Министерство Российской федерации

по связи и информатизации

Сибирский государственный университет

телекоммуникаций и информатики

**С.Н. Новиков**

**защита информации**

**в сетях связи с гарантированным качеством обслуживания**

**учебное пособие**

Новосибирск

2003

УДК 681.327.8(031)+681.3224(031)

С.Н. Новиков. Защита информации в сетях связи с гарантированным качеством обслуживания / Учебное пособие. ⎯ Новосибирск: 2003.⎯ 84 с.: ил.

Учебное пособие посвящено вопросам защиты информации в сетях связи с гарантированным качеством обслуживания (ATM и IP v6.0). В частности, представлены специальные протоколы и механизмы, обеспечивающие защиту соединений ATM и IP v6.0.

Приведены основные определения, сокращения и выражения, которые часто встречаются в литературе на английском языке по данной тематике.

При написании учебного пособия использованы материалы ATM Forum, IETF, монографий, статей отечественных и зарубежных авторов.

Для специалистов в области сетей связи и защиты информации, аспирантов и студентов старших курсов, обучающихся по специальностям: 200900 – сети связи и системы коммутации; 201800 – защищенные системы связи.

Каф. РТС

Иллюстраций ⎯ 33, таблиц ⎯ 3, приложений ⎯ 3,

список литературы ⎯ 16 названий.

Рецензенты:

Утверждено редакционно-издательским советом СибГУТИ

в качестве учебного пособия.

© Сибирский государственный университет

телекоммуникаций и информатики, 2003 г.

ОГЛАВЛЕНИЕ

введение 5

1 Общие положения 6

1.1 Основные определения 6

1.2 Требования к системам телекоммуникаций 7

1.2 Классификация нарушений передачи информации 8

1.3 Сервисные службы, профиль защиты и соединения защиты информации 12

Контрольные вопросы 16

2 криптографические системы 18

2.1 Криптосистема с одним ключом 18

2.2 Криптосистемы с открытым ключом 20

2.3 Распределение открытых ключей 23

2.4 Применение криптосистемы с открытым ключом для распределения секретных ключей 26

2.5 Применение криптосистемы с открытым ключом для аутентификации пользователя со стороны автономного объекта 29

Контрольные вопросы 31

3 общие критерии оценки безопасности информационных технологий 33

3.1 Целевая направленность общих критериев 33

3.2 Концепция общих критериев 34

3.3 Профили защиты 34

3.4 Нормативные документы оценки безопасности информационных технологий в Российской Федерации 34

4 защита информации в сетях с технологией ATM 35

4.1 Обмен информацией между агентами защиты 35

4.1 Защита информации в плоскости пользователя 36

4.1 Сервисные службы защиты информации плоскости пользователя 36

4.2 Службы поддержки 38

4.2 Защита информации плоскости управления 41

4.2 Сервисные службы защиты информации плоскости управления 41

4.3 Защита информации плоскости менеджмента 42

4.3 Сервисные службы защиты информации плоскости менеджмента 42

Контрольные вопросы 42

5 защита информации в сетях с технологией IP 43

5.1 43

приложение 1 англо-русский словарь 44

Список сокращений 46

список литературы 47

# введение

Ни одна сфера жизни современного общества не может функционировать без развитой информационной структуры. Национальный информационный ресурс является сегодня одним из главных источников экономической и военной мощи государства. Проникая во все сферы деятельности государства, информация приобретает конкретное политическое, экономическое и материальное выражение. На этом фоне все более актуальный характер приобретает в последние десятилетия и, особенно в настоящее время, задача обеспечения информационной безопасности Российской Федерации как неотъемлемого элемента ее национальной безопасности, а защита информации превращается в одну из приоритетных государственных задач.

Вопросы защиты информации всегда занимали особое место в любом обществе и государстве. В настоящее время, когда сохраняется лавинообразное распространение компьютерных систем и их взаимодействие посредством телекоммуникационных сетей, защита информации пользователей и служебной информации выступает на одно из первых мест.

# 1 Общие положения

## 1.1 Основные определения

Введем некоторые понятия и определения, необходимые в дальнейшем.

На рисунке 1.1 приведена классификация основных определений и понятий предметной области «Защита информации» [1, 2].



*Информация* [1]– сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

*Защищаемая информация –* информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации. Собственником информации может быть: государство, юридическое лицо, группа физических лиц, отдельное физическое лицо.

*Защита информации* – деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

*Защита информации от утечки* – деятельность, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения, несанкционированного доступа к информации и получения защищаемой информации разведками.

*Защита информации от несанкционированного воздействия* – деятельность, направленная на предотвращение воздействия на защищаемую информацию с нарушением установленных прав и (или) правил на изменение информации, приводящего к ее искажению, уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

*Защита информации от непреднамеренного воздействия* – деятельность, направленная на предотвращение воздействия на защищаемую информацию ошибок ее пользователя, сбоя технических и программных средств информационных систем, природных явлений или иных нецеленаправленных на изменение информации мероприятий, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

*Защита информации от разглашения –* деятельность, направленная на предотвращение несанкционированного доведения защищаемой информации до потребителей, не имеющих права доступа к этой информации.

*Защита информации от несанкционированного доступа* – деятельность, направленная на предотвращение получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации.

## 1.2 Требования к системам телекоммуникаций

Приведем основные требования, предъявляемые пользователями к системам телекоммуникаций с позиций обеспечения защиты передаваемой информации. Системы телекоммуникаций должны обеспечить:

* *конфиденциальность информации* – обеспечение просмотра информации в приемлемом формате только для пользователей, имеющих право доступа к этой информации;
* *целостность информации* – обеспечение неизменности информации при ее передаче;
* *аутентичность информации* – обеспечение надежной идентификации источника сообщения, а также гарантия того, что источник не является поддельным.
* *доступность информации* – гарантия доступа санкционированных пользователей к информации.

## 1.2 Классификация нарушений передачи информации

*Нормальная передача информации* (рисунок 1.2 а)) в сетях с гарантируемым качеством обслуживания пользователей подразумевает выполнение трех этапов (рисунок 1.2 а)) [3, 4].

1. В плоскости менеджмента – формирование и корректировка баз данных (БД) о состоянии элементов сети. Конечным результатом функционирования данного этапа является формирование плана распределения информации на сети - расчет таблиц маршрутизации (ТМ) во всех узлах для каждой службы электросвязи.
2. В плоскости управления (стек протоколов сигнализации) - организацию маршрута между узлом – источником (УИ) и узлом – получателем (УП) в виде виртуального коммутируемого либо постоянного соединения (канала или тракта). Конечным результатом функционирования данного этапа является заполнение и обнуление таблиц коммутации (ТК).
3. В плоскости пользователя - непосредственная передача пользовательской информации.

При этом передача всех видов информации в сети (служебной – для формирования БД и ТК; пользовательской) осуществляется по своим отдельно выделенным виртуальным соединениям (каналам и трактам).

Под *нарушением передачи информации* будем понимать одну из ситуаций, которые могут быть организованы нарушителем (рисунок 1.3).

* Прерывание или разъединение (рисунок 1. 3. а)). Информация уничтожается или становится недоступной либо непригодной для использования. В этом случае *нарушается доступность информации*. Примером таких нарушений может быть воздействие нарушителя на элементы сети (линии связи (ЛС), узлы коммутации (УК), устройства управления, БД и так далее) с целью их уничтожения или приведение в нерабочее состояние.
* Перехват (рисунок 1. 3. б)). К информации открывается несанкционированный доступ. *Нарушается конфиденциальность передаваемой информации*. Примером такого типа нарушений является несанкционированное подключение к каналу связи.



* Модификация (рисунок 1. 3. в)). К информации открывается несанкционированный доступ с целью изменения информации. При этом *нарушается конфиденциальность передаваемой информации и ее целостность*. Целью такого типа нарушений является изменение информации, передаваемой по сети.
* Фальсификация (рисунок 1. 3. г)). Нарушитель выдает себя за источник информации. При этом *нарушается аутентичность информации*. Примером такого типа нарушений является отправка поддельных сообщений по сети.



Приведенные выше типы нарушений можно разделить на две группы:

* активные;
* пассивные.

К первой группе относятся:

* прерывание - нарушение доступности и конфиденциальности;
* модификация - нарушение целостности;
* фальсификация - нарушение аутентичности.



Данный тип нарушений имеет активный характер воздействия на элементы сети и передаваемую информацию. Основная цель этих нарушений состоит в изменении либо уничтожении потоков информации на сети.

К пассивным нарушениям относится перехват с целью получения передаваемой информации, ее анализа и использования в определенных целях.

Достаточно уверенно можно утверждать, что пассивные нарушения ставят своей конечной целью переход в группу активных нарушений.

Приведенная выше классификация нарушений защиты информации представлена в таблице 1.1.

Перечисленные виды нарушений могут иметь место, как в плоскости пользователя, так и в плоскостях управления и менеджмента (рисунок 1.2 б)). Причем, активные виды нарушений (прерывание, модификация и фальсификация) в плоскости менеджмента ведут к нарушениям либо уничтожению информации, хранимой в базах данных УК. В результате нарушаются таблицы маршрутизации и как результат – невозможность нормального функционирования плоскостей управления (сигнализации) и пользователя.

## 1.3 Сервисные службы, профиль защиты и соединения защиты информации

*Сервисные службы защиты информации* (рисунок 1.4) являются ответственными за обеспечение основных требований пользователей, предъявляемых к телекоммуникационным системам (с точки зрения ее надежности). Причем данные службы должны функционировать во всех трех плоскостях: менеджмента, управления и пользовательской.



Совокупность сервисных служб защиты информации, обеспечивающих требования пользователей, образуют *профиль защиты*.

За установку и прекращение действия той или иной службы отвечают *агенты защиты* (Security Agent , SA). Согласование служб защиты между агентами происходит *через соединения защиты*. По этим соединениям производится обмен *информацией защиты*.

Рисунок 1.5 демонстрирует самый простой вариант организации соединения защиты - агенты защиты размещены в пределах конечных систем пользователей. В данном случае конечные системы и агенты защиты взаимодействуют с сетью через интерфейс «пользователь – сеть + защита» (UNI+Sec).

Агенты защиты для виртуального соединения (канала либо тракта), который установлен между конечными системами пользователей, последовательно выполняют следующие действия:

* определяют вид сервисных служб защиты, которые должны быть применены к данному виртуальному соединению;
* согласовывают службы защиты между собой;
* применяют требуемые службы защиты к данному виртуальному соединению.





Количество соединений защиты должно быть равно количеству установленных служб защиты. То есть, если для данного виртуального соединения одновременно требуется аутентификация, конфиденциальность и достоверность данных, то устанавливается три самостоятельных соединения защиты.

Рисунок 1.6 показывает другой вариант организации соединения защиты. В этом случае один агент защиты размещается на конечной системе пользователя, а другой на коммутаторе виртуальных каналов. Соответственно, пользователи и агенты защиты взаимодействуют с сетью связи через интерфейсы «пользователь – сеть» (UNI) либо UNI+Sec; коммутатор виртуальных каналов через интерфейс «узел – сеть + защита» (NNI+Sec). В данном случае агент защиты, размещенный в пределах коммутатора виртуальных каналов, имеет возможность обеспечивать службы защиты не только для пользователя *П*2, но и для других узлов и сетей, которые подсоединяются к данному коммутатору виртуальных каналов. Часто таких агентов защиты называют *брандмауэрами*. Фактически брандмауэр – это шлюз, который выполняет функции защиты сети от несанкционированного доступа из вне (например, из другой сети).

Различают три типа брандмауэров (рисунок 1.7).

*Шлюз уровня приложений* часто называют *прокси – сервером* (proxy server) - выполняет функции ретранслятора данных для ограниченного числа приложений пользователя. То есть, если в шлюзе не организована поддержка того или иного приложения, то соответствующий сервис не предоставляется, и данные соответствующего типа не могут пройти через брандмауэр.



*Фильтрующий маршрутизатор.* Точнее это маршрутизатор, в дополнительные функции которого входит фильтрование пакетов (packet-filtering router). Используется на сетях с коммутацией пакетов в режиме дейтаграмм. То есть, в тех технологиях передачи информации на сетях связи, в которых плоскость сигнализации (предварительного установления соединения между УИ и УП) отсутствует (например, IP V 4). В данном случае принятие решения о передаче по сети поступившего пакета данных основывается на значениях его полей заголовка транспортного уровня. Поэтому брандмауэры такого типа обычно реализуются в виде списка правил, применяемых к значениям полей заголовка транспортного уровня.

*Шлюз уровня коммутации* – защита реализуется в плоскости управления (на уровне сигнализации) путем разрешения или запрета тех или иных соединений.

Для увеличения надежности защиты виртуальных соединений (каналов и трактов) возможно использование более одной пары агентов защиты и более одного соединения защиты. В данном случае формируется *топология соединений защиты*, в основе которой заложен принцип *вложения* и *не пересечения* соединений защиты вдоль всего маршрута между УИ и УП (или конечными системами пользователей). Пример принципа вложения и не пересечения соединений защиты приведен на рисунке 1.8. В данном случае защита виртуального канала, организованного между конечными системами, осуществляется четырьмя соединениями защиты и восьмью агентами защиты (*SA*1– *SA*8). Причем, каждое соединение не знает о существовании других соединений и не заботится о том, какую службу защиты последние обеспечивают. То есть, *соединения защиты абсолютно независимы друг от друга*. Данный подход позволяет применять многочисленные стратегии и тактики защиты различных участков сети. Например, соединение защиты между агентами *SA*1и *SA*8 обеспечивает аутентификацию между конечными системами. Независимо от данного соединения соединение между *SA*2и *SA*7 обеспечивает конфиденциальность, а *SA*2*, SA*3*, SA*4 и *SA*4*, SA*5*, SA*6 достоверность данных.



Каждое соединение защиты можно представить в виде сегмента

,

где *k* – порядковый номер соединения защиты; *i, j* – порядковые номера агентов защиты.

Для рисунка 1.8 соединения защиты можно записать соответствующими сегментами:

;

;

;

.

В свою очередь второй сегмент оказывается вложенным в первый. То есть, в символьной форме это выглядит следующим образом:

.

Не пересечение сегментов  и можно представить в виде:

.

Учитывая, что  вложены в , то получим:

.

Окончательная символьная запись топологии соединений защиты, представленная на рисунке 1.8, выглядит следующим образом:

.

Из рисунка 1.8 и полученного выражения и видно, что данная топология соединений защиты виртуального канала между конечными системами имеет три уровня вложения.

Таким образом:

* *принцип вложения и не пересечения соединений защиты;*
* *предельное количество уровней вложения ( для технологии ATM до 16 уровней)*

*являются единственными ограничениями организации топологии соединений защиты для одного виртуального соединения (канала либо тракта).*

В тоже время, для топологии защиты, изображенной на рисунке 1.8, соединение между агентами *SA*3и *SA*5не возможно, так как нарушается принцип не пересечения.

Таким образом, ***топология соединений защиты реализует профиль защиты пользователя, который является распределенным по сети****.*

Выбор топологии соединений защиты во многом определяется требованиями пользователей к степени защищенности передаваемой информации и ресурсными возможностями самой сети обеспечить данные требования.

## Контрольные вопросы

1. Приведите характеристики основных нарушений передачи информации через телекоммуникационные системы.
2. Почему нарушения в служебных плоскостях (менеджмента и управления) затрудняют, а порой делают невозможным функционирование пользовательской плоскости?
3. Дайте определения следующих свойств информации:
	* конфиденциальность;
	* доступность;
	* целостность;
	* аутентичность.
4. Какие нарушения относятся к группе активных и какие свойства информации они нарушают?
5. Назовите основное назначение сервисных служб и соединений защиты информации.
6. Какие функции выполняют брандмауэры?
7. Какие функции выполняет прокси – сервер?
8. Какие функции выполняют следующие устройства: фильтрующий маршрутизатор; шлюз уровня коммутации?
9. Какие ограничения накладываются на организацию топологии соединений защиты?
10. Перечислите основные функции протокола обмена сообщениями защиты.

# 2 криптографические системы

## 2.1 Криптосистема с одним ключом

На рисунке 2.1 представлена модель *криптосистемы* (шифрование и дешифрование), которую часто называют *традиционной, симметричной или с одним ключом*.



Пользователь 1 создает *открытое сообщение* ,

элементами которого являются символы конечного алфавита. Для шифрования открытого сообщения X генерируется *ключ шифрования* .

С помощью *алгоритма шифрования* формируется *шифрованное сообщение*

.

Формальное представление алгоритма шифрования выглядит следующим образом: .

Данная запись означает, что *Y* формируется путем применения алгоритма шифрования *E* к открытому сообщению *X* при использовании ключа шифрования *K*.

Шифрованное сообщение *Y* передается по каналу либо тракту связи к пользователю 2. Ключ шифрования также передается пользователю 2 по защищенному (секретному) каналу связи для дальнейшего дешифрования принятого сообщения *Y*.

Общий вид математической записи процедуры дешифрования выглядит следующим образом: .

Приведенная модель предусматривает, что ключ шифрования генерируется там же, где само сообщение. Однако, возможно и другое решение создания ключа – ключ шифрования создается третьей стороной (центром распределения ключей), которой доверяют оба пользователя. В данном случае за доставку ключа обоим пользователям ответственность несет третья сторона (рисунок 2.2). Вообще говоря, данное решение противоречит самой сущности криптографии – обеспечение секретности передаваемой информации пользователей.



Криптосистемы с одним ключом используют принципы подстановки (замены), перестановки (транспозиции) и композиции. При *подстановке* отдельные символы открытого сообщения заменяются другими символами. Шифрование с применением принципа *перестановки* подразумевает изменение порядка следования символов в открытом сообщении. С целью повышения надежности шифрования шифрованное сообщение, полученное применением некоторого шифра, может быть еще раз зашифровано с помощью другого шифра. Говорят, что в данном случае применен *композиционный* подход. Следовательно, *симметричные криптосистемы (с одним ключом) можно классифицировать на системы, которые используют шифры подстановки, перестановки и композиции.*

## 2.2 Криптосистемы с открытым ключом

Если пользователи при шифровании и дешифровании используют разные ключи *K*Ои *K*З, то есть: , ,

то криптосистему называют *асимметричной*, *с двумя ключами* или *с открытым ключом.*

Алгоритмы криптографии с открытым ключом в отличие от подстановок и перестановок используют математические функции.

На рисунке 2.3 представлена модель криптосистемы с открытым ключом, которая обеспечивает конфиденциальность передаваемой информации между пользователями.



Получатель сообщения (пользователь 2) генерирует *связанную пару ключей*:

* *K*О– открытый ключ, который публично доступен и, таким образом, оказывается доступным отправителю сообщения (пользователь 1);
* *K*С – секретный, личный ключ, который остается известным только получателю сообщения (пользователь 1).

Пользователь 1, имея ключ шифрования *K*О, с помощью алгоритма шифрования  формирует шифрованный текст .

Пользователь 2, владея секретным ключом *K*с, имеет возможность выполнить обратное преобразование .

Для обеспечения аутентификации необходимо использовать криптосистему, изображенную на рисунке 2.4.



В этом случае пользователь 1 готовит сообщение пользователю 2 и перед отправлением шифрует это сообщение с помощью личного ключа *K*С. Пользователь 2 может дешифрировать это сообщение, используя открытый ключ *K*О. Так как, сообщение было зашифровано личным ключом отправителя, то оно может выступать в качестве *цифровой подписи*. Кроме того, в данном случае невозможно изменить сообщение без доступа к личному ключу пользователя 1, поэтому сообщение решает так же задачи идентификации отправителя и целостности данных.

Для обеспечения аутентификации и конфиденциальности с открытым ключом необходимо использовать криптосистему, изображенную на рисунке 2.5. В данном случае пользователь 1 с помощью личного ключа  шифрует сообщение. Тем самым обеспечивает цифровую подпись. Затем с использованием открытого ключа  пользователя 2 шифрует сообщение, предназначенное для пользователя 2. Так как шифрованное сообщение может дешифрировать только пользователь 2 личным ключом , то это обеспечивает конфиденциальность передаваемой информации.

Таким образом, *криптосистемы с открытым ключом характеризуются тем, что при шифровании и дешифровании используют два ключа, один из которых остается в личном пользовании (секретный), а второй открыт для всех пользователей.*

Из вышеизложенного следует, что криптосистемы с открытым ключом должны удовлетворять следующим условиям:

1. для пользователя процесс генерирования открытого и личного ключей не должен вызывать вычислительных трудностей;



1. для пользователя, отправляющего сообщение, процесс шифрования с помощью открытого ключа не должен вызывать вычислительных трудностей;
2. процесс дешифрования, полученного шифрованного сообщения, с помощью личного ключа не должен вызывать вычислительных трудностей;
3. для противника должны быть значительные вычислительные трудности восстановления личного ключа из имеющего открытого ключа;
4. для противника должны быть значительные вычислительные трудности восстановления оригинального сообщения из имеющегося открытого ключа и шифрованного сообщения.

Таким образом, практическая реализация перечисленных условий сводятся к нахождению односторонней функции со следующими свойствами:

* +  - вычисляется легко, если известны *K*О и *X*;
	+  - вычисляется легко, если известны *K*С и *Y*;
	+  - практически не поддается вычислению, если *Y* известно, а *K*С – нет.

С подробным описанием различных систем криптографии можно познакомиться в [7].

## 2.3 Распределение открытых ключей

На сегодняшний день известны следующие методы распределения открытых ключей [7]:

* индивидуальное публичное объявление открытых ключей пользователями;
* использование публично доступного каталога открытых ключей;
* участие авторитетного источника открытых ключей;
* сертификаты открытых ключей.

Рассмотрим каждый из перечисленных методов.

При *индивидуальном публичном объявлении открытых ключей* любая сторона, участвующая в обмене сообщениями (X), может предоставить свой открытый ключ (*K*О) любой другой стороне. Недостатком данного подхода является невозможность обеспечить аутентификацию отправителя открытого ключа (*K*О). То есть, при данном подходе у нарушителя появляется возможность фальсификации пользователей (рисунок 1. 3 г)).

*Использование публично доступного каталога открытых ключей* позволяет добиться более высокой степени защиты информации и пользователей сети. В данном случае за ведение и распространение публичного каталога должна отвечать надежная организация (уполномоченный объект) (рисунок 2.6). При этом должны соблюдаться следующие правила.

1. Пользователи должны регистрировать свои открытые ключи в публичном каталоге, который ведет уполномоченный объект.
2. Регистрация должна проходить либо по заранее защищенным каналам связи, либо при личной (физической) явке пользователей на уполномоченный объект.
3. Уполномоченный объект должен периодически публиковать каталог открытых ключей. Например, в виде печатной продукции (книга, газета и тому подобное) либо в электронной версии (размещение на собственном сервере).

Недостатком данного подхода является следующее. Если нарушителю удастся изменить записи, хранящиеся в каталоге открытых ключей, то он сможет авторитетно выдавать фальсифицированные открытые ключи и, следовательно, выступать от имени любого из участников обмена данными и читать сообщения, предназначенные любому пользователю.

*Участие авторитетного источника открытых ключей* представлено на рисунке 2.7. Обязательным условием данного варианта распределения открытых ключей пользователей является условие, что авторитетный источник открытых ключей имеет свой секретный ключ, и каждый пользователь знает его открытый ключ. При этом выполняется следующий порядок действий (номера, проставленные у стрелочек, совпадают с последовательностью действий участников обмена сообщениями):



1. Пользователь 1 посылает запрос авторитетному источнику открытых ключей о текущем значении открытого ключа пользователя 2. При этом указывается дата и время запроса (д. вр.).
2. Авторитетный источник, используя свой секретный ключ , шифрует и передает сообщение пользователю 1 , в котором содержится следующая информация:
*  - открытый ключ пользователя 2;
* д. вр. - дата и время отправки сообщения.
1. Пользователь 1, используя , шифрует и передает пользователю 2 шифрованное сообщение , содержащее:
* *ID*1 – идентификатор отправителя (пользователь 1);
* *N*1 - уникальную метку данного сообщения.

4, 5. Пользователь 2, получив шифрованное сообщение , дешифрирует его с помощью своего секретного ключа   и в соответствии с идентификатором *ID*1, аналогично с пунктами 1 и 2 выше перечисленных действий получает от авторитетного источника открытый ключ пользователя 1 .

1. Пользователь 2, используя , посылает пользователю 1 шифрованное сообщение , где *N*2 - уникальная метка данного сообщения.
2. Пользователь 1 шифрует с помощью открытого ключа  сообщение *Y*, предназначенное пользователю 1 и передает .

Приведенный вариант распределения открытых ключей имеет некоторые недостатки:



* каждый раз, когда пользователь намерен передать информацию новому адресату, то он должен обращаться к авторитетному источнику с целью получения открытого ключа;
* каталог имен и открытых ключей, поддерживаемый авторитетным источником, является привлекательным местом для нарушителя передачи информации пользователей.

На рисунке 2.8 представлен сценарий распределения открытых ключей с применением *сертификатов открытых ключей*. Обязательным условием данного варианта распределения открытых ключей пользователей является условие, что авторитетный источник сертификатов имеет свой секретный ключ , и каждый пользователь знает его открытый ключ . При этом выполняется следующий порядок действий (номера, проставленные у стрелочек, совпадают с последовательностью действий участников обмена сообщениями):

1. Пользователь 1 генерирует пару ключей  (соответственно, открытый и секретный) и по защищенному каналу связи обращается к авторитетному источнику сертификатов с целью получения сертификата.
2. Авторитетный источник шифрует с помощью своего секретного ключа сертификат  и выдает его пользователю 1. Сертификат содержит:
*  - открытый ключ пользователя 1 (данный ключ пользователь 1 сам сгенерировал и передал авторитетному источнику для сертификации);
* *ID*П1 - идентификатор пользователя 1;
* *T*П1 - срок действия сертификата пользователя.



1. Пользователь 1 пересылает свой сертификат , полученный от авторитетного источника, пользователю 2. Последний, зная открытый ключ авторитетного источника сертификатов , имеет возможность прочитать и удостовериться, что полученное сообщение является сертификатом .
2. 4, 5, 6. Пользователь 2 выполняет аналогичные действия, которые были выполнены пользователем 1 в пунктах 1, 2 и 3. То есть получает от авторитетного источника сертификат . Пересылает его пользователю 1. Последний, зная открытый ключ авторитетного источника сертификатов , имеет возможность прочитать и удостовериться, что полученное сообщение является сертификатом

.

В результате перечисленных действий пользователи обменялись открытыми ключами и готовы к передаче и приему пользовательских сообщений.

## 2.4 Применение криптосистемы с открытым ключом для распределения секретных ключей

На сегодняшний день существует несколько подходов применения криптосистемы с открытым ключом для распределения секретных ключей [7]. Рассмотрим некоторые из них.

*Простое распределение секретных ключей* состоит в выполнении следующих действий:

1. Пользователь 1 генерирует пару ключей , соответственно, открытый и секретный.
2. Пользователь 1 передает пользователю 2 сообщение , где  *–* идентификатор пользователя 1.
3. Пользователь 2, получив сообщение  от пользователя 1, так же генерирует свою пару ключей .
4. Пользователь 2, используя открытый ключ пользователя 1, шифрует и передает сообщение  пользователю 1.
5. Пользователь 1 уничтожает свой секретный ключ , а пользователь 2 уничтожает открытый ключ пользователя 1 .

Таким образом, оба пользователя имеют сеансовый (секретный) ключ и могут использовать его для передачи информации, защищенной традиционным шифрованием. По окончании сеанса передачи информации ключ  уничтожается. Однако данный подход уязвим для активных нарушений. Действительно, если нарушитель имеет возможность внедрения в соединение между пользователями, то, выполняя следующие действия (рисунок 2.9), он будет иметь возможность знать секретный (сеансовый) ключ.

1. Пользователь 1 генерирует пару ключей  и передает пользователю 2 сообщение .
2. Нарушитель перехватывает сообщение , создает собственную пару ключей  и передает пользователю 2 сообщение .
3. Пользователь 2, получив сообщение , генерирует свою пару ключей , шифрует (используя открытый ключ нарушителя ) и передает сообщение  пользователю 1.
4. Нарушитель перехватывает сообщение , дешифрирует его , определяет сеансовый ключ  и передает пользователю 2 сообщение .

В результате оба пользователя имеют сеансовый ключ , однако не будут подозревать, что он тоже известен и нарушителю.



Сценарий *распределения секретных ключей с обеспечением конфиденциальности и аутентичности* изображен на рисунке 2.10 и состоит в выполнении следующих действий.

1. Пользователи генерируют пары ключей, соответственно , , и обмениваются между собой открытыми ключами  и .
2. Пользователь 1, используя , передает пользователю 2 сообщение , содержащее: свой идентификатор - *ID*П1;  - уникальная метка данного сообщения.
3. Пользователь 2, используя , передает пользователю 1 сообщение , содержащее  и - уникальные метки данного сообщения. Наличие метки  убеждает пользователя 1 в том, что только пользователь 2 мог дешифрировать сообщение .
4. Пользователь 1, используя , передает пользователю 2 сообщение , содержащее уникальную метку . Данное сообщение выполняет функцию подтверждения для пользователя 2, что его респондентом является пользователь 1.
5. Пользователь 1 генерирует секретный (сеансовый) ключ , который дважды шифруется с использованием: своего секретного ключа  и открытого ключа пользователя 2 . После выполнения процедуры шифрования сообщение  передается пользователю 2. Последний, имея открытый ключ пользователя 1 и свой секретный ключ, дешифрирует полученное сообщение.

В результате перечисленных действия оба пользователя имеют секретный (сеансовый) ключ .



## 2.5 Применение криптосистемы с открытым ключом для аутентификации пользователя со стороны автономного объекта

На рисунке 2.11 представлена структура телекоммуникационной системы, состоящая из удаленного объекта и пользователя. Удаленный объект в автономном режиме выполняет некоторые функции, например, осуществляет сбор информации *J*. Через неопределенное время пользователь по каналу связи передает автономному объекту некоторое сообщение, например команду *K* – «Выйти на связь и передать собранную информацию *J*». Приведенную систему часто называют системой дистанционного управления объектом.



В подобных системах возникает задача аутентификации пользователя со стороны автономного объекта. Действительно, если не принять соответствующих мер по организации защищенного канала доступа к автономному объекту, то нарушитель, используя перехват сообщения *K*, может несанкционированно управлять автономным объектом.



На рисунке 2.12 приведен сценарий, реализующий надежную аутентификацию пользователя со стороны автономного объекта, который содержит два этапа и состоит в выполнении следующих процедур.

1 Этап – предварительная настройка параметров объекта и пользователя. Данный этап выполняется один раз перед началом автономного функционирования объекта. Пользователь генерирует и размещает в оперативной памяти автономного объекта идентификатор *ID* и временной параметр .

2 Этап: - сеанс связи пользователя с объектом:

1. Пользователь по открытому каналу связи посылает автономному объекту сигнал *S*, который приводит автономный объект в активное состояние – выйти на связь с пользователем.
2. Автономный объект генерирует сеансовую, связанную пару ключей , включает таймер, фиксирует время начала сеанса  и передает пользователю свой открытый ключ . Значения открытого  и секретного  ключей имеют случайный характер.
3. Пользователь генерирует свою сеансовую, связанную пару ключей , значения которых тоже имеют случайный характер. Используя открытый ключ объекта, передает ему сообщение , содержащее общий идентификатор *ID* и свой открытый ключ .
4. Автономный объект, используя свой секретный ключ , дешифрирует принятое сообщение от пользователя . По таймеру фиксирует время принятия сообщения . Рассчитывает  и принимает решение: если , то конец связи с пользователем. В противном случае проверяет: идентификатор *ID*, полученный в сообщении от пользователя, совпадает с собственным идентификатором? Если нет, то конец связи. Иначе – используя открытый ключ пользователя , передает ему сообщение , содержащее запрос *X* на выполнение команды *K*, и фиксирует время .
5. Пользователь:
* используя свой секретный ключ , дешифрирует принятое сообщение ;
* используя открытый ключ объекта , передает удаленному объекту сообщение , содержащее команду управления *K* и новый идентификатор, который будет использован в будущем сеансе связи (значение нового *ID* имеет случайный характер);
* фиксирует в своей оперативной памяти значение нового идентификатора;
* уничтожает свою сеансовую пару ключей  и открытый сеансовый ключ объекта .
1. Объект дешифрирует принятое сообщение. Рассчитывает  и принимает решение: если , то конец связи с пользователем. В противном случае размещает в оперативной памяти новый идентификатор *ID*, уничтожает свою пару ключей  и выполняет команду *K*.

Таким образом, каждый сеанс связи пользователя с удаленным объектом характеризуется использованием «своих» сеансовых ключей и «своего» сеансового идентификатора. Значения данных параметров имеет случайный характер, что гарантирует надежную аутентификацию пользователя со стороны удаленного объекта.

## Контрольные вопросы

1. Изобразите модель криптосистемы с одним ключом и поясните принцип ее работы.
2. Изобразите модель криптосистемы с одним ключом и участием центра распределения ключей и поясните принцип ее работы.
3. Изобразите модель криптосистемы с открытым ключом, обеспечивающей конфиденциальность передаваемой информации. Поясните принцип работы данной модели.
4. Изобразите модель криптосистемы с открытым ключом, обеспечивающей аутентификацию передаваемой информации. Поясните принцип работы данной модели.
5. Изобразите модель криптосистемы с открытым ключом, обеспечивающей конфиденциальность и аутентификацию передаваемой информации. Поясните принцип работы данной модели.
6. Перечислите основные требования, которым должны удовлетворять криптосистемы с открытым ключом.
7. Поясните, в чем состоит суть индивидуального публичного объявления открытых ключей пользователями?
8. Изобразите сценарий распределения открытых ключей с использованием публично доступного каталога открытых ключей.
9. Изобразите сценарий распределения открытых ключей с участием авторитетного источника открытых ключей.
10. Поясните, в чем состоит суть сертификации открытых ключей.
11. В чем суть простого распределения секретных ключей?
12. Поясните сценарий распределения секретных ключей с обеспечением конфиденциальности и аутентичности.
13. Изобразите сценарий применения криптосистемы с открытым ключом для аутентификации пользователя со стороны автономного объекта
14. Поясните, почему применение криптосистемы с открытым ключом гарантирует надежную аутентификацию пользователя со стороны автономного объекта,

# 3 общие критерии оценки безопасности информационных технологий

## 3.1 Целевая направленность общих критериев

В РФ нормативными документами по разработке систем защиты информации, средств вычислительной техники и автоматизированных систем являются Руководящие документы Гостехкомисси РФ. До недавнего времени Руководящие документы разрабатывались с учетом международных документов конца 80-х, начала 90-х годов. В июне 1999 года Международной организацией по стандартизации (International Organization Standardization, ISO) при содействии ряда стран был принят стандарт «Критерии оценки безопасности информационных технологий» [5], [6], [7] (в научной литературе и в литературе по стандартизации исторически закрепилось название «Общие критерии» (ОК)).

В 2001 г. под эгидой Гостехкомисси России был подготовлен стандарт ГОСТ Р ИСО/МЭК 15408-2001 [8], который после соответствующей апробации вступит в силу с 2004 г.. Данный стандарт является механизмом, предназначенным для разработки нормативных документов, позволяющих оценивать средства безопасности информационные технологий (ИТ) определенного назначения.

Для обеспечения действия данного стандарта ожидается выпуск целого ряда организационно-методологических документов, определяющих порядок разработки профилей защиты их оценки, регистрации и применения.

ОК направлены на обеспечение конфиденциальности, целостности и доступности информации пользователей. ОК дают возможность выработки системы требований, критериев и показателей для оценки уровня безопасности информационных технологий.

ОК предназначены для пользователей, разработчиков и специалистов, обеспечивающих оценку характеристик безопасности систем ИТ.

## 3.2 Концепция общих критериев

## 3.3 Профили защиты

Профиль защиты предназначен для сертификации средств защиты информации продуктов и систем ИТ и получения сопоставимых оценок их безопасности. Профили защиты служат также основой для разработки разделов требований безопасности информации (заданий по безопасности) в ТЗ (ТТЗ) на конкретные изделия ИТ.

## 3.4 Нормативные документы оценки безопасности информационных технологий в Российской Федерации

# 4 защита информации в сетях с технологией ATM

## 4.1 Обмен информацией между агентами защиты

Установление и поддержание соединений защиты на сетях ATM достаточно сложный и ответственный процесс, который состоит из двух этапов и базируется на протоколе обмена сообщениями защиты (Security Message Exchange, SME) и передаче специальных ячеек защиты OAM (рисунок 1.9).



Протокол обмена сообщениями защиты SME используется для:

* аутентификации агентов между собой;
* согласования служб защиты между агентами защиты;
* установления соединения защиты.

Возможно два варианта реализации протокола SME.

1. В плоскости управления (с использованием канала сигнализации).
2. В плоскости пользователя (с использованием канала данных, установленного сигнализацией ранее).

В первом случае агенты защиты добавляют к сигнальному сообщению информационный элемент служб защиты (Security Services Information Element, SSIE).

Во втором случае протокол SME реализуется через установленное соединение между пользователями сети ATM. При этом на время действия протокола обмена сообщениями защиты передача данных пользователей блокируется.

В случае если часть элементов сети не поддерживает протокол SME с использованием сигнализации, то допускается комбинированное применение обоих вариантов. То есть, часть сети применяет протокол SME в плоскости управления (сигнализации), а другая в плоскости пользователей.

Передача ячеек защиты OAM используется только для поддержания соединений защиты и применяется после завершения протокола SME.

## 4.1 Защита информации в плоскости пользователя

## 4.1 Сервисные службы защиты информации плоскости пользователя

Аутентификация плоскости пользователя или аутентификация объекта – эта служба отвечает за определение идентичности вызывающего и/или вызываемого пользователей оригиналу. Аутентификация является основной для установления надежных соединений. Данная служба является базовой для остальных служб защиты.

Аутентификация может быть как *взаимной (симметричной)*, так и *односторонней (асимметричной)*. В первом случае оба пользователя аутентифицируются друг для друга. При односторонней аутентификации только один пользователь аутентифицируется для другого.

Аутентификация обеспечивается через обмен информацией между агентами безопасности, которые обмениваются между собой сообщениями безопасности (Security Message Exchange, SAsme). В свою очередь, обмен сообщениями безопасности возможен либо в плоскости сигнализации, либо в плоскости пользователя. Рисунки 3.1 и 3.2, соответственно, показывают уровневые модели аутентификации основанной на сигнализации и полосовой (функционирующей непосредственно в полосе данных).



Конфиденциальность плоскости пользователя обеспечивается криптографическими механизмами, которые защищают данные «пользователя» в виртуальных каналах и трактах от несанкционированного вскрытия. Данная служба функционирует на уровне ячеек АТМ. При этом шифруется только пользовательская часть ячейки ATM.Заголовок ячейки передается незашифрованным.

Достоверность данных или «оригинальная аутентификация данных» плоскости пользователя обеспечивается механизмом, который позволяет определять умышленную модификацию данных. Данная служба функционирует между пользователями на уровне AAL (для AAL ѕ и AAL 5) и может быть реализована в двух вариантах:

* + 1. достоверность данных без защиты от повторной модификации;
		2. достоверность данных с защитой от повторной модификации.

В первом случае источник перед передачей добавляет криптографическую характеристику в конце каждой AAL SDU. Эта характеристика вычисляется по всем AAL SDU. Этот вариант реализации достоверности данных полезен для протоколов верхнего уровня, которые обеспечивают свою собственную нумерацию последовательности (например TCP), без добавления заголовка, требуемого для дублирования данной функции на уровне AAL.

Второй вариант реализации достоверности данных детектирует и отбраковывает «старые» или «переупорядоченные» AAL-SDU. Это достигается сначала добавлением номера последовательности в конце каждой AAL-SDU, а затем вычислением характеристики для совокупности AAL-SDU, включая номера последовательности. Это характеристика, которая защищает и AAL-SDU и номер последовательности, затем добавляется к общей AAL-SDU (которая включает номер последовательности). Этот метод обеспечивает защиту приложений ATM, которые не осуществляют свою собственную нумерацию последовательности.

Контроль доступа плоскости пользователя – это применение набора правил для запроса услуги. Эти правила могут зависеть от атрибутов вызывающего объекта, таких как идентичность, атрибутов соответствующих параметров, таких как целевой адрес, системных атрибутов, таких как время и история предыдущих запросов данным или другими объектами клиента. Правила контроля доступа могут быть предикатом, сформированным всеми этими атрибутами. Если предикат удовлетворен, то запрашиваемая служба (услуга) предоставляется, если предикат не удовлетворен, то запрашиваемая служба не предоставляется.

Контроль доступа плоскости пользователя требует механизмов для транспортировки информации контроля доступа, используемой во время установления соединения, так как механизмы внутри компонентов АТМ используют эту информацию, чтобы определить нужно ли предоставлять доступ к соединению. Контроль доступа плоскости пользователя может основываться на метках защиты (например, стандартные метки защиты [10]), идентичности источника или получателя, времени дня, типе службы, полях вышележащего протокола (например, протокол Интернет), или на других параметрах, которые могут быть определены во время установления соединения.

Контроль доступа плоскости пользователя обеспечивается на уровне АТМ.

## 4.2 Службы поддержки

Перечисленные в 3.1 службы защиты информации, которые часто называют *базисом служб защиты*. Помимо данного базиса существуют также *службы поддержки*, которые необходимы для обеспечения масштабируемости и повышения эффективности базиса служб защиты (Рисунок 3.1):

* обмен сообщениями защиты и согласование опций защиты
* обмен ключами
* обновление ключей
* инфраструктура сертификации.



Обмен сообщениями защиты и согласование. Для того чтобы предоставить большинство служб, описанных выше, должны передаваться сообщения между вовлеченными агентами защиты (SA). Данная спецификация описывает два метода обмена сообщениями защиты – обмен сообщениями по сигнализации UNI 4.0 и обмен сообщениями in-band (т.е. обмен сообщениями защиты по уместному виртуальному каналу плоскости пользователя).

Эти методы обмена сообщениями также обеспечивают механизм для согласования опций защиты. Т.к. требования защиты различные для разных организаций, важно обеспечить ассортимент служб защиты, алгоритмов и длительностей ключей, которые соответствуют широкой области потребностей защиты. Кроме того, законы экспорта и/или импорта некоторых стран накладывают ограничения, через которые зашифрованные продукты могут импортироваться/экспортироваться. По этим причинам механизмы защиты АТМ поддерживают множественные службы защиты, алгоритмы и длительности ключей. Для того чтобы агент защиты соответствовал общим параметрам защиты (таким как алгоритмы и длительности ключей), эти методы обмена сообщениями защиты обеспечивают согласование этих параметров как часть процедуры установления защиты для VC.

Обмен ключами – это механизм, посредством которого два агента защиты обмениваются секретными ключами для служб конфиденциальности и/или достоверности. Для того чтобы противостоять атакам типа «человек в середине», обмен ключом обычно связан со службой аутентификации. Это может быть осуществлено путем включения «конфиденциального» ключа внутри параметров обмена потоков аутентификации.

Также как аутентификация, обмен ключом представлен и для симметричных (секретный ключ) и для асимметричных (публичный ключ) алгоритмов. Кроме того, обмен ключом может быть двунаправленным (два пути) и однонаправленным (один путь).

Обновление ключа сеанса. Ключи сеанса – это ключи, используемые напрямую для обеспечения служб конфиденциальности и достоверности плоскости пользователя через виртуальные каналы АТМ. Так как скорость данных может быть высокой в VC, крайне необходимо периодически менять ключи, чтобы избежать «повторного использования ключа». Данная спецификация определяет службу обновления ключа сеанса, которая обеспечивает эту возможность.

Эта служба представлена в двух фазах – фаза обмена ключом сеанса и фаза смены ключа сеанса. Фаза обмена ключом сеанса использует «мастер ключ», которым обмениваются при установлении соединения (используя службу обмена ключом), чтобы зашифровать новый ключ сеанса. При приеме зашифрованного ключа сеанса, приемник расшифровывает ключ сеанса, используя общий мастер ключ, и сохраняет его для второй фазы – смены ключа.

Инфраструктура сертификации. В криптосистеме публичного ключа каждая сторона (агент защиты) Х имеет пару ключей: один – публично известный – «публичный ключ» Х (РКХ), и другой, известный только Х – «приватный ключ» Х (SKX). Для того, чтобы сторона А послала секретную информацию стороне В (или чтобы сторона могла проверить характеристику, переданную стороной В), А должна получит публичный ключ В, РКВ. Хотя РКВ – публичный, по определению, никакая сторона Х не должна иметь возможность заменить РКВ  на другой (например РКХ). Чтобы предотвратить такого рода воздействия, публичным ключом можно обмениваться в форме «сертификата».

Сертификат содержит имя стороны, ее публичный ключ и некоторую дополнительную информацию и обозначается доверяющей стороной, «орган сертификации» (СА). Эта характеристика жестко связывает публичный ключ с предметной стороной. Любая сторона, имеющая доступ к публичному ключу СА может проверять подлинность сертификата (путем проверки характеристики СА в сертификате) и использовать публичный ключ, который сертифицирован. Один раз отмеченные сертификаты могут передаваться через коммутаторы сообщений не поддерживающие защиту.

## 4.2 Защита информации плоскости управления

## 4.2 Сервисные службы защиты информации плоскости управления

Плоскость контроля – это механизм, который позволяет устройствам конфигурировать сеть, чтобы добиться определенных целей (например, установить коммутируемый виртуальный канал). Так как сообщение плоскости контроля могут влиять на состояние и работоспособность сети, их защита крайне важна.

В данной спецификации защиты определен механизм сигнализации, который может обеспечить устойчивую криптографическую достоверность данных с защитой от повторного воспроизведения/переупорядочивания. Этот механизм позволяет объектам плоскости контроля АТМ проверять источник и содержимое сигнальных сообщений до того, как этот источник выделяется по запросу.

Аутентификация и достоверность плоскости контроля– это службы защиты АТМ, которые увязывают сообщения сигнализации АТМ с его источником. Путем создания такой увязки, получатель сообщения может конфиденциально проверить, что сообщение было отправлено именно заявленным источником. Это обеспечивает механизм, который снижает количество воздействий. Например, воздействия, направленные на разрыв активного соединения путем скрытого ввода сообщений RELEASE или DROP PARTY, могут быть предотвращены, если для канала сигнализации обеспечена аутентификация. Эта служба также защищает и от умышленной модификации. В данной спецификации определен механизм аутентификации достоверности плоскости контроля между соседними объектами сигнализации. Используемый механизм идентичен механизму, применяемому для достоверности данных с защитой от повторного воспроизведения/переупорядочивания для плоскости пользователя.

## 4.3 Защита информации плоскости менеджмента

## 4.3 Сервисные службы защиты информации плоскости менеджмента

# приложение 1 англо-русский словарь

A

|  |  |  |
| --- | --- | --- |
|  | Access controlAuthentication | Контроль доступаАутентификация |

C

|  |  |  |
| --- | --- | --- |
|  | Certification authorityCiphertext interfaceConfidentialityCryptographic system | Орган сертификацииИнтерфейс зашифрованного текстаКонфиденциальностьКриптографическая система |

D

|  |  |  |
| --- | --- | --- |
| DES DHDSADSS | Digital signatureData Encryption StandardDiffie-HellmanDigital Signature AlgorithmDigital Signature Standard | Цифровая подписьСтандарт шифрования данныхАлгоритм совпадения ключаАлгоритм цифровой подписиСтандарт цифровой подписи |

E

|  |  |  |
| --- | --- | --- |
| ECBECCECKAS-DH ECDSA-likeESIGN | Electronic CodeBookElliptic Curve CryptosystemElliptic Curve Key Agreement Scheme - Diffie-HellmanElliptic Curve Digital Signature AlgorithmEfficient digital SIGNature scheme | Электронная книга кодовКриптосистема с эллиптической характеристикойСхема совпадения ключей с эллиптической характеристикой Diffie-Hellman Алгоритм цифровой подписи с эллиптической характеристикойЭффективная схема цифровой подписи |

F

|  |  |  |
| --- | --- | --- |
| FEAL | Fast Data Encipherment Algorithm | Алгоритм быстрого шифрования данных |

H

|  |  |  |
| --- | --- | --- |
| HMAC H-SHA and H-SHA-1 | Hashed Message Authentication CodeHMAC using the SHA-1 hash algorithm | Кэшированный код аутентификации сообщенийHMAC, использующий кэш-алгоритм SHA -1 |

I

|  |  |  |
| --- | --- | --- |
| ISO | In-Band Message ExchangeInitiatorIntegrityInternational Organization Standardization | Обмен сообщениями в полосеИнициаторДостоверностьМеждународная организация по стандартизации |

K

|  |  |  |
| --- | --- | --- |
|  | KeyKey Exchange | КлючОбмен ключом |

L

|  |  |  |
| --- | --- | --- |
| LIJ | Leaf Initiated Join | Наращивание, инициируемое получателем информации |

M

|  |  |  |
| --- | --- | --- |
| MAC | Message Authentication Code | Код аутентификации сообщений |

N

|  |  |  |
| --- | --- | --- |
| NIST | (U.S.) National Institute of Standards and Technology | (США) Национальный институт стандартов и технологий |

P

|  |  |  |
| --- | --- | --- |
|  | Packet-filtering RouterPlaintext InterfacePrivate KeyProxy ServerPublic Key | Маршрутизатор фильтрующий пакетыИнтерфейс обычного текстаПриватный ключПрокси - серверКлюч общего пользования |

R

|  |  |  |
| --- | --- | --- |
|  | Replay PreventionResponder | Предотвращение повторного воспроизведенияОтвечающий |

S

|  |  |  |
| --- | --- | --- |
| SASASSHA-1SMESSCOPSSIE | Security AgentSecurity AssociationSecurity Association SectionSecure Hash Algorithm (Revision 1)Secret KeySecurity Message ExchangeSecurity NegotiationService Specific Connection Oriented ProtocolSignaling-Based Message ExchangeSecurity Services Information Element | Агент защитыСоединение защитыСекция защиты связиЗащитный кэш-алгоритм (первая редакция)Секретный ключОбмен сообщением защитыСогласование защитыСлужебно-ориентированный протокол с установлением соединенияОбмен сообщениями, основанный на сигнализацииИнформационный элемент служб защиты |

# Список сокращений

|  |  |
| --- | --- |
| ВКВТИВКИВТИТМСЭ-ТОКТПСУИУКУП | Виртуальный КаналВиртуальный ТрактИдентификатор Виртуального КаналаИдентификатор Виртуального ТрактаИнформационная Технологиясектор по стандартизации Телекоммуникаций Международного Союза ЭлектросвязиОбщие КритерииТракт Передачи СообщенияУзел-ИсточникУзел КоммутацииУзел-Получатель |

# список литературы

1. Федеральный закон «Об информации, информатизации и защите информации» принят Государственной Думой 25 января 1995 г. № 24 – ФЗ.
2. ГОСТ Р 50922-96. Защита информации. Основные термины и определения.
3. Новиков С.Н. Методы маршрутизации в цифровых широкополосных сетях связи: Ч. 1 / Учебное пособие. ⎯ Новосибирск: 2001.⎯ 84 с.: ил.
4. Новиков С.Н. Методы маршрутизации в цифровых широкополосных сетях связи: Ч. 2 / Учебное пособие. ⎯ Новосибирск: 2002.⎯ 62 с.: ил.
5. Evaluation Criteria for IT Security. Part 1: Introduction and general model. -- ISO/IEC 15408-1: 1999
6. Evaluation Criteria for IT Security. Part 2: Security functional requirements. -- ISO/IEC 15408-2: 1999
7. Evaluation Criteria for IT Security. Part 3: Security assurance requirements. -- ISO/IEC 15408-3: 1999
8. ГОСТ Р ИСО/МЭК 15408-2001. Методы и средства обеспечения безопасности. Критерии оценки безопасности ИТ (часть1, часть 2, часть3).
9. ATM Security Specification Version 1.0 ⎯ ATM Forum ⎯ af-sec-0100.000, february, 1999.
10. ATM Security Specification Version 2.0 ⎯ ATM Forum ⎯ af-sec-0100.002, february, 2002.
11. Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях. М.: КУДИЦ-ОБРАЗ, 2001 – 368 с.
12. ITU-T Recommendation X.509 «The Directory: Authentication Framework», 1993.
13. Interim Inter-switch Signaling Protocol (IISP) Specification v1.0 ⎯ ATM Forum ⎯ af-pnni-0026.000, december, 1994.