлению доступом содержатся требования к управлению доступом на сервере приложений и к управлению доступом на подвижном терминале:

Управление доступом на сервере приложений

Это обеспечивает защиту от несанкционированного доступа к серверу приложений или от его несанкционированного использования.

Управление доступом должно производиться в соответствии со стратегией безопасности поставщика ASP.

Управление доступом на подвижном терминале

Это обеспечивает защиту от несанкционированного доступа к данным или контентам, передаваемым поставщиком ASP подвижному терминалу.

Управление доступом должно производиться в соответствии со стратегией безопасности поставщика ASP.

В "модели шлюза" требования поставщика ASP к управлению доступом охватывают также:

Управление доступом на шлюзе безопасности подвижной связи

Это обеспечивает защиту от несанкционированного доступа к данным или контентам, передаваемым поставщиком ASP на шлюз безопасности подвижной связи.

Управление доступом должно производиться в соответствии со стратегией безопасности поставщика ASP.

9.2.5 Фиксация авторства

Это существует в одном или обоих из двух вариантов, описанных ниже:

Фиксация авторства с подтверждением источника

Это используется, чтобы удостовериться, что источником принятых данных является отдельный подвижный пользователь. Это необходимо для защиты от любой попытки подвижного пользователя ложно отказаться от передачи этих данных.

Фиксация данных с подтверждением доставки

Это используется, чтобы удостовериться доставку данных подвижному пользователю. Это необходимо для защиты от любой последующей попытки подвижного пользователя ложно отказаться от приема этих данных.

Требования фиксации авторства поставщика ASP связаны со следующим: конфиденциальностью данных, передаваемых между подвижным терминалом и сервером приложений; целостностью данных, передаваемых между подвижным терминалом и сервером приложений; целостностью данных, хранящихся на подвижном терминале; аутентификацией подвижного пользователя и управлением доступом на подвижном терминале.

"Модель шлюза" связана со следующими требованиями: конфиденциальности данных, передаваемых между подвижным терминалом и шлюзом безопасности подвижной связи; конфиденциальности данных, передаваемых между шлюзом безопасности подвижной связи и сервером приложений; целостности данных, передаваемых между подвижным терминалом и шлюзом безопасности подвижной связи; целостности данных, передаваемых между шлюзом безопасности подвижной связи и сервером приложений; целостности данных, хранящихся в шлюзе безопасности подвижной связи.

9.2.6 Готовность

Это предоставляет подвижному пользователю возможность получать прикладную услугу откуда угодно и в любое время.

9.3 Взаимоотношения между требованиями безопасности и угрозами безопасности

Всякое требование безопасности является контрмерой против определенных угроз безопасности. Взаимоотношения между требованиями безопасности и угрозами безопасности показаны в таблицах 3 и 4.

Таблица 3/X.1121 – Взаимоотношения между требованиями безопасности и угрозами безопасности

Требования \ Угрозы	Подслушивание	Создание помех средствам связи	Вставка/Изменение	Прерывание	Несанкционированный доступ	Непризнание авторства
Управление идентификацией	X				X	X
Конфиденциальность передаваемых данных	X					
Конфиденциальность хранящихся данных					X	
Целостность передаваемых данных			X			
Целостность хранящихся данных					X	
Аутентификация объекта			X		X	X
Аутентификация сообщения			X			
Управление доступом			X		X	
Фиксация авторства						X
Анонимность					X	
Секретность	X				X	
Применимость						
Готовность		X		X		

Таблица 4/X.1121 – Взаимоотношения между требованиями безопасности и угрозами безопасности, ориентированными на подвижную связь

Требования \ Угрозы	Подслушивание	Создание помех средствам связи	Блуждание с подглядыванием	Потерянный/Похищенный терминал	Неподготовленное завершение связи	Ошибочное чтение/Ошибка ввода
Управление идентификацией	X					
Конфиденциальность передаваемых данных	X					
Конфиденциальность хранящихся данных				X		
Целостность передаваемых данных						
Целостность хранящихся данных				X		
Аутентификация объекта				X		
Аутентификация сообщения						

Управление доступом				X		
Фиксация авторства						
Анонимность				X		
Секретность	X		X	X		
Применимость						X
Готовность		X			X	

10 Функции безопасности для удовлетворения требований безопасности подвижной связи

Для удовлетворения требований безопасности подвижной передачи данных от конца до конца существуют несколько функций безопасности, которые могут быть использованы, как следующие:

- шифрование;
- обмен ключами;
- цифровая подпись;
- управление доступом;
- целостность данных;
- обмен данными аутентификации;
- заверение.

Шифрование

Функция шифрования может обеспечить конфиденциальность передаваемых или хранящихся данных.

Алгоритмы шифрования могут быть обратимыми или необратимыми. Существуют две общие классификации обратимого алгоритма шифрования:

- a) симметричное (т. е. с секретным ключом) шифрование, в котором знание ключа шифрования предполагает знание ключа дешифрирования, и наоборот;
- b) асимметричное (например, с открытым ключом) шифрование, в котором знание ключа шифрования не подразумевает знания ключа дешифрирования, и наоборот. Два ключа такой системы иногда называются "открытым ключом" и "личным ключом".

Алгоритмы необратимого шифрования могут использовать, а могут не использовать ключ. Когда они используют ключ, этот ключ может быть открытым или секретным.

В связи с низкой производительностью или малым объемом памяти подвижных терминалов имеются некоторые трудности с реализацией существующих функций шифрования, в особенности асимметричного алгоритма, используемого в действующих открытых сетях. В случае продолжения использования существующих функций шифрования на серверах в открытых сетях часто используется модель со шлюзом.

Обмен ключами

Функция обмена ключами позволяет совместно использовать ключи при реализации шифрования, в особенности в алгоритме симметричного шифрования.

Цифровая подпись

Функция цифровой подписи определяет два процесса:

- a) подписания данных; и
- b) верификации подписанных данных.

В первом процессе подписантом используется информация, которая является частной (т. е. уникальной и конфиденциальной). Во втором процессе используются процедуры и информация, которые широко доступны, но из которых нельзя установить частную информацию подписанта.

В процессе подписания применяется либо шифрование данных, либо выработка криптографического проверочного значения данных, использующего в качестве частного ключа частную информацию подписанта.

Процесс верификации включает использование открытых процедур и информации для определения правильности построения подписи по частной информации подписанта.

Основной особенностью функции подписи является то, что подпись может быть выработана только с использованием частной информации подписанта. Таким образом, когда подпись верифицирована, то впоследствии в любое время третьей стороной (например, судьей или арбитром) может быть удостоверено, что данную подпись мог выработать только единственный держатель частной информации.

Что касается функции шифрования, то в связи с низкой производительностью или малым объемом памяти подвижных терминалов имеются некоторые трудности с применением существующих функций цифровой подписи, используемых в действующих открытых сетях.

Управление доступом

В функции управления доступом может использоваться аутентифицированная идентификация объекта или информация об объекте (такая как причастность, к известной совокупности объектов) или о возможностях объекта с целью определить и обеспечить соблюдение прав доступа, имеющихся у объекта. Если объект пытается использовать неразрешенный ресурс или разрешенный ресурс с неподходящим типом доступа, то функция управления доступом отклонит эту попытку и, кроме того, может сообщить о происшествии с целью выработки аварийного сигнала и/или записи его как части данных аудита безопасности.

Функция управления доступом может основываться на использовании следующих пунктов:

- a) баз информации об управлении доступом, в которых хранятся права доступа равноправных объектов;
- b) информации об аутентификации, такой как пароли, владение и последующее представление которой свидетельствует о авторизации объекта, претендующего на получение доступа;
- c) возможностей, владение и последующее представление которых свидетельствует о праве доступа к объекту или ресурсу, определенному возможностью;
- d) меток безопасности, которые, будучи связаны с объектом, могут быть использованы для предоставления или отказа в доступе, обычно в соответствии со стратегией безопасности;
- e) времени попытки доступа;
- f) маршрута попытки доступа;
- g) продолжительности доступа; и
- h) физического местоположения попытки доступа.

Функция управления доступом может быть применима либо к равноправным объектам, участвующим в связи, и/или в шлюзе безопасности подвижной связи.

Управление доступом подразумевает, что исходящий объект или шлюз безопасности подвижной связи используется для определения, уполномочен ли отправитель связываться с получателем и/или использовать запрашиваемые связные ресурсы.

Целостность данных

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

Определение целостности отдельного блока данных включает два процесса: один на передающем объекте и один на принимающем. Передающий объект добавляет к данным величину, которая является функцией самих данных. Эта величина может содержать дополнительную информацию, такую как блоковый проверочный код или криптографическая проверочная величина, и может быть зашифрована. Принимающий объект генерирует соответствующую величину и сравнивает ее с

принятой величиной, чтобы определить, не были ли данные изменены при передаче. Один этот процесс не защитит от повторения отдельного блока данных.

Защита целостности последовательности блоков данных (т.е. защита от изменения порядка следования, потерь, повторения и вставки или изменения данных) требует добавления некоторой формы явного упорядочивания, такой как нумерация последовательности, временные метки или криптографическое связывание.

Обмен данными аутентификации

К обмену данными аутентификации могут быть применены некоторые технологии безопасности:

- a) использование информации об аутентификации, такой как пароли, поставляемые передающим объектом и проверяемые принимающим объектом;
- b) криптографические технологии; и
- c) использование свойств и/или собственности объекта.

Функция обмена данными аутентификации может быть включена для проведения аутентификации равноправных объектов. Если функция не осуществит аутентификации объекта, то это будет следствием отклонения или завершения соединения и может послужить причиной входа в данные аудита безопасности и/или в сообщение центру управления безопасностью.

Когда используются криптографические методы, то они могут быть объединены с протоколами "установления связи" ("handshaking") для защиты от повторений (т.е. чтобы гарантировать жизненность).

Выбор технологии безопасности, которая реализует обмен данными аутентификации, будет зависеть от обстоятельств, в которых требуется их использовать совместно с:

- a) временными метками и синхронизированными часами;
- b) двух- и трехступенчатым установлением связи (для односторонней и обоюдной аутентификации соответственно); и
- c) функциями фиксации авторства, осуществляемыми с помощью цифровой подписи и/или механизмов заверения.

Заверение

Свойства данных, передаваемых между двумя или более объектами, такие как целостность, источник, время и пункт назначения, могут быть гарантированы путем выполнения функции заверения. Гарантия обеспечивается нотариусом третьей стороны, которой доверяют обменивающиеся объекты и которая содержит информацию, необходимую для предоставления требуемой гарантии, путем использования верификации. В каждом случае связи могут использоваться цифровая подпись, шифрование и функции целостности, которые выделены услуге, обеспечиваемой нотариусом. Когда вызвана такая функция заверения, данные между обменивающимися объектами передаются через защищенные инстанции связи и нотариуса.

Эти функции безопасности используются для удовлетворения некоторых требований безопасности. В таблице 5 показано, какие функции безопасности каким требованиям удовлетворяют.

Таблица 5/X.1121 – Иллюстрация взаимоотношений между требованиями и функциями безопасности

Требования \ Функции	Шифрование	Обмен ключами	Цифровая подпись	Управление доступом	Целостность данных	Аутентификационный обмен	Заверение
Управление идентификацией	X	X	X			X	
Конфиденциальность передаваемых данных	X	X		X		X	
Конфиденциальность хранящихся данных	X			X			
Целостность передаваемых данных	X	X	X	X	X	X	
Целостность хранящихся данных	X		X	X	X		
Аутентификация объекта	X		X			X	
Аутентификация сообщения	X	X	X		X	X	
Управление доступом				X		X	
Фиксация авторства			X			X	X
Анонимность	X						
Применимость				X			
Секретность	X			X		X	
Готовность				X		X	

11 Технологии безопасности для подвижной передачи данных от конца до конца

Для реализации функций безопасности, описанных в разделе 10, используются различные технологии безопасности для подвижной передачи данных от конца до конца (т. е. технологии безопасной подвижной связи). Эти технологии безопасной подвижной связи классифицируются по функциям безопасности, реализуемым технологией безопасности, и местам применения технологии безопасности. Поскольку технология безопасности применяется к объекту или к отношению между объектами в моделях подвижной передачи данных от конца до конца, места, в которых применяется технология безопасности, указывают на объекты или отношения между объектами. В таблицах 1 и 2 показывается, где в моделях подвижной передачи данных от конца до конца появляются угрозы безопасности. В таблицах 3 и 4 показывается, какие требования безопасности создаются в качестве контрмер отдельным угрозам безопасности, а в таблице 5 показываются функции безопасности, которые удовлетворяют требованиям безопасности. Вследствие этого взаимоотношение между функциями безопасности и местами применения этих функций безопасности в моделях может быть показано в таблице 6. Другими словами, в таблице 6 показывается, где в моделях применяются технологии безопасности в подвижной связи, которые реализуют некоторые функции безопасности.

Отдельная технология безопасности в подвижной связи может реализовать только часть функций безопасности или быть применимой в отдельном месте. Например, криптографический алгоритм с эллиптическими кривыми может быть использован для реализации функции обмена ключами при отношениях между пользователем и подвижным терминалом. Биометрическая технология аутентификации может быть использована для реализации функции обмена данными аутентификации при отношениях между пользователем и подвижным терминалом. Технология инфраструктуры открытого ключа (PKI) может использоваться для реализации всех функций безопасности при отношениях между подвижным терминалом и сервером, отношениях между подвижным терминалом и шлюзом безопасности подвижной связи и отношениях между сервером и шлюзом безопасности подвижной связи.

Таблица 6/X.1121 – Взаимоотношения между технологиями безопасности подвижной связи и моделями

Места, в которых применяются технологии Функции, реализуемые технологиями	Подвижный терминал	Сервер приложений/ Шлюз безопасности подвижной связи	Отношение между подвижным пользователем и подвижным терминалом	Отношение между подвижным терминалом и сервером приложений или другие отношения
Шифрование	X	X	X	X
Обмен ключами				X
Цифровая подпись	X	X		X
Управление доступом	X	X	X	X
Целостность данных	X	X		X
Обмен данными аутентификации	X	X	X	X
Заверение				X

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия А	Организация работы МСЭ-Т
Серия В	Средства выражения: определения, символы, классификация
Серия С	Общая статистика электросвязи
Серия D	Общие принципы тарификации
Серия E	Общая эксплуатация сети, телефонная служба, функционирование служб и человеческие факторы
Серия F	Нетелефонные службы электросвязи
Серия G	Системы и среда передачи, цифровые системы и сети
Серия H	Аудиовизуальные и мультимедийные системы
Серия I	Цифровая сеть с интеграцией служб
Серия J	Кабельные сети и передача сигналов телевизионных и звуковых программ и других мультимедийных сигналов
Серия K	Защита от помех
Серия L	Конструкция, прокладка и защита кабелей и других элементов линейно-кабельных сооружений
Серия M	TMN и техническое обслуживание сетей: международные системы передачи, телефонные, телеграфные, факсимильные и арендованные каналы
Серия N	Техническое обслуживание: международные каналы передачи звуковых и телевизионных программ
Серия O	Требования к измерительной аппаратуре
Серия P	Качество телефонной передачи, телефонные установки, сети местных линий
Серия Q	Коммутация и сигнализация
Серия R	Телеграфная передача
Серия S	Оконечное оборудование для телеграфных служб
Серия T	Оконечное оборудование для телематических служб
Серия U	Телеграфная коммутация
Серия V	Передача данных по телефонной сети
Серия X	Сети передачи данных и взаимосвязь открытых систем
Серия Y	Глобальная информационная инфраструктура, аспекты межсетевого протокола (IP) и сети последующих поколений
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи