Предварительные вопросы

1. **Что такое компьютер (ЭВМ)**

Многофункциональное программируемое устройство, позволяющее вводить, обрабатывать и выводить информацию, решая различные прикладные задачи.

2. **Что такое компьютерная сеть**

Совокупность компьютеров и/или компьютерного оборудования использующих коммуникационную сеть для обмена информацией

Промежуточные вопросы

1. **Как происходит передача информации в сети**

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**.

2. **Что такое протокол и стек протоколов**

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.

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**.

3. **Как обеспечивается 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:

- 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.
- 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.

4. Как обеспечивается защита информационной системы

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 межсетевые экраны (firewalls), которые предотвращают атаки, 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.

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

5. Что такое алгоритм 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.

6. Что такое межсетевые экраны

Межсетевые экраны являются аппаратными устройствами или программными системами, которые разрешают или запрещают прохождение сетевого трафика между сетями с различными требованиями к безопасности.

7. Что такое пакетные фильтры

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.

8. Что такое прокси сервер прикладного уровня

Прокси прикладного уровня являются более мощными межсетевыми экранами, которые комбинируют управление доступом на низком уровне с функциональностью прикладного уровня.

9. Что такое Демилитаризованные (DMZ) сети

В большинстве случаев окружение межсетевого экрана образует так называемую DMZ сеть или сеть демилитаризованной зоны. DMZ сеть является сетью, расположенной между двумя межсетевыми экранами.

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.

10. Что такое системы обнаружения вторжения - Intrusion Detection Systems (IDS)

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.

11. Какие существуют способы классификации IDS

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.

Итоговые вопросы

Основные понятия, относящиеся к защите информации

1. **Уязвимость**

Слабое место в системе, с использованием которого может быть осуществлена атака.

2. **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.

3. **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.

4. **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*.

5. **Механизм безопасности**

Программное или аппаратное средство, которое определяет или предотвращает атаку.

6. **Сервис безопасности**

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

7. **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**.

8. **Активная атака**

Активной называется такая атака, при которой противник имеет возможность **модифицировать передаваемые сообщения и вставлять свои сообщения**.

9. 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.

10. 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.

11. 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.

12. 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.

13. Контроль доступа

Возможность ограничить и контролировать доступ к компьютерам и программам по коммуникационным линиям.

14. Доступность

Результатом атак может быть потеря или снижение доступности того или иного сервиса. Данный сервис предназначен для того, чтобы минимизировать возможность осуществления DoS-атак.

15. 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**.

16. 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**.

17. 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.