**МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ М.В.ЛОМОНОСОВА**

**Отчет по мероприятию**

Организация учебных выездных лекций и семинаров для школьников и абитуриентов в образовательных учреждениях общего среднего образования города Москвы

**НОМ 3**

Научно-популярные материалы для школьников о современной информатике

Москва 2011

# Защита информации в сети интернет

## Введение

За несколько последних десятилетий требования к защите информации существенно изменились. До начала широкого использования автоматизированных систем обработки данных защита информации достигалась исключительно надежными замками, охраной помещения 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.

Вопросы защиты информации несомненно являются одними из самых важных при развертывании сетей и подключении их к интернету.

Сегодня подключение корпоративной сети к интернету стало обыденным явлением. Большинство компаний сегодня имеют свои сайты в интернете. За удобства и новые возможности приходится расплачиваться появлением новых проблем, связанных с безопасностью. И в первом, и во втором случае для того, что не иметь проблем, связанных с нежелательным присутствием посторонних в вашей корпоративной сети или на сайте, необходимо учитывать многие аспекты и достаточно свободно разбираться во многих технологиях. Для обеспечения безопасности приходится создавать так называемую «оборону вглубь», потому что не существует единственного универсального средства или единственной универсальной технологии, которые позволили бы решить все проблемы информационной безопасности.

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, интернет) необходимо быть уверенным, что никто не сможет ни подсмотреть, ни изменить эту информацию.

2. Сетевой администратор осуществляет удаленное управление компьютером. Кто-то другой перехватывает это управляющее сообщение, изменяет его содержание и отправляет сообщение на данный компьютер.

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 интернет-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 интернет. 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.

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**.

Давайте вначале рассмотрим в самых общих чертах, что такое интернет и как происходит передача информации в сети интернет. Интернет состоит из огромного числа **компьютеров**, соединенных между собой специальными **проводами**. На компьютерах **выполняются программы**, а по проводам передаются **данные**, которые **обрабатываются** этими программами. В настоящее время существуют технологии, позволяющие передавать данные между компьютерами без проводов, аналогично тому, как передаются данные при использовании мобильной телефонной связи. Для нас с вами сейчас не будет иметь значение по проводам передаются данные или используются беспроводные технологии. В обоих случаях будем говорить, что **компьютеры связаны в сеть**. **Слайд № 2.**

Одновременно на каждом компьютере может быть запущено очень большое количество программ, которые умеют получать информацию из сети и посылать информацию в сеть. Каждая из этих программ обрабатывает свою часть данных, получаемых из сети, и посылает в сеть новые данные, предназначенные для других компьютеров.

Давайте посмотрим, как происходит пересылка информации в компьютерных сетях. Данные по сети интернет передаются отдельными блоками, которые в сетях называются **пакетами**. У каждого пакет есть **заголовок**, в котором содержится вся информация, необходимая программам для обработки этого пакета, и **тело** пакета. **Слайд № 3.**

Все пакеты передаются в заранее определенной последовательности. Эта заранее определенная последовательность пакетов называется **протоколом**. Также каждый пакет имеет заранее определенный **формат** данных, **содержимое** же данных в каждом пакете естественно разное. **Слайд № 4.**

В теле пакета может содержаться другой пакет, который относится к другому протоколу. В этом случае говорят о **стеке протоколов**. Стек протоколов означает, что пакеты одного протокола как матрешки вложены в тело других пакетов другого протокола. Можно сказать, что каждый протокол выполняется на определенном **уровне** стека протоколов. Либо в теле пакета содержится информация, ради которой и создана сеть Интернет. Такой информацией может быть, например, почтовое сообщение или веб-страница с какого-либо сайта. Поток пакетов между отдельными компьютерами, которые передаются в соответствии с определенным протоколом, называется **сетевым трафиком**. Пакеты передаются от одного компьютера к другому до тех пор, пока не достигнут того компьютера (и той программы), для которого они предназначены. Компьютеры, через которые проходит сетевой трафик, называются **маршрутизаторами**. Каждый маршрутизатор обычно бывает соединен с несколькими компьютерами и принимает решение, какому из этих компьютеров переслать пакет, чтобы в конечном счете пакет достиг компьютера, для которого он предназначен. Этот процесс называется **маршрутизацией**. **Слайд № 5.**

Рассмотрим основные понятия, относящиеся к защите информации, и их взаимосвязи. **Слайд № 6.**

Любая информация должна кому-то принадлежать, кто будет заботиться о ее защите. Эта информация должна быть для него важной и ценной, иначе не стоит ее защищать. Поэтому мы говорим не просто об информации, а об информационных ценностях. Кроме того, эта информация должна представлять определенный интерес еще для кого-то, кто будет пытаться получить к ней доступ, но кому собственник информации не хочет давать

эту информацию. Этого человека (или программу, запущенную этим человеком) будем называть нарушителем, атакующим или оппонентом.

**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).

Собственники информационных ценностей анализируют уязвимости защищаемых ресурсов и возможные атаки, которые могут иметь место в данных условиях. 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 условиям, в котором они используются.

На Рис. 1 показана взаимосвязь рассмотренных выше понятий информационной безопасности.


**Рис. 1. Взаимосвязь основных понятий безопасности информационных систем**

Будем использовать следующие термины и понятия:

**Слайд № 7.***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.

**Слайд № 8.***Атака* – любое действие, нарушающее безопасность информационной системы. Атакой может быть не только отдельное действие, но и последовательность

связанных между собой действий, использующих *уязвимости* данной информационной системы и приводящих к нарушению *политики безопасности*.

*Механизм безопасности* – программное или аппаратное средство, которое определяет или предотвращает атаку.

*Сервис безопасности* – сервис, который обеспечивает задаваемую политикой безопасности защиту систем и передаваемых данных, либо определяет осуществление атаки. Сервис использует один или более механизмов безопасности.

# Защита информации в сетях

**Слайд № 9.**

## Основные сетевые атаки

**Слайд № 10.**Взаимодействие по сети означает, что существует информационный поток данных от отправителя к получателю. Отправителем и получателем в данном случае могут являться как компьютеры, так и отдельные программы, запущенные на этих компьютерах.

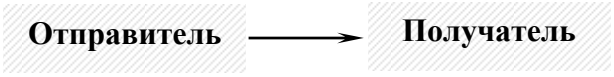


**Рис. 2. Информационный поток**

Все атаки можно разделить на пассивные и активные.

### *I. 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**.

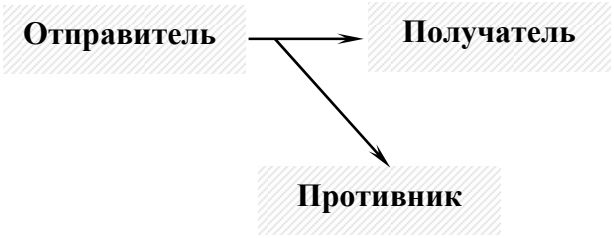


**Рис. 3. Пассивная атака**

### *II.* Активная атака

**Слайд № 11.**Активной называется такая атака, при которой противник имеет возможность **модифицировать передаваемые сообщения и вставлять свои сообщения**. Различают следующие типы активных атак:

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

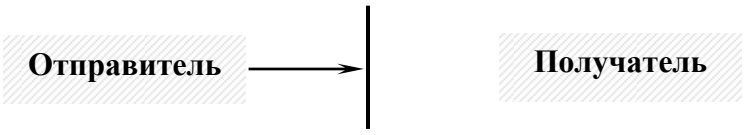

**Рис. 4. DoS-атака**

Отказ в обслуживании нарушает нормальное функционирование сетевого сервиса (в данном случае Получателя), когда законный пользователь (в данном случае Отправитель) не может получить сетевой сервис.

**2. Модификация потока данных - атака "man in the middle"**

Модификация потока данных означает либо изменение содержимого пересылаемого сообщения, либо изменение порядка сообщений.

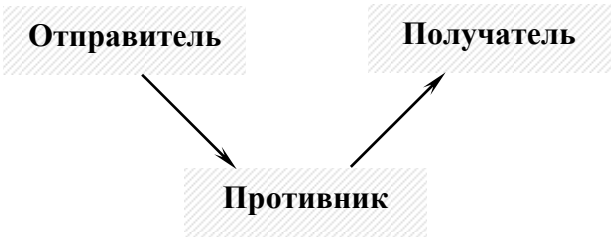


**Рис. 5. Атака "man in the middle"**

**Слайд № 12.**

**3. Создание ложного потока (фальсификация)**

Фальсификация (нарушение аутентичности) означает попытку одного субъекта выдать себя за другого. В данном случае Отправитель не передает никакого сообщения, а Противник пытается выдать себя за Отправителя.


**Рис. 6. Создание ложного потока**

**4. Повторное использование**

Повторное использование означает перехват данных с последующей их пересылкой через некоторое время Получателю 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.

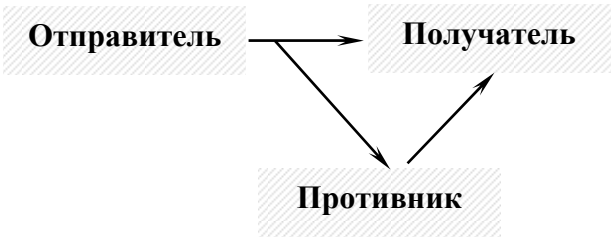


**Рис. 7. Replay-атака**

Перечисленные атаки могут существовать в любых типах сетей, а не только в сети интернет. Но в сети интернет эти атаки встречаются чаще, потому что, во-первых, интернет стал самой распространенной сетью, а во-вторых, при разработке протоколов, которые используются в сети интернет, требования безопасности никак не учитывались.

## Сервисы безопасности

**Слайд № 13.**Перечислим основные сервисы безопасности.

*Конфиденциальность* – предотвращение пассивных атак для передаваемых или хранимых данных. Сервис конфиденциальности преобразует передаваемое сообщение таким образом, чтобы никто, кроме Получателя, не мог понять передаваемое сообщение. Для всех остальных передаваемое сообщение должно казаться случайным набором нулей и единиц.

*Аутентификация* – подтверждение того, что информация получена от законного Отправителя, 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, т.е. когда между Отправителем и Получателем передает поток сообщений в обе стороны, 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.

*Целостность* – сервис, гарантирующий, что информация при хранении или передаче не изменилась. Сервис может относиться к потоку сообщений, единственному сообщению или отдельным полям в сообщении, а также к хранимым файлам и отдельным записям файлов.

**Слайд № 14.***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 компьютерам и программам 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

**Слайд № 15.**Перечислим основные механизмы безопасности:

*Алгоритмы симметричного шифрования* – криптографические алгоритмы, предназначенные для преобразования сообщения таким образом, чтобы невозможно было получить исходное сообщение без знания некоторой дополнительной информации, называемой **ключом**. Такое преобразование называется **шифрованием**. Обратное преобразование зашифрованного сообщения в исходное называется **расшифрованием**. В этих алгоритмах для шифрования и расшифрования используется один и тот же ключ, поэтому эти алгоритмы называется **симметричными**.

*Алгоритмы асимметричного шифрования* – криптографические алгоритмы, в которых для шифрования и расшифрования используются **два разных ключа**, называемые **открытым и закрытым ключами**, причем, **зная закрытый ключ, вычислить открытый невозможно**.

*Хэш-функции* – криптографические 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.

## Защита информации при сетевом взаимодействии

**Слайд № 16.** Безопасное сетевое взаимодействие в общем виде можно представить следующим образом:

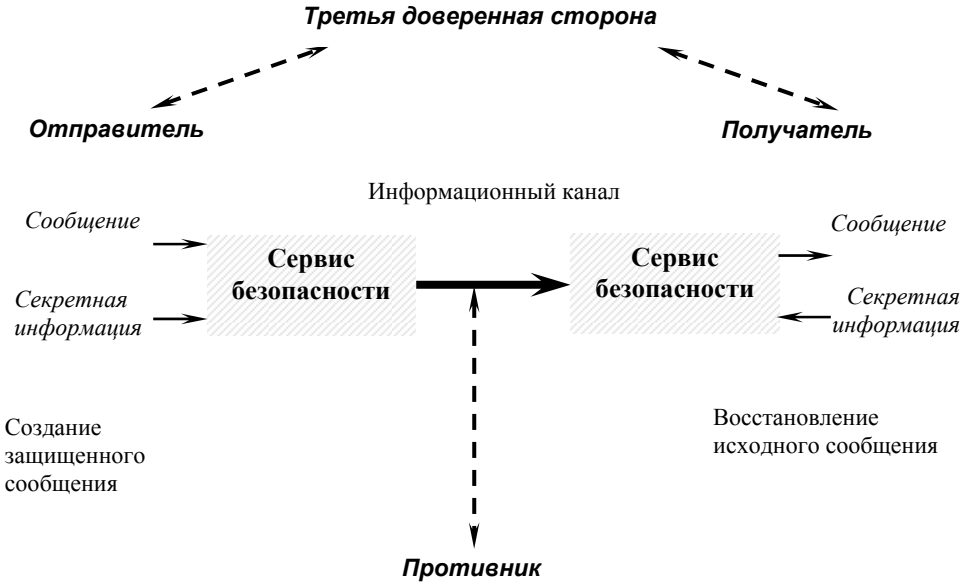


**Рис. 8. Защита информации при сетевом взаимодействии**

Сообщение, которое передается от одного участника другому, проходит через большое количество других компьютеров с использованием большого количества протоколов. Можно считать, что устанавливается информационный канал от Отправителя к Получателю. Сервисы безопасности должны обеспечивать защиту этого информационного канала от всех типов атак, перечисленных выше.

Средства защиты 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, используя шифрование, при котором сообщение изменяется таким образом, что противнику кажется случайным набором нулей и единиц. И, возможно, в сообщение добавляются данные для обеспечения целостности сообщения, т.е. данные, которые позволяют Получателю с большой долей вероятности определить, что сообщение не было изменено.

2. Некоторая секретная информация, разделяемая обоими участниками и неизвестная противнику, которая используется для шифрования сообщения.

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.

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

1. Разработать алгоритм шифрования/расшифрования 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.

## Защита информационной системы

**Слайд № 17.**Другой, относящейся к защите информации ситуации, является обеспечение безопасности некоторой информационной системы, к которой необходимо предотвратить нежелательный доступ. Общую схему этих ситуаций можно проиллюстрировать следующим образом:


**Рис. 9. Модель безопасности информационной системы**

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 каким-то образом изменяет работу программ в компьютере. 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 или нарушить их работу.

Вирусы и черви - примеры подобных атак.

Сервисы безопасности, которые предотвращают нежелательный доступ, можно разбить на две категории:

1. 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 межсетевые экраны (firewalls), которые предотвращают атаки,

и, в частности, позволяют предупреждать проникновение червей, вирусов, а также предотвращать другие подобные атаки.

2. Вторая линия обороны состоит из различных внутренних мониторов, контролирующих доступ и анализирующих деятельность пользователей.

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

# Алгоритмы симметричного шифрования

**Слайд № 18.**Рассмотрим общую схему симметричной, или традиционной, криптографии.

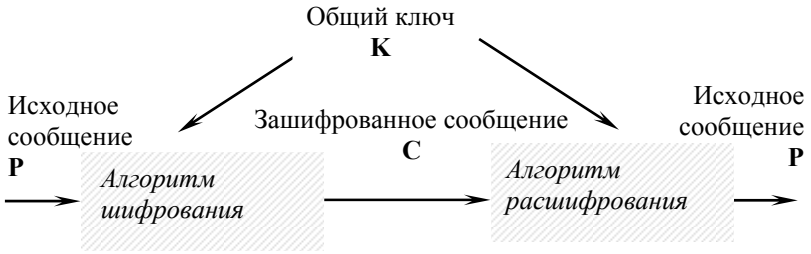


**Рис. 10. Общая схема симметричного шифрования**

В процессе шифрования используется определенный алгоритм шифрования, на вход которому подаются исходное незашифрованное сообщение, называемое также plaintext, и ключ. Выходом алгоритма является зашифрованное сообщение, называемое также ciphertext. Ключ является значением, не зависящим от шифруемого сообщения. Изменение ключа должно приводить к изменению зашифрованного сообщения.

Зашифрованное сообщение передается получателю. Получатель преобразует зашифрованное сообщение в исходное незашифрованное сообщение с помощью алгоритма расшифрования и того же самого ключа, который использовался при шифровании.

Безопасность, обеспечиваемая традиционной криптографией, зависит от нескольких факторов.

Во-первых, криптографический алгоритм должен быть достаточно сильным, чтобы передаваемое зашифрованное сообщение невозможно было расшифровать без ключа, используя только различные статистические закономерности зашифрованного сообщения или какие-либо другие способы его анализа.

Во-вторых, безопасность передаваемого сообщения должна зависеть от секретности ключа, но не от секретности алгоритма. Алгоритм должен быть проанализирован специалистами, чтобы исключить наличие слабых мест, при которых плохо скрыта взаимосвязь между незашифрованным и зашифрованным сообщениями. К тому же при выполнении этого условия производители могут создавать дешевые аппаратные чипы и свободно распространяемые программы, реализующие данный алгоритм шифрования.

В-третьих, алгоритм должен быть таким, чтобы нельзя было узнать ключ, даже зная достаточно много пар (зашифрованное сообщение, незашифрованное сообщение), полученных при шифровании с использованием данного ключа.

Алгоритмы симметричного шифрования различаются способом, которым обрабатывается исходный текст. Возможно шифрование блоками или шифрование потоком.

Блок текста рассматривается как неотрицательное целое число, либо как несколько независимых неотрицательных целых чисел. Длина блока всегда выбирается равной степени двойки. В большинстве блочных алгоритмов симметричного шифрования используются следующие типы операций:

- Табличная подстановка, при которой группа битов отображается в другую группу битов. Это так называемые S-box.
- Перемещение, с помощью которого биты сообщения переупорядочиваются.
- Операция сложения по модулю 2, обозначаемая XOR или $\oplus$.
- Операция сложения по модулю $2^{32}$ или по модулю $2^{16}$.
- Циклический сдвиг на некоторое число битов.

Эти операции циклически повторяются в алгоритме, образуя так называемые раунды. Входом каждого раунда является выход предыдущего раунда и ключ, который получен по определенному алгоритму из ключа шифрования K. Ключ раунда называется подключом. Каждый алгоритм шифрования может быть представлен следующим образом:

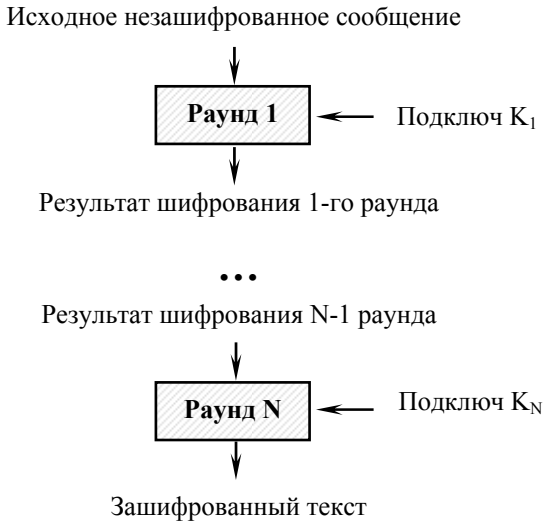


**Рис. 11 . Структура алгоритма симметричного шифрования**

# Хэш-функции

**Слайд № 19.**Хэш-функцией называется функция, с помощью которой получается дайджест (или хэш-код) сообщения, т.е. блок данный фиксированной длины, который с большой вероятностью будет другим для другого сообщения. Это позволяет использовать вычисленный хэш-код в качестве дайджеста сообщения.

# Криптография с открытым ключом

## Требования к алгоритмам асимметричного шифрования

**Слайд № 20.**Создание алгоритмов асимметричного шифрования является величайшим и, возможно, единственным революционным достижением в истории криптографии.

Алгоритмы асимметричного шифрования, называемые также алгоритмами с открытым ключом, принципиально отличаются от алгоритмов симметричного шифрования.

Шифрование с открытым ключом является асимметричным, поскольку использует два различных ключа для шифрования и расшифрования, в отличие от симметричного шифрования, в котором для шифрования и расшифрования используется один и тот же ключ.

В результате этого алгоритмы с открытым ключом гораздо больше основаны на свойствах математических функций, чем алгоритмы симметричного шифрования, использующие в основном только операции подстановки и перемещения. Применение двух ключей имеет важные следствия в таких областях, как аутентификация, распределение ключа и конфиденциальность.

Алгоритмы шифрования с открытым ключом разрабатывались для того, чтобы решить две наиболее трудные задачи, возникшие при использовании симметричного шифрования.

Первой задачей является распределение ключа. При симметричном шифровании требуется, чтобы обе стороны уже имели общий ключ, который каким-то образом должен быть им заранее передан.

Второй задачей является необходимость создания таких механизмов, при использовании которых невозможно было бы подменить кого-либо из участников, т.е. нужна цифровая подпись. При использовании сетей в коммерческих и частных целях электронные сообщения и документы должны иметь эквивалент подписи, содержащейся в бумажных документах. Необходимо создать метод, при использовании которого все участники будут убеждены, что электронное сообщение было послано конкретным участником.

**Слайд № 21.**При описании симметричного шифрования и шифрования с открытым ключом будем использовать следующую терминологию. Ключ, используемый в симметричном шифровании, будем называть **секретным ключом**. Два ключа, используемые при шифровании с открытым ключом, будем называть **открытым ключом** и **закрытым ключом**. Закрытый ключ держится в секрете, но называть его будем закрытым ключом, а не секретным, чтобы избежать путаницы с ключом, используемым в симметричном шифровании. Закрытый ключ будем обозначать **KR**, открытый ключ - **KU**.

Будем предполагать, что все участники имеют доступ к открытым ключам друг друга, а закрытые ключи создаются локально каждым участником и, следовательно, распределяться не должны.

В любое время участник может изменить свой закрытый ключ и опубликовать составляющий пару открытый ключ, заменив им старый открытый ключ.

Требования, которым должен удовлетворять алгоритм шифрования с открытым ключом:

1. Вычислительно легко создавать пару (открытый ключ **KU**, закрытый ключ **KR**).
2. Вычислительно невозможно, зная открытый ключ **KU**, определить закрытый ключ **KR**.

## Основные способы использования алгоритмов с открытым ключом

Основными способами использования алгоритмов с открытым ключом являются шифрование/расшифрование, создание и проверка подписи и обмен ключа.

**Шифрование** с открытым ключом состоит из следующих шагов:

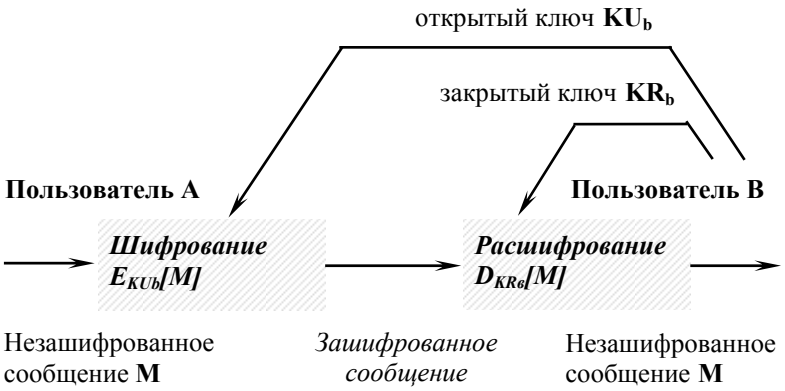


**Рис. 12. Шифрование с открытым ключом**

1. Пользователь В создает пару ключей $KU_b$ и $KR_b$, используемых для шифрования и расшифрования передаваемых сообщений.
2. Пользователь В делает доступным некоторым надежным способом свой ключ шифрования, т.е. открытый ключ $KU_b$. Составляющий пару закрытый ключ $KR_b$ держится в секрете.
3. Если А хочет послать сообщение В, он шифрует сообщение, используя открытый ключ В $KU_b$.
4. Когда В получает сообщение, он расшифрует его, используя свой закрытый ключ $KR_b$. Никто другой не сможет расшифровать сообщение, так как этот закрытый ключ знает только В.

Если пользователь надежно хранит свой закрытый ключ, никто не сможет подсмотреть передаваемые сообщения.

**Слайд № 22.** **Создание и проверка подписи** состоит из следующих шагов:

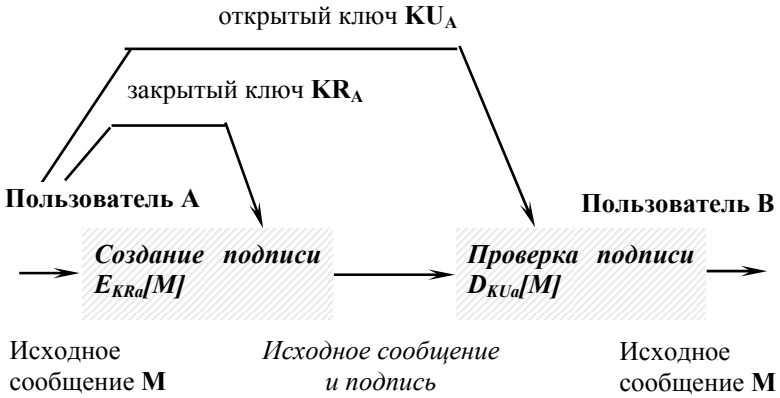


**Рис. 13. Создание и проверка подписи**

1. Пользователь А создает пару ключей $KR_A$ и $KU_A$, используемых для создания и проверки подписи передаваемых сообщений.
2. Пользователь А делает доступным некоторым надежным способом свой ключ проверки, т.е. открытый ключ $KU_A$. Составляющий пару закрытый ключ $KR_A$ держится в секрете.
3. Если А хочет послать подписанное сообщение В, он создает подпись $E_{KRa}[M]$ для этого сообщения, используя свой закрытый ключ $KR_A$.

4. Когда B получает подписанное сообщение, он проверяет подпись $\mathbf{D_{KUa}[M]}$, используя открытый ключ A $\mathbf{KU_A}$. Никто другой не может подписать сообщение, так как этот закрытый ключ знает только A.

До тех пор, пока пользователь надежно хранит свой закрытый ключ, его подписи достоверны.

Кроме того, невозможно изменить сообщение, не имея доступа к закрытому ключу A; тем самым обеспечивается аутентификация и целостность данных.

В нашем случае подписывается все сообщение. Более эффективно подписывать небольшой блок данных, который зависит от сообщения. Такой блок называется аутентификатором и обладает таким свойством, что малейшее изменение сообщения приводит к изменению аутентификатора. Если такой аутентификатор подписать закрытым ключом отправителя, то такая цифровая подпись обеспечивает аутентификацию отправителя и целостность сообщения.

Важно подчеркнуть, что описанный процесс создания подписи не обеспечивает конфиденциальность. Это означает, что сообщение, посланное таким способом, невозможно изменить, но можно подсмотреть. Это очевидно в том случае, если подпись основана на аутентификаторе, так как само сообщение передается в явном виде. Но даже если подписывается все сообщение, конфиденциальность не обеспечивается, так как любой может расшифровать сообщение, используя открытый ключ отправителя.

**Обмен ключей:** две стороны взаимодействуют для обмена ключом сессии, который в дальнейшем можно использовать в алгоритме симметричного шифрования.

Некоторые алгоритмы можно использовать всеми тремя способами, другие могут использоваться одним или двумя способами.

## Цифровая подпись

Аутентификация с помощью пароля или общего секрета защищает двух участников от нарушителя. Однако такая аутентификация не защищает участников друг от друга, тогда как и между ними тоже могут возникать определенные формы споров.

В ситуации, когда обе стороны не доверяют друг другу, необходимо нечто большее, чем аутентификация на основе общего секрета. Возможным решением подобной проблемы является использование цифровой подписи. Цифровая подпись должна обладать следующими свойствами:

1. Цифровая подпись должна зависеть от подписываемого сообщения.
2. Цифровая подпись должна использовать некоторую уникальную информацию отправителя.
3. Создавать цифровую подпись должно быть относительно легко.
4. Должно быть относительно легко проверять цифровую подпись.
5. Должно быть невозможно подделать цифровую подпись как созданием нового сообщения для существующей цифровой подписи, так и созданием новой цифровой подписи для существующего сообщения.
6. Подпись должна быть проверяема третьей стороной для разрешения споров.

Таким образом, цифровая подпись обеспечивает аутентификацию отправителя и целостность передаваемого сообщения.

Хэш-функция, подписанная закрытым ключом отправителя, удовлетворяет перечисленным требованиям.

# Инфраструктура Открытого Ключа

**Слайд № 23.**Одним из требований к алгоритмам цифровой подписи является требование, чтобы было вычислительно невозможно, зная открытый ключ **KU**, определить закрытый ключ **KR**. Казалось бы, открытый ключ **KU** можно распространять по небезопасным сетям и хранить в небезопасных хранилищах. Но при этом следует помнить, что при использовании цифровой подписи необходимо быть уверенным, что участник, которого мы аутентифицировали с помощью проверки цифровой подписи, является собственником соответствующего закрытого ключа. В противном случае возможна атака, когда оппонент заменяет открытый ключ законного участника своим открытым ключом, оставив при этом идентификатор законного участника без изменения. Это позволит ему создавать подписи от имени законного участника и читать зашифрованные сообщения, посланные законному участнику, используя для этого свой закрытый ключ, соответствующий подмененному открытому ключу. Для предотвращения такой ситуации следует использовать сертификаты, которые являются структурами данных, связывающими значения открытого ключа с субъектом. Для связывания необходимо наличие доверенного сертификационного центра (Certification Authority – CA), который проверяет идентификацию субъекта и подписывает его открытый ключ и некоторую дополнительную информацию своим закрытым ключом.

**Целью PKI является предоставление доверенного и действительного открытого ключа участника, а также управление всем жизненным циклом сертификата открытого ключа.**

Основным понятием Инфраструктуры Открытого Ключа является понятие сертификата.

Сертификат участника, созданный CA, имеет следующие характеристики:

1. Любой участник, имеющий открытый ключ CA, может восстановить открытый ключ участника, для которого CA создал сертификат.
2. Никто другой, кроме данного сертификационного центра, не может модифицировать сертификат без обнаружения этого проверяющей стороной.

Чаще всего используется формат сертификатов X.509, хотя существует достаточно много сертификатов других форматов.

# Межсетевые экраны

**Слайд № 24.**Межсетевые экраны являются аппаратными устройствами или программными системами, которые разрешают или запрещают прохождение сетевого трафика между сетями с различными требованиями к безопасности. Часто в сети предприятия ставят межсетевые экраны для ограничения трафика из и во внутренний сети, обрабатывающие информацию разного уровня секретности, такую как бухгалтерская информация или информация о заказчиках. Ставя межсетевые экраны для контроля соединений с этими областями, организация может предотвратить неавторизованный доступ к соответствующим системам и ресурсам внутри секретных областей.

**Слайд № 25.**Одним из способов сравнения возможностей разных типов межсетевых экранов является указание уровней в стеке протоколов, которые данный тип межсетевого экрана может анализировать.

Стек протоколов сети Интернет имеет следующие уровни:

| **Название уровня** | **Для чего он предназначен** |
|---|---|

| | |
|---|---|
| Прикладной | В теле пакета содержится информация, ради которой и создавалась сеть Интернет. Это могут быть, например, почтовые сообщения или страницы сайтов. |
| Транспортный | В теле пакета содержится пакет прикладного уровня, а в заголовке содержится адрес программы, для которой предназначен пакет. Это так называемый **порт**. А также в заголовке содержится все необходимое для надежной доставки пакетов. Доставка называется надежной, если ни один пакет не будет потерян. |
| Сетевой | В теле пакета содержится пакет транспортного уровня, а в заголовке адрес компьютера, с которого отправлен пакет, и адрес компьютера, которому предназначен пакет. Это так называемые IP-адреса. |

Современные межсетевые экраны функционируют на любом из этих уровней. Первоначально межсетевые экраны анализировали меньшее число уровней; более мощные межсетевые экраны охватывают большее число уровней. С точки зрения функциональности межсетевой экран, имеющий возможность анализировать большее число уровней, является более совершенным и эффективным. Возможность охватывать дополнительный уровень также увеличивает возможность более тонкой настройки конфигурации межсетевого экрана. Возможность анализировать более высокие уровни позволяет межсетевому экрану предоставлять сервисы, которые ориентированы на пользователя, такие как аутентификация пользователя. Межсетевой экран, который анализирует сетевой и транспортный уровни, не может выполнить аутентификацию пользователя.

Многие межсетевые экраны также имеют различные технологии фильтрации содержимого прикладного уровня. Например, межсетевой экран может сканировать присоединенные к почтовому сообщению файлы на наличие вирусов. Он также может использоваться для фильтрации наиболее опасных технологий создания так называемого динамического содержимого сайтов. Или он может быть использован для фильтрации содержимого или ключевых слов для ограничения доступа к неподходящим сайтам.

## Пакетные фильтры

**Слайд № 26.**Первый разработанный тип межсетевого экрана называется пакетным фильтром. Для указания того, какой трафик следует пропускать через пакетный фильтр, а какой отбрасывать, используются специальный набор правил.

Вначале пакетные фильтры работали только на сетевом уровне. В настоящее время все пакетные фильтры также анализируют и транспортный уровень.

Пакетные фильтры фильтруют сетевой трафик, основываясь на определенных характеристиках этого трафика.

Пакетные фильтры могут быть реализованы в следующих компонентах сетевой инфраструктуры:

- Маршрутизаторы, которые стоят на границе сети.
- Операционные системы.
- Персональные межсетевые экраны.

Основным преимуществом пакетных фильтров является их скорость.

Пакетным фильтрам присущи определенные недостатки. Так как пакетные фильтры не анализируют данные более высоких уровней, они не могут предотвратить атаки, которые используют уязвимости, специфичные для программы. Например, пакетный фильтр не может блокировать конкретные команды программы; если пакетный фильтр разрешает трафик для программы, то все команды, доступные данной программе, будут разрешены.

## Межсетевые экраны для отдельного компьютера

Межсетевые экраны реализованы во многих операционных системах; в частности, они могут использоваться только для обеспечения безопасности компьютера, на котором они функционируют.

***Преимущества межсетевых экранов, защищающих единственный компьютер:***

- Программы на сервере защищены лучше, чем если бы они выполнялись на ОС, не имеющей межсетевого экрана, защищающего данный компьютер; серверы должны быть хорошо защищены, и не следует предполагать, что они не могут быть атакованы только потому, что они расположены позади основного межсетевого экрана.
- Выполнение межсетевого экрана на отдельном компьютере не является необходимым условием для обеспечения безопасности сервера; межсетевой экран, защищающий только данный компьютер, достаточно хорошо выполняет функции обеспечения безопасности именно этого компьютера.
- Программное обеспечение, реализующее межсетевой экран для единственного компьютера, обычно предоставляют возможность управления доступом для ограничения трафика к и от серверов, выполняющихся на том же компьютере. Хотя межсетевые экраны для единственного компьютера менее предпочтительны в случае большого трафика и в окружениях с высокими требованиями к безопасности, для внутренних сетей небольших офисов они обеспечивают адекватную безопасность при меньшей цене.

***Недостаток межсетевых экранов, защищающих единственный компьютер:***

- Каждый такой межсетевой экран должен администрироваться самостоятельно, и после определенного количества серверов с межсетевыми экранами для единственного компьютера легче и дешевле просто разместить все серверы позади выделенного межсетевого экрана.

## Персональные межсетевые экраны и персональные устройства межсетевого экрана

Обеспечение безопасности персональных компьютеров дома или в мобильном варианте сейчас становится столь же важным, как и обеспечение безопасности компьютеров в офисе; домашние пользователи, подключающиеся по dial-up к провайдеру, могут обеспечить защиту с помощью небольшого межсетевого экрана, доступного им. Это необходимо, потому что провайдер может иметь много различных политик безопасности, не всегда соответствующих нуждам конкретного пользователя. Тем самым, персональные межсетевые экраны разрабатываются для обеспечения защиты удаленных систем и выполняют во многом те же самые функции, что и большие межсетевые экраны.

Эти программные продукты обычно реализованы в одном из двух вариантов. Первый вариант представляет собой *Personal Firewall*, который инсталлируется на защищаемую систему; персональные межсетевые экраны обычно не предполагают защиту каких-либо других систем или ресурсов. Более того, персональные межсетевые экраны обычно не

обеспечивают управление сетевым трафиком, который проходит через компьютер – они только защищают систему, на которой они инсталлированы.

Второй вариант называется *устройством персонального межсетевого экрана*, чей подход более похож на традиционный межсетевой экран. В большинстве случаев устройства персонального межсетевого экрана разрабатываются для защиты небольших сетей, таких как домашние сети. Эти устройства обычно выполняются на специализированной аппаратуре и имеют некоторые другие компоненты сетевой архитектуры в дополнение к самому межсетевому экрану.

Удобство управления устройством или программой является важным фактором при оценки или выборе персонального межсетевого экрана и устройства персонального межсетевого экрана. Идеально, когда управление позволяет реализовать определенную политику безопасности на всех системах, которые присоединяются к сети. Поэтому управление персональным межсетевым экраном должно быть по возможности централизовано.

## Прокси сервер прикладного уровня

**Слайд № 27.**Прокси прикладного уровня являются более мощными межсетевыми экранами, которые комбинируют управление доступом на низком уровне с функциональностью прикладного уровня.

Аутентификация пользователя может иметь много форм, например, такие:

- Аутентификация с помощью идентификатора пользователя и пароля.
- Аутентификация с помощью аппаратного брелка.
- Аутентификация по адресу источника.
- Биометрическая аутентификация.

Межсетевые экраны прикладного уровня имеют много преимуществ по сравнению с пакетными фильтрами.

***Преимущества прокси серверов прикладного уровня:***

- Прокси сервер имеет возможность выполнять аутентификацию пользователя. Часто существует возможность указывать способ аутентификации пользователя, который является предпочтительным. Прикладные прокси имеют возможность аутентифицировать самих пользователей в противоположность пакетным фильтрам, которые обычно проверяют только адрес сетевого уровня, с которого пришел пакет. Эти адреса сетевого уровня могут быть легко подменены без обнаружения этого пакетным фильтром.
- Так как возможности аутентификации на прикладном уровне, лучше аутентификации, выполняемой пакетными фильтрами, то прикладные прокси могут быть сделаны менее уязвимыми для атак подделки адреса.
- Межсетевые экраны прикладного уровня обычно имеют больше возможностей анализировать весь пакет, а не только сетевые адреса и порты. Например, они могут определять команды и данные, специфичные для каждой программы.

Более развитая функциональность прикладного прокси имеет также несколько недостатков по сравнению с пакетными фильтрами.

***Недостатки прокси серверов прикладного уровня:***

- Так как прикладные прокси «знают о пакете все», межсетевой экран вынужден тратить много времени для чтения и интерпретации каждого пакета. По этой причине прикладные прокси обычно не подходят для программ, которым необходима высокая пропускная способность, или программ реального времени. Для уменьшения загрузки межсетевого экрана может использоваться выделенный прокси сервер для обеспечения безопасности менее чувствительных ко времени сервисов, таких как e-mail и большинство веб-трафика.
- Другим недостатком является то, что прикладные прокси обрабатывают ограниченное количество сетевых программ и протоколов и не могут автоматически поддерживать новые сетевые программы и протоколы. Для каждого прикладного протокола, который должен проходить через межсетевой экран, необходим свой прокси сервер. Большинство производителей прикладных прокси предоставляют общий прокси сервер для поддержки неизвестных сетевых программ или протоколов. Однако этот общий прокси не имеют большинства преимуществ прикладных прокси, как правило он просто передает трафик через межсетевой экран.

# Окружение межсетевого экрана

Окружение межсетевого экрана является термином, используемым для описания множества систем и компонент, используемых для поддержки функционирования межсетевого экрана в конкретной сети. Простое окружение межсетевого экрана может состоять только из пакетного фильтра. В более сложном и безопасном окружении оно может состоять из нескольких межсетевых экранов и прокси со специальной топологией. Рассмотрим возможные сетевые топологии, используемые в качестве окружений межсетевого экрана.

## Принципы построения окружения межсетевого экрана

Существует четыре принципа, которым необходимо следовать:

1. **Простота (Keep It Simple)**

Данный принцип говорит о первом и основном, о чем надо помнить при разработки топологии сети, в которой функционирует межсетевой экран. Важно принимать наиболее простые решения, более безопасным является то, чем легче управлять. Трудно понимаемые функциональности часто приводит к ошибкам в конфигурации.

2. **Использовать устройства по назначению**

Использование сетевых устройств для того, для чего они первоначально предназначались, в данном контексте означает, что не следует делать межсетевые экраны из оборудования, которое не предназначено для использования в качестве межсетевого экрана.

3. **Создавать оборону вглубь**

Оборона вглубь означает создание нескольких уровней обороны в противоположность наличию единственного уровня. Не следует всю защиту обеспечивать исключительно межсетевым экраном.

4. **Уделять внимание внутренним угрозам**

Наконец, если уделять внимание только внешним угрозам, то это приводит в тому, что сеть становится открытой для атак изнутри. Хотя это и маловероятно, но следует рассматривать возможность, что нарушитель может как-то обойти межсетевой экран и получить свободу действий для атак внутренних или внешних систем. Следовательно,

важные системы, такие как внутренние веб- или e-mail сервера или финансовые системы, должны быть размещены позади внутренних межсетевых экранов.

В качестве итога можно заметить, что выражение «всю защиту можно взломать» особенно применимо к построению окружений межсетевого экрана. При развертывании межсетевых экранов следует помнить о перечисленных выше правилах при определении окружений, но в каждом случае могут иметь место свои собственные требования, возможно требующие уникальных решений.

## Демилитаризованные (DMZ) сети

**Слайд № 28.**В большинстве случаев окружение межсетевого экрана образует так называемую DMZ сеть или сеть демилитаризованной зоны. DMZ сеть является сетью, расположенной между двумя межсетевыми экранами.

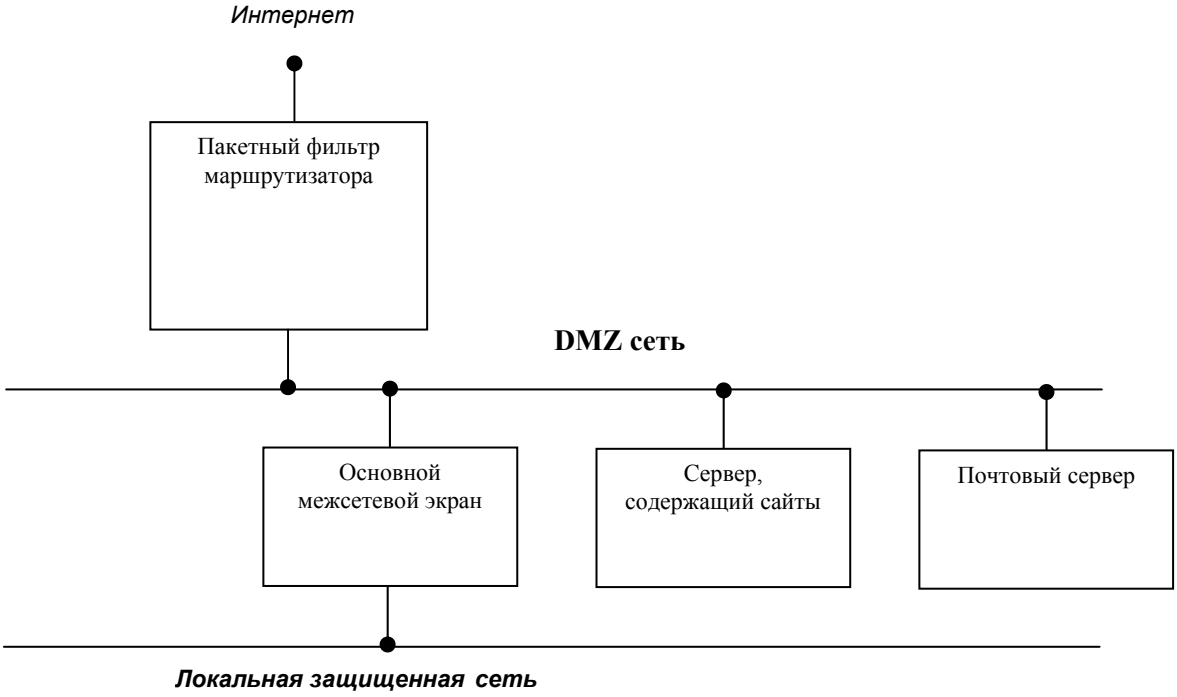


**Рис. 14 Пример окружения межсетевого экрана с DMZ-сетью**

DMZ сети предназначены для расположения систем и ресурсов, которым необходим доступ либо только извне, либо только из внутри, либо и извне, и изнутри, но которые не должны быть размещены во внутренних защищенных сетях. Это связано с тем, что никогда нельзя гарантировать, что эти системы и ресурсы не могут быть взломаны. Но взлом этих систем не должен автоматически означать доступ ко всем внутренним системам.

DMZ сети создаются между двумя межсетевыми экранами. Размещение компьютеров, к которым необходим доступ извне, в DMZ сети уменьшает вероятность того, что удаленные атакующие будут иметь возможность использовать эти сервера в качестве точки входа в локальные сети. Кроме того, размещение таких компьютеров в DMZ сетях позволяет межсетевым экранам служить дополнительными средствами для контроля прав доступа пользователей, которые получают доступ с использованием этих компьютеров к локальной сети.

# Системы обнаружения вторжения - Intrusion Detection Systems (IDS)

**Слайд № 29.**IDS являются программными или аппаратными системами, которые автоматизируют процесс просмотра событий, возникающих в компьютерной системе или сети, и анализируют их с точки зрения безопасности. Так как количество сетевых атак возрастает, IDS становятся необходимым дополнением инфраструктуры безопасности.

Обнаружение проникновения является процессом мониторинга событий, происходящих в компьютерной системе или сети, и анализа их для обнаружения *проникновений*, определяемых как попытки компрометации конфиденциальности, целостности, доступности или обхода механизмов безопасности компьютера или сети. Проникновения могут осуществляться как атакующими, получающими доступ к системам из интернет, так и авторизованными пользователями систем, пытающимися получить дополнительные привилегии, которых у них нет.

IDS состоят их трех компонентов: **источник** информации, **анализ** информации для обнаружения проникновения и создание **ответа**, если имеет место проникновение. Система получает информацию о событии из одного или более источников информации, выполняет определяемый конфигурацией анализ данных и затем создает специальные ответы, от простейших отчетов до активного вмешательства при определении проникновений.

## Почему следует использовать IDS

Обнаружение проникновения позволяет организациям защищать свои системы от угроз, которые связаны с возрастанием сетевой активности и важностью информационных систем. Понимая уровень и природу современных угроз сетевой безопасности, вопрос должен стоять не в том, что *следует ли* использовать системы обнаружения проникновений, а в том, *какие* возможности и особенности систем обнаружения проникновений следует использовать.

**Почему следует использовать IDS, особенно если уже имеются межсетевые экраны, антивирусные инструментальные средства и другие средства защиты?**

Каждое средство защиты адресовано конкретной угрозе безопасности в системе. Более того, каждое средство защиты имеет слабые и сильные стороны. Только комбинируя их (данная комбинация иногда называет *безопасностью в глубину*), можно защититься от максимально большого спектра атак.

Межсетевые экраны являются механизмами создания барьера, преграждая вход некоторым типам сетевого трафика и разрешая другие типы трафика. Создание такого барьера происходит на основе политики межсетевого экрана. IDS служат механизмами мониторинга, наблюдения активности и принятия решений о том, являются ли наблюдаемые события подозрительными. Они могут обнаружить атакующих, которые обошли межсетевой экран, и выдать отчет об этом администратору, который в свою очередь предпримет шаги по предотвращению атаки.

**Слайд № 30.**IDS становятся необходимым дополнением инфраструктуры безопасности в каждой организации. Технологии обнаружения проникновений не делают систему абсолютно безопасной. Тем не менее практическая польза от IDS существует, и не маленькая. Использовании IDS помогает достичь нескольких целей:

1. Возможность иметь реакцию на атаку позволяет заставить атакующего нести ответственность за собственную деятельность. Это определяется следующим

образом: *«Я могу прореагировать на атаку, которая произведена на мою систему, так как я знаю, кто это сделал или где его найти»*. Это трудно реализовать в сети интернет, где протоколы позволяют атакующим подделать идентификацию адресов источника или другие идентификаторы источника.

**2.** Возможность блокирования означает возможность распознать некоторую активность или событие как атаку и затем выполнить действие по блокированию источника. Данная цель определяется следующим образом: *«Я не забочусь о том, кто атакует мою систему, потому что я могу распознать, что атака имеет место и блокировать ее»*. Заметим, что требования реакции на атаку полностью отличаются от возможности блокирования.

Атакующие, используя свободно доступные технологии, могут получить неавторизованный доступ к системам, если найденные в системах уязвимости не исправлены, а сами системы подсоединены к публичным сетям.

Хотя объявления о появлении новых уязвимостей являются общедоступными, существует много ситуаций, в которых использование этих уязвимостей все же возможно:

- Во многих наследуемых системах не могут быть выполнены все необходимые обновления и модификации.
- Даже в системах, в которых обновления могут быть выполнены, администраторы иногда не имеют достаточно времени или ресурсов для отслеживания и инсталлирования всех необходимых обновлений. Это является общей проблемой, особенно в окружениях, включающих большое количество компьютеров или широкий спектр аппаратуры и программного обеспечения.
- Пользователям могут требоваться функциональности сетевых сервисов и протоколов, которые имеют известные уязвимости.
- Как пользователи, так и администраторы делают ошибки при конфигурировании и использовании систем.

В идеальном случае производители программного обеспечения должны минимизировать уязвимости в своих продуктах, и администраторы должны быстро и правильно корректировать все найденные уязвимости. Однако в реальной жизни это происходит редко, к тому же новые ошибки и уязвимости обнаруживаются ежедневно.

Поэтому обнаружение проникновения может являться отличным выходом из существующего положения, при котором обеспечивается дополнительный уровень защиты системы. IDS может определить, когда атакующий осуществил проникновение в систему, используя нескорректированную или некорректируемую ошибку. Более того, IDS может служить важным звеном в защите системы, указывая администратору, что система была атакована, чтобы тот мог ликвидировать нанесенный ущерб. Это гораздо предпочтительнее простого игнорирования угроз сетевой безопасности, что позволяет атакующему иметь продолжительный доступ к системе и хранящейся в ней информации.

**3.** Возможно определение преамбул атак, обычно имеющих вид сетевого зондирования или некоторого другого тестирования для обнаружения уязвимостей, и предотвращения их дальнейшего развития.

Когда нарушитель атакует систему, он обычно выполняет некоторые предварительные действия. Первой стадией атаки обычно является зондирование или проверка системы или сети на возможные точки входа. В системах без IDS атакующий может свободно тщательно анализировать систему с минимальным

риском обнаружения и наказания. Имея такой неограниченный доступ, атакующий в конечном счете может найти уязвимость и использовать ее для получения необходимой информации.

Та же самая сеть с IDS, просматривающей выполняемые операции, представляет для атакующего более трудную проблему. Хотя атакующий и может сканировать сеть на уязвимости, IDS обнаружит сканирование, идентифицирует его как подозрительное, может выполнить блокирование доступа атакующего к целевой системе и оповестит персонал, который в свою очередь может выполнить соответствующие действия для блокирования доступа атакующего. Даже наличие простой реакции на зондирование сети будет означать повышенный уровень риска для атакующего и может препятствовать его дальнейшим попыткам проникновения в сеть.

4. Выполнение документирования существующих угроз для сети и систем.

   При составлении отчета о бюджете на сетевую безопасность бывает полезно иметь документированную информацию об атаках. Более того, понимание частоты и характера атак позволяет принять адекватные меры безопасности.

5. Обеспечение контроля качества разработки и администрирования безопасности, особенно в больших и сложных сетях и системах.

   Когда IDS функционирует в течении некоторого периода времени, становятся очевидными типичные способы использования системы. Это может выявить изъяны в том, как осуществляется управление безопасностью, и скорректировать это управление до того, как недостатки управления приведут к инцидентам.

6. Получение полезной информации о проникновениях, которые имели место, предоставляя улучшенную диагностику для восстановления и корректирования вызвавших проникновение факторов.

   Даже когда IDS не имеет возможности блокировать атаку, она может собрать детальную, достоверную информацию об атаке. Данная информация может лежать в основе принятия соответствующих законодательных мер. В конечном счете, такая информация может определить проблемы, касающиеся конфигурации или политики безопасности.

7. IDS помогает определить расположение источника атак по отношению к локальной сети (внешние или внутренние атаки), что важно при принятии решений о расположении ресурсов в сети.

## Типы IDS

**Слайд № 31.**Существует несколько способов классификации IDS, каждый из которых основан на различных характеристиках IDS. Тип IDS следует определять, исходя из следующих характеристик:

- *Способ мониторинга системы*. По способам мониторинга системы делятся на сетевые и предназначенные для отдельного компьютера.
- *Способ анализа*. Это часть системы определения проникновения, которая анализирует события, полученные из источника информации, и принимает решения, что имеет место проникновение. Способами анализа являются обнаружение злоупотреблений (misuse detection) и обнаружение аномалий (anomaly detection).
- *Задержка во времени* между получением информации из источника и ее анализом и принятием решения. В зависимости от задержки во времени IDS делятся на

работающие в течении определенного интервала (или в пакетном режиме) и непрерывно работающие системы. **Слайд № 32.**

Большинство коммерческих IDS являются непрерывно работающими сетевыми системами.

К характеристикам IDS также относятся:

- *Источник информации* – IDS может использовать различные источники информации о событии для определения того, что проникновение имело место. Эти источники могут быть получены из различных уровней системы, из сети, компьютера и отдельной программы.
- *Ответ* – набор действий, которые выполняет система после определения проникновений. Они обычно разделяются на активные и пассивные меры, при этом под активными мерами понимается автоматическое вмешательство в некоторую другую систему, под пассивными мерами понимается отчет IDS, сделанный для людей, которые затем выполнят некоторое действие на основе данного отчета.

## Архитектура IDS

Архитектура IDS определяет, какие имеются функциональные компоненты IDS и как они взаимодействуют друг с другом. Основными архитектурными компонентами являются: Host - система, на которой выполняется программное обеспечение IDS, и Target - система, за которой IDS наблюдает.

### *Совместное расположение Host и Target*

Первоначально многие IDS выполнялись на тех же системах, которые они защищали. Основная причина этого была в том, что большинство систем относилось к классу так называемых «больших компьютеров», и стоимость выполнения IDS на отдельном компьютере была очень большой. Это создавало проблему с точки зрения безопасности, так как любой атакующий, который успешно атаковал целевую систему, мог в качестве одной из компонент атаки просто запретить функционирование IDS.

### *Разделение Host и Target*

С появлением рабочих станций и персональных компьютеров в большинстве архитектур IDS предполагается выполнение IDS на отдельном компьютере, тем самым разделяя системы Host и Target. Это улучшает безопасность функционирования IDS, так как в этом случае проще спрятать существование IDS от атакующих.

Современные IDS как правило состоят из следующих компонент:

- Сенсор, который отслеживает события в сети или системе.
- Анализатор событий, обнаруженных сенсорами.
- Компонента принятия решения.

## Способы управления

Стратегия управления описывает, каким образом можно управлять элементами IDS, их входными и выходными данными.

В сети должны поддерживаться следующие связи:

- Связи для передачи отчетов IDS. Эти связи создаются между сенсорами как сетевого мониторинга, так и мониторинга компьютера, и центральной консолью IDS.
- Связи для мониторинга компьютеров и сетей.
- Связи для выполнения ответов IDS.

## Скорость реакции

Скорость реакции указывает на время, прошедшее между событиями, которые были обнаружены сенсором, анализом этих событий и реакцией на них.

1. **IDS, реакция которых происходит через определенные интервалы времени (пакетный режим)**

В IDS, реакция которых происходит через определенные интервалы времени, информационный поток от точек мониторинга до инструментов анализа не является непрерывным. В результате информация обрабатывается способом, аналогичным коммуникационным схемам «сохранить и перенаправить». Многие ранние IDS, работающие на компьютере, используют данную схему хронометража, так как они зависят от записей аудита в ОС. Основанные на интервале IDS не выполняют никаких действий, являющихся результатом анализа событий.

2. **Real-Time (непрерывные)**

Real-time IDS обрабатывают непрерывный поток информации от источников. Чаще всего это является преобладающим способом в сетевой IDS, которые получают информацию из потока сетевого трафика. Термин «реальное время» означает, что определение проникновения, выполняемое такой IDS, приводит к результатам достаточно быстро, что позволяет IDS выполнять определенные действия в автоматическом режиме.

### *Сетевая IDS*

Основными коммерческими IDS являются сетевые. Эти IDS определяют атаки, захватывая и анализируя сетевые пакеты. Сетевая IDS может просматривать сетевой трафик от нескольких компьютеров, которые присоединены к сетевому сегменту, и таким образом защищать эти компьютеры.

### *IDS для отдельного компьютера*

Эти IDS имеют дело с информацией, собранной внутри единственного компьютера. Такое выгодное расположение позволяет этим IDS анализировать деятельность с большой достоверностью и точностью, определяя только те процессы и пользователей, которые имеют отношение к конкретной атаке в ОС. Более того, в отличии от сетевых IDS, IDS для отдельного компьютера могут «видеть» последствия предпринятой атаки, так как они могут иметь непосредственный доступ к системной информации и файлам данных и системным процессам, являющихся целью атаки.

## Анализ, выполняемый IDS

Существует два основных подхода к анализу событий для определения атак: **определение злоупотреблений** (misuse detection) и **определение аномалий** (anomaly detection).

В технологии определения злоупотреблений известно, какая последовательность данных является признаком атаки. Анализ событий состоит в определении таких «плохих»

последовательностей данных. Технология определения злоупотреблений используется в большинстве коммерческих систем.

В технологии определения аномалий известно, что представляет собой «нормальная» деятельность и «нормальная» сетевая активность. Анализ событий состоит в попытке определить аномальное поведение пользователя или аномальную сетевую активность. Данная технология на сегодняшний день является предметом исследований и используется в ограниченной форме небольшим числом IDS. Существуют сильные и слабые стороны, связанные с каждым подходом; считается, что наиболее эффективные IDS используют в основном определение злоупотреблений с небольшими компонентами определения аномалий.

## *Определение злоупотреблений*

Детекторы злоупотреблений анализируют деятельность системы, анализируя событие или множество событий на соответствие заранее определенному образцу, который описывает известную атаку. Соответствие образца известной атаке называется *сигнатурой*, определение злоупотребления иногда называют «сигнатурным определением». Наиболее общая форма определения злоупотреблений, используемая в коммерческих продуктах, определяет каждый образец событий, соответствующий атаке, как отдельную сигнатуру. Тем не менее существует несколько более сложных подходов для выполнения определения злоупотреблений (называемых «state-based» технологиями анализа), которые могут использовать единственную сигнатуру для определения группы атак.

***Преимущества сигнатурного метода:***

- Детекторы злоупотреблений являются очень эффективными для определения атак, не создавая при этом огромного числа ложных сообщений.
- Детекторы злоупотреблений могут быстро и надежно диагностировать использование конкретного инструментального средства или технологии атаки. Это может помочь администратору скорректировать меры обеспечения безопасности.
- Детекторы злоупотреблений позволяют администраторам, не зависимо от уровня их квалификации в области безопасности, использовать IDS.

***Недостатки сигнатурного метода:***

- Детекторы злоупотреблений могут определить только те атаки, о которых они знают. Следовательно, надо постоянно обновлять их базы данных для получения сигнатур новых атак.
- Многие детекторы злоупотреблений разработаны таким образом, что могут использовать только строго определенные сигнатуры, что не допускает определения вариантов общих атак. State-based детекторы злоупотреблений могут обойти данное ограничение, но они не очень широко используются в коммерческих IDS.

## *Определение аномалий*

Детекторы аномалий определяют ненормальное (необычное) поведение на компьютере или в сети. Они предполагают, что атаки отличаются от «нормальной» (законной) деятельности и могут, следовательно, быть определены системой, которая может отслеживать эти отличия. Детекторы аномалий хранят информацию о нормальном поведении пользователей, компьютеров или сетевого трафика. Эти информация получается из данных истории, собранных в период нормального функционирования. Затем детекторы собирают данные о событиях и используют различные методики для определения того, что анализируемая деятельность отклоняется от нормальной.

Хотя некоторые коммерческие IDS включают ограниченные формы определения аномалий, мало кто полагается исключительно на данную технологию. Определение аномалий, которое существует в коммерческих системах, обычно используется для определения зондирования сети или сканирования портов. Тем не менее, определение аномалий остается предметом исследований в области активного определения проникновений, и скорее всего будет играть возрастающую роль в IDS следующих поколений.

***Преимущества определения аномалий:***

- IDS, основанные на определении аномалий, обнаруживают неожиданное поведение и, таким образом, имеют возможность определить симптомы атак без знания конкретных деталей атаки.
- Детекторы аномалий могут создавать информацию, которая в дальнейшем будет использоваться для определения сигнатур для детекторов злоупотреблений.

***Недостатки определения аномалий:***

- Подходы определения аномалий обычно создают большое количество ложных сигналов при непредсказуемом поведении пользователей и непредсказуемой сетевой активности.
- Подходы определения аномалий часто требуют некоторого этапа обучения системы, во время которого определяются характеристики нормального поведения.

## Возможные ответные действия IDS

После того, как IDS получила информацию о событии и проанализировав ее, обнаружила симптомы атаки, она должна как-то прореагировать на это. В некотором случае реакция может представлять собой отчеты, созданные в некотором стандартном формате. Другой реакцией могут быть определенные действия. Хотя часто недооценивают важность наличия хороших ответов в IDS, на самом деле наличие разнообразных возможностей в ответах очень важно. Коммерческие IDS поддерживают широкий диапазон опций ответов, часто разбивая их на активные ответы, пассивные ответы и некоторую смесь из них.

### *Активные действия*

Активные ответы представляют собой автоматизированные действия, которые выполняются, когда определены конкретные типы проникновений. Существует три категории активных ответов.

***Сбор дополнительной информации***

Наиболее безвредный, но часто наиболее продуктивный активный ответ состоит в сборе дополнительной информации о предполагаемой атаке. Это может включать возрастающий уровень внимания к источникам информации. Например, можно начать собирать большее количество информации и настроить сетевой сенсор на перехват всех пакетов, а не только тех, которые предназначены конкретному порту или компьютеру. Сбор дополнительной информации производится по нескольким причинам. Во-первых, собранная дополнительная информация может помочь обнаружить атаку. Во-вторых, позволяет получить информацию, которая затем может использоваться при юридическом расследовании и задержании атакующего.

***Изменение окружения***

Другое активное действие состоит в том, чтобы остановить выполняемую атаку и затем блокировать последующий доступ атакующим. Обычно IDS не имеют возможностей

блокировать доступ конкретного человека, но вместо этого могут блокировать IP адреса, с которых вошел атакующий.

***Выполнение действия против атакующего***

В некоторых дискуссиях обсуждается, что первой опцией в активном ответе должно быть выполнение действия против проникающего. Наиболее агрессивная форма данного ответа включает запуск атаки против него или попытка активного сбора информации о компьютере или сети атакующего. Тем не менее, сколь бы это не было заманчиво, такой ответ не рекомендуется. С точки зрения закона данный ответ может быть более наказуем, чем атака, которую предполагается блокировать.

Первой причиной, по которой данную опцию следует использовать с большой осторожностью, являются требования законодательства. Более того, так как многие атакующие используют подделанные сетевые адреса, это может нанести большой вред невинным компьютерам и пользователям. Наконец, ответный удар может спровоцировать атакующего, который первоначально намеревался только просмотреть компьютер жертвы, не выполняя более никаких агрессивных действий.

Рекомендуется проконсультироваться с законодательством перед тем, как использовать какие-либо опции «ответного удара».

## *Пассивные действия*

Пассивные ответы IDS предоставляют информацию пользователям системы, предполагая, что человек сам выполнит дальнейшие действия на основе данной информации. Многие коммерческие IDS предполагают исключительно пассивные ответы.

***Тревоги и оповещения***

Тревоги и оповещения создаются IDS для информирования администраторов об обнаружении атак. Большинство коммерческих IDS позволяют администраторам определять детали того, какие и когда тревоги создаются и кому и как они передаются.

Чаще всего сигнал тревоги выводится на экран или в выпадающее окно на консоли IDS или других систем, что может быть указано администратором при конфигурировании IDS. Информация, указываемая в сообщении о тревоги, может сильно отличаться, от простого уведомления, что имеет место проникновение, до очень детализированных сообщений, указывающих IP адреса источника и цели атаки, конкретное инструментальное средство атаки, используемое для получения доступа, и результат атаки.

Другим множеством опций, используемых в больших или распределенных организациях, является возможность удаленного оповещения о тревогах. Это позволяет организации сконфигурировать IDS таким образом, чтобы она посылала сообщение о тревоги на сотовые телефоны.

В некоторых случаях также можно, например, использовать e-mail в качестве канала передачи сообщений об атаках. Это не всегда продуманно, так как атакующий может иметь возможность просматривать исходящий e-mail трафик и блокировать это сообщение.