[ИНФОРМАЦИОННАЯ БЕЗОПАСТНОСТЬ]

[Институт ИИБС, Кафедра ИСКТ]

[Шумейко Е.В.]

КРИПТОГРАФИЧЕСКИЕ ОСНОВЫ БЕЗОПАСНОСТИ.

Основные понятия и определения

За несколько последних десятилетий требования к информационной безопасности существенно изменились. До начала широкого использования автоматизированных систем обработки данных безопасность информации достигалась исключительно физическими и административными мерами. С появлением компьютеров стала очевидной необходимость использования автоматических средств защиты файлов данных и программной среды. Следующий этап развития автоматических средств защиты связан с появлением распределенных систем обработки данных и компьютерных сетей, в которых средства сетевой безопасности используются в первую очередь для защиты передаваемых по сетям данных. В наиболее полной трактовке под средствами сетевой безопасности мы будем иметь в виду меры предотвращения нарушений безопасности, которые возникают при передаче информации по сетям, а также меры, позволяющие определять, что такие нарушения безопасности имели место. Именно изучение средств сетевой безопасности и связанных с ними теоретических и прикладных проблем, составляет основной материал книги.

Основные понятия и определения

Термины "безопасность информации" и "защита информации" отнюдь не являются синонимами. Термин "безопасность" включает в себя не только понятие защиты, но также и аутентификацию, аудит, обнаружение проникновения.

Перечислим некоторые **характерные проблемы**, связанные с безопасностью, которые возникают при использовании компьютерных сетей:

1. Фирма имеет несколько офисов, расположенных на достаточно большом расстоянии друг от друга. При пересылке конфиденциальной информации по общедоступной сети (например, Internet) необходимо быть уверенным, что никто не сможет ни подсмотреть, ни изменить эту информацию.
2. Сетевой администратор осуществляет удаленное управление компьютером. Пользователь перехватывает управляющее сообщение, изменяет его содержание и отправляет сообщение на данный компьютер.

Основные понятия и определения

3. Пользователь несанкционированно получает доступ к удаленному компьютеру с правами законного пользователя, либо, имея право доступа к компьютеру, получает доступ с гораздо большими правами.
4. Фирма открывает Internet-магазин, который принимает оплату в электронном виде. В этом случае продавец должен быть уверен, что он отпускает товар, который действительно оплачен, а покупатель должен иметь гарантии, что он, во-первых, получит оплаченный товар, а во-вторых, номер его кредитной карточки не станет никому известен.
5. Фирма открывает свой сайт в Internet. В какой-то момент содержимое сайта заменяется новым, либо возникает такой поток и такой способ обращений к сайту, что сервер не справляется с обработкой запросов. В результате обычные посетители сайта либо видят информацию, не имеющую к фирме никакого отношения, либо просто не могут попасть на сайт фирмы.

Основные понятия и определения

Рассмотрим основные понятия, относящиеся к информационной безопасности, и их взаимосвязь.

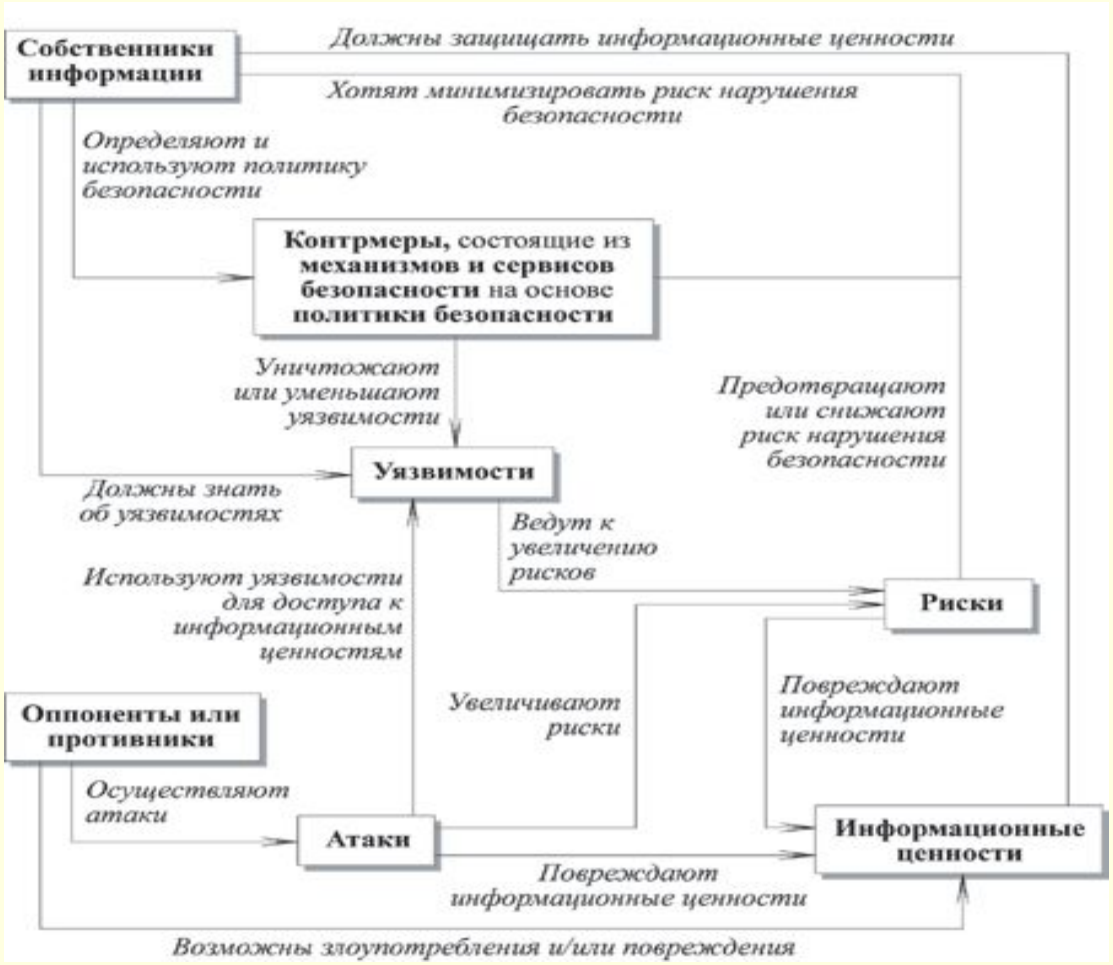
Собственник определяет множество **информационных ценностей**, которые должны быть защищены от различного рода *атак*. *Атаки* осуществляются *противниками* или *оппонентами*, использующими различные *уязвимости* в защищаемых ценностях. Основными нарушениями безопасности являются раскрытие информационных ценностей (потеря *конфиденциальности*), их неавторизованная модификация (потеря *целостности*) или неавторизованная потеря доступа к этим ценностям (потеря *доступности*).

Основные понятия и определения

Собственники информационных ценностей анализируют *уязвимости* защищаемых ресурсов и возможные *атаки*, которые могут иметь место в конкретном окружении. В результате такого анализа определяются *риски* для данного набора информационных ценностей. Этот анализ определяет выбор контрмер, который задается политикой безопасности и обеспечивается с помощью *механизмов* и *сервисов безопасности*. Следует учитывать, что отдельные *уязвимости* могут сохраниться и после применения *механизмов* и *сервисов безопасности*. ***Политика безопасности*** определяет согласованную совокупность *механизмов* и *сервисов безопасности*, адекватную защищаемым ценностям и окружению, в котором они используются.

Взаимосвязь понятий информационной безопасности

На рисунке показана взаимосвязь рассмотренных выше понятий информационной безопасности.



Основные понятия и определения

Дадим следующие определения:

Уязвимость - слабое место в системе, с использованием которого может быть осуществлена *атака*.
Риск - вероятность того, что конкретная *атака* будет осуществлена с использованием конкретной *уязвимости*. В конечном счете, каждая организация должна принять решение о допустимом для нее уровне *риска*. Это решение должно найти отражение в политике безопасности, принятой в организации.
Политика безопасности - правила, директивы и практические навыки, которые определяют то, как информационные ценности обрабатываются, защищаются и распространяются в организации и между информационными системами; набор критериев для предоставления *сервисов безопасности*.
Атака - любое действие, нарушающее безопасность информационной системы. Более формально можно сказать, что *атака* - это действие или последовательность связанных между собой действий, использующих *уязвимости* данной информационной системы и приводящих к нарушению политики безопасности.

Основные понятия и определения

Механизм безопасности - программное и/или аппаратное средство, которое определяет и/или предотвращает *атаку*.
Сервис безопасности - сервис, который обеспечивает задаваемую политикой безопасность систем и/или передаваемых данных, либо определяет осуществление *атаки*. *Сервис* использует один или более механизмов безопасности.
Рассмотрим модель сетевой безопасности и основные типы *атак*, которые могут осуществляться в этом случае. Затем рассмотрим основные типы *сервисов* и *механизмов безопасности*, предотвращающих такие *атаки*.

Классификация сетевых атак

В общем случае существует информационный поток от отправителя (файл, пользователь, компьютер) к получателю (файл, пользователь, компьютер):

Рис. 1.2. Информационный поток

Все *атаки* можно разделить на два класса: **пассивные и активные**.

Пассивная атака

Пассивная атака

Пассивной называется такая ***атака***, при которой *противник* не имеет возможности модифицировать передаваемые сообщения и вставлять в информационный канал между отправителем и получателем свои сообщения. Целью *пассивной атаки* может быть только прослушивание передаваемых сообщений и анализ трафика.

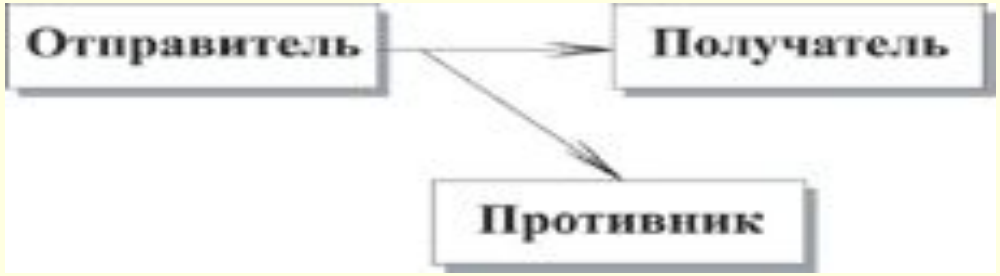


Рис. 1.3. Пассивная атака

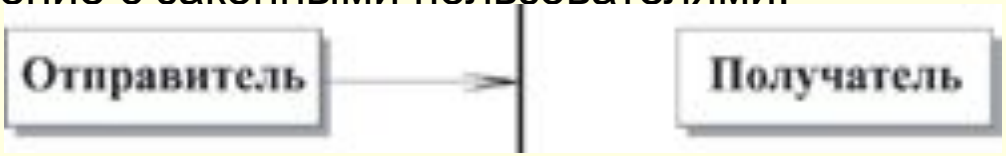
Активная атака

1. Активная атака

Активной называется такая ***атака***, при которой *противник* имеет возможность модифицировать передаваемые сообщения и вставлять свои сообщения. Различают **следующие типы активных атак:**

Отказ в обслуживании - ***DoS-атака (Denial of Service)***

Отказ в обслуживании нарушает нормальное функционирование сетевых сервисов. *Противник* может перехватывать все сообщения, направляемые определенному адресату. Другим примером подобной *атаки* является создание значительного трафика, в результате чего сетевой сервис не сможет обрабатывать запросы законных клиентов. Классическим примером такой *атаки* в сетях TCP/IP является SYN-атака, при которой нарушитель посылает пакеты, инициирующие установление TCP-соединения, но не посылает пакеты, завершающие установление этого соединения. В результате может произойти переполнение памяти на сервере, и серверу не удастся установить соединение с законными пользователями.



Активная атака

2. Модификация потока данных - ***атака "man in the middle"***
Модификация потока данных означает либо изменение содержимого пересылаемого сообщения, либо изменение порядка сообщений.

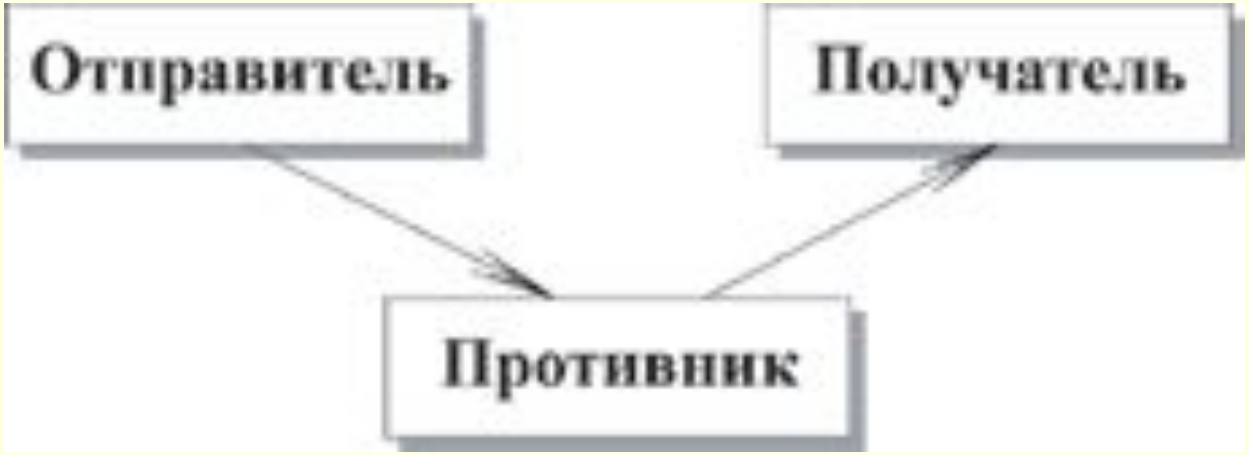


Рис. 1.5. Атака "man in the middle"

Активная атака

3. Создание ложного потока (фальсификация)
Фальсификация (нарушение аутентичности) означает попытку одного субъекта выдать себя за другого.

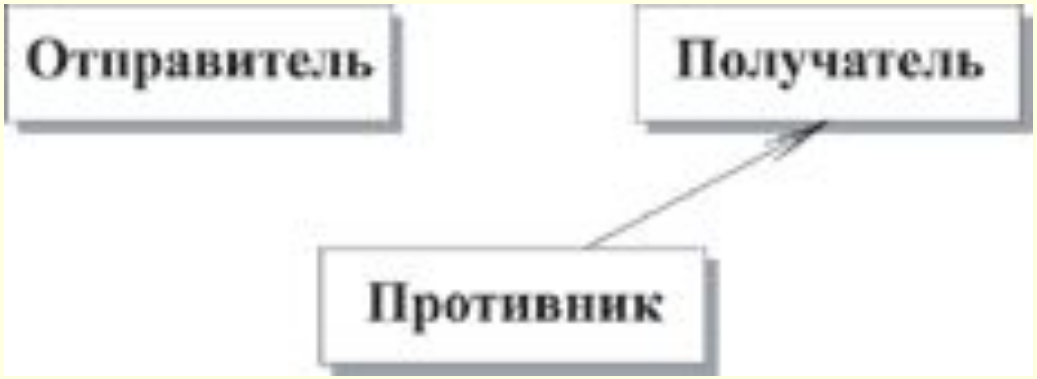


Рис. 1.6. Создание ложного потока

Активная атака

4. Повторное использование

Повторное использование означает пассивный захват данных с последующей их пересылкой для получения несанкционированного доступа - это так называемая ***replay-атака***. На самом деле *replay-атаки* являются одним из вариантов фальсификации, но в силу того, что это один из наиболее распространенных вариантов *атаки* для получения несанкционированного доступа, его часто рассматривают как отдельный тип *атаки*.

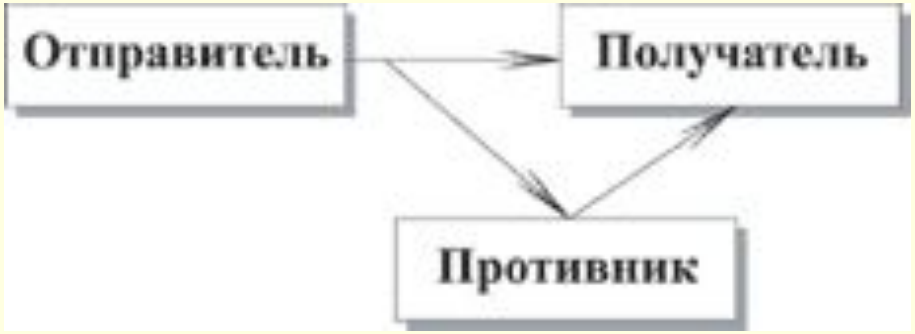


Рис. 1.7. Replay-атака

Активная атака

Перечисленные *атаки* могут существовать в любых типах сетей, а не только в сетях, использующих в качестве транспорта протоколы TCP/IP, и на любом уровне модели OSI. Но в сетях, построенных на основе TCP/IP, *атаки* встречаются чаще всего, потому что, во-первых, Internet стал самой распространенной сетью, а во-вторых, при разработке протоколов TCP/IP требования безопасности никак не учитывались.

Сервисы безопасности

Основными *сервисами безопасности* являются следующие:

Конфиденциальность - предотвращение *пассивных атак* для передаваемых или хранимых данных.
Аутентификация - подтверждение того, что информация получена из законного источника, и получатель действительно является тем, за кого себя выдает. В случае передачи единственного сообщения *аутентификация* должна гарантировать, что получателем сообщения является тот, кто нужно, и сообщение получено из заявленного источника. В случае установления соединения имеют место два аспекта. Во-первых, при инициализации соединения *сервис* должен гарантировать, что оба участника являются требуемыми. Во-вторых, *сервис* должен гарантировать, что на соединение не воздействуют таким образом, что *третья сторона* сможет маскироваться под одну из легальных сторон уже после установления соединения.

Сервисы безопасности

Целостность - *сервис*, гарантирующий, что информация при хранении или передаче не изменилась. Может применяться к потоку сообщений, единственному сообщению или отдельным полям в сообщении, а также к хранимым файлам и отдельным записям файлов.
Невозможность отказа - невозможность, как для получателя, так и для отправителя, отказаться от факта передачи. Таким образом, когда сообщение отправлено, получатель может убедиться, что это сделал легальный отправитель. Аналогично, когда сообщение пришло, отправитель может убедиться, что оно получено легальным получателем.
Контроль доступа - возможность ограничить и контролировать доступ к системам и приложениям по коммуникационным линиям.
Доступность - результатом *атак* может быть потеря или снижение доступности того или иного сервиса. Данный *сервис* предназначен для того, чтобы минимизировать возможность осуществления *DoS-атак*.

Механизмы безопасности

Перечислим основные *механизмы безопасности*:

Алгоритмы симметричного шифрования - алгоритмы шифрования, в которых для шифрования и дешифрования используется один и тот же ключ или ключ дешифрования легко может быть получен из ключа шифрования.

Алгоритмы асимметричного шифрования - алгоритмы шифрования, в которых для шифрования и дешифрования используются два разных ключа, называемые открытым и закрытым ключами, причем, зная один из ключей, вычислить другой невозможно.

Хэш-функции - функции, входным значением которых является сообщение произвольной длины, а выходным значением - сообщение фиксированной длины. *Хэш-функции* обладают рядом свойств, которые позволяют с высокой долей вероятности определять изменение входного сообщения.

Модель сетевого взаимодействия

Модель безопасного сетевого взаимодействия в общем виде можно представить следующим образом:

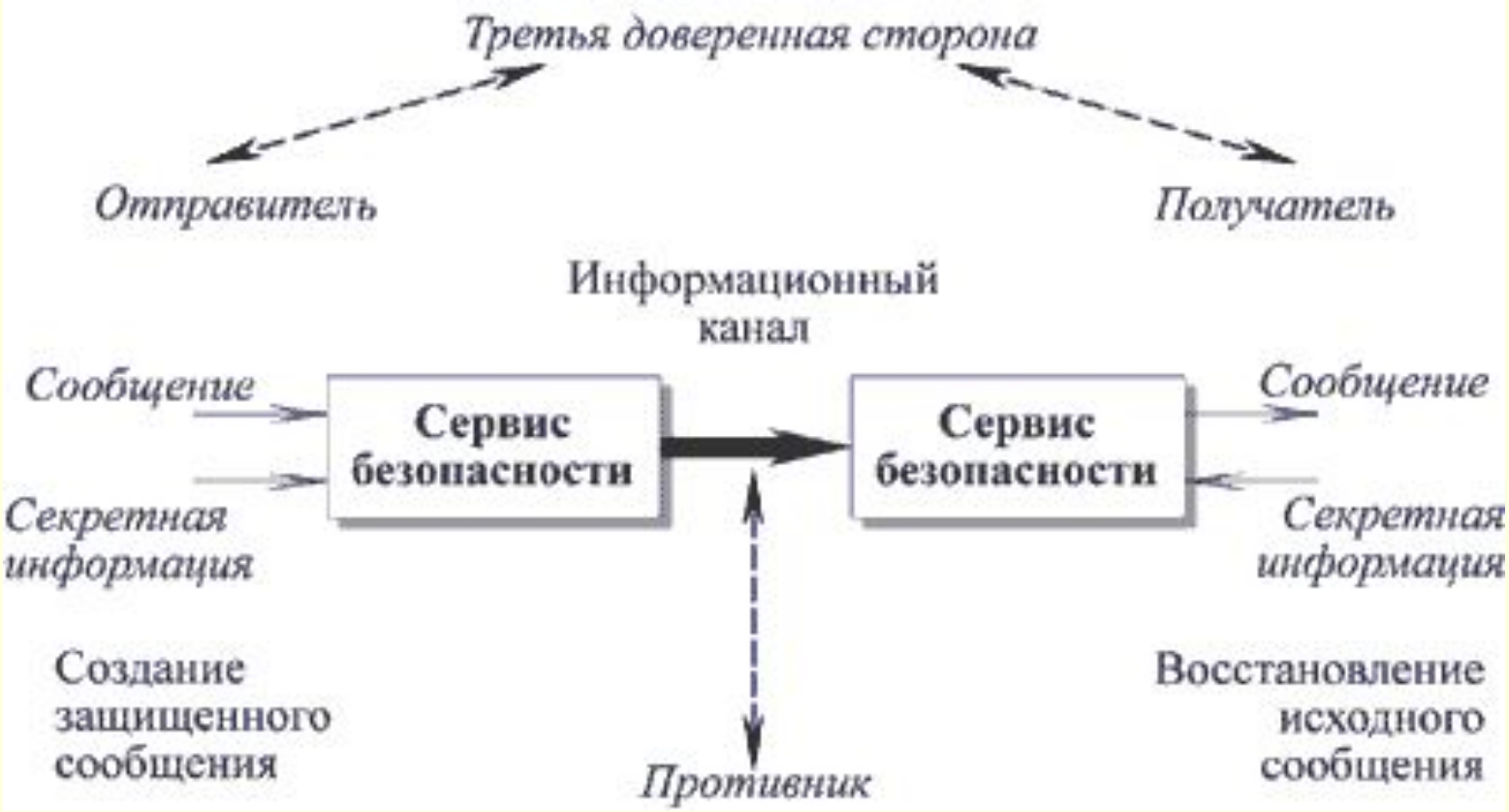


Рис. 1.8. Модель сетевой безопасности

Модель сетевого взаимодействия

Сообщение, которое передается от одного участника другому, проходит через различного рода сети. При этом будем считать, что устанавливается логический информационный канал от отправителя к получателю с использованием различных коммуникационных протоколов (например, TCP/IP).
Средства безопасности необходимы, если требуется защитить передаваемую информацию от ***противника***, который может представлять угрозу ***конфиденциальности***, ***аутентификации***, ***целостности*** и т.п. Все технологии повышения безопасности имеют два компонента:

1.Относительно безопасная передача информации. Примером является шифрование, когда сообщение изменяется таким образом, что становится нечитаемым для **противника**, и, возможно, дополняется кодом, который основан на содержимом сообщения и может использоваться для **аутентификации** отправителя и обеспечения **целостности** сообщения.

Модель сетевого взаимодействия

2. Некоторая секретная информация, разделяемая обоими участниками и неизвестная ***противнику***. Примером является ключ шифрования.

Кроме того, в некоторых случаях для обеспечения безопасной передачи бывает необходима **третья доверенная сторона** (third trusted party - TTP). Например, **третья сторона** может быть ответственной за распределение между двумя участниками секретной информации, которая не стала бы доступна ***противнику***. Либо **третья сторона** может использоваться для решения споров между двумя участниками относительно достоверности передаваемого сообщения.

Модель сетевого взаимодействия

Из данной общей модели вытекают три основные задачи, которые необходимо решить при разработке конкретного ***сервиса безопасности***:

1. Разработать алгоритм шифрования/дешифрования для выполнения безопасной передачи информации. Алгоритм должен быть таким, чтобы *противник* не мог расшифровать перехваченное сообщение, не зная секретную информацию.
2. Создать секретную информацию, используемую алгоритмом шифрования.
3. Разработать протокол обмена сообщениями для распределения разделяемой секретной информации таким образом, чтобы она не стала известна *противнику*.

Модель безопасности информационной системы

Существуют и другие относящиеся к безопасности ситуации, которые не соответствуют описанной выше модели сетевой безопасности. Общую модель этих ситуаций можно проиллюстрировать следующим образом:

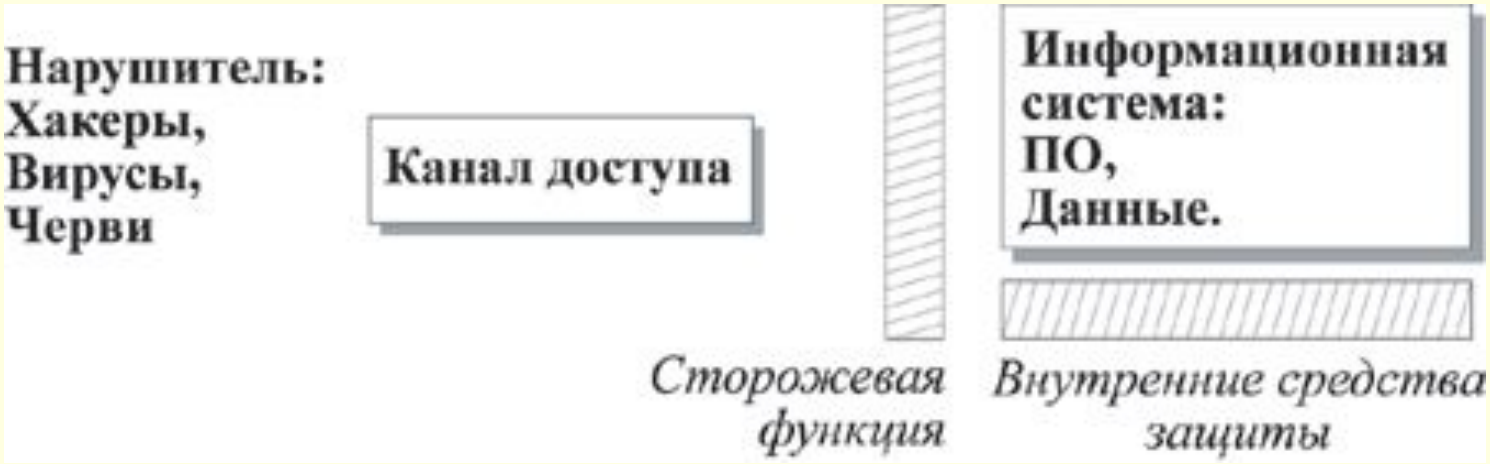


Рис. 1.9. Модель безопасности информационной системы

Модель безопасности информационной системы

Данная модель иллюстрирует концепцию безопасности информационной системы, с помощью которой предотвращается нежелательный доступ. Хакер, который пытается осуществить незаконное проникновение в системы, доступные по сети, может просто получать удовольствие от взлома, а может стараться повредить информационную систему и/или внедрить в нее что-нибудь для своих целей. Например, целью хакера может быть получение номеров кредитных карточек, хранящихся в системе.

Другим типом нежелательного доступа является размещение в вычислительной системе чего-либо, что воздействует на прикладные программы и программные утилиты, такие как редакторы, компиляторы и т.п. Таким образом, существует **два типа *атак***:

1. Доступ к информации с целью получения или модификации хранящихся в системе данных.

2. *Атака* на сервисы, чтобы помешать использовать их.

Модель безопасности информационной системы

Вирусы и черви - примеры подобных **атак**. Такие **атаки** могут осуществляться как с помощью дискет, так и по сети.
Сервисы безопасности, которые предотвращают нежелательный доступ, можно разбить на две категории:
Первая категория определяется в терминах сторожевой функции. Эти **механизмы** включают процедуры входа, основанные, например, на использовании пароля, что позволяет разрешить доступ только авторизованным пользователям. Эти **механизмы** также включают различные защитные экраны (firewalls), которые предотвращают **атаки** на различных уровнях стека протоколов TCP/IP, и, в частности, позволяют предупреждать проникновение червей, вирусов, а также предотвращать другие подобные **атаки**.
Вторая линия обороны состоит из различных внутренних мониторов, контролирующих доступ и анализирующих деятельность пользователей.

Модель безопасности информационной системы

Одним из основных понятий при обеспечении безопасности информационной системы является понятие ***авторизации*** - определение и предоставление прав доступа к конкретным ресурсам и/или объектам.

В основу безопасности информационной системы должны быть положены следующие основные принципы:

1. Безопасность информационной системы должна соответствовать роли и целям организации, в которой данная система установлена.
2. Обеспечение информационной безопасности требует комплексного и целостного подхода.
3. Информационная безопасность должна быть неотъемлемой частью системы управления в данной организации.
4. Информационная безопасность должна быть экономически оправданной.

Модель безопасности информационной системы

5. Ответственность за обеспечение безопасности должна быть четко определена.
6. Безопасность информационной системы должна периодически переоцениваться.
7. Большое значение для обеспечения безопасности информационной системы имеют социальные факторы, а также меры административной, организационной и физической безопасности.