Информационная безопасность

Работу выполнили:
сту-ты ЭФ гр-пы БИН-22(оз)
Дьяконова Ю,
Сидикова Д.

Информационная безопасность

-это задача направленная на обеспечение безопасности, реализуемая внедрением системы безопасности.

Свойства информации

- **доступность –** возможность получения информации или информационной услуги за приемлемое время;
- **целостность –** свойство актуальности и непротиворечивости информации, ее защищенность от разрушения и несанкционированного изменения;
- **конфиденциальность –** защита от несанкционированного доступа к информации.

Взаимосвязь определений

- **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.
- **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.

Классификация атаки и угрозы информации

Классификация атак на информационную систему может быть выполнена по нескольким признакам:

- По месту возникновения:
  - Локальные атаки (источником данного вида атак являются пользователи и/или программы локальной системы);
  - Удаленные атаки (источником атаки выступают удаленные пользователи, сервисы или приложения);
- По воздействию на информационную систему
  - Активные атаки (результатом воздействия которых является нарушение деятельности информационной системы);
  - Пассивные атаки (ориентированные на получение информации из системы, не нарушая функционирование информационной системы);

Классификация сетевых атак

I. Пассивная атака

II. Активная атака

а) Отказ в обслуживании

б) Модификация потока данных

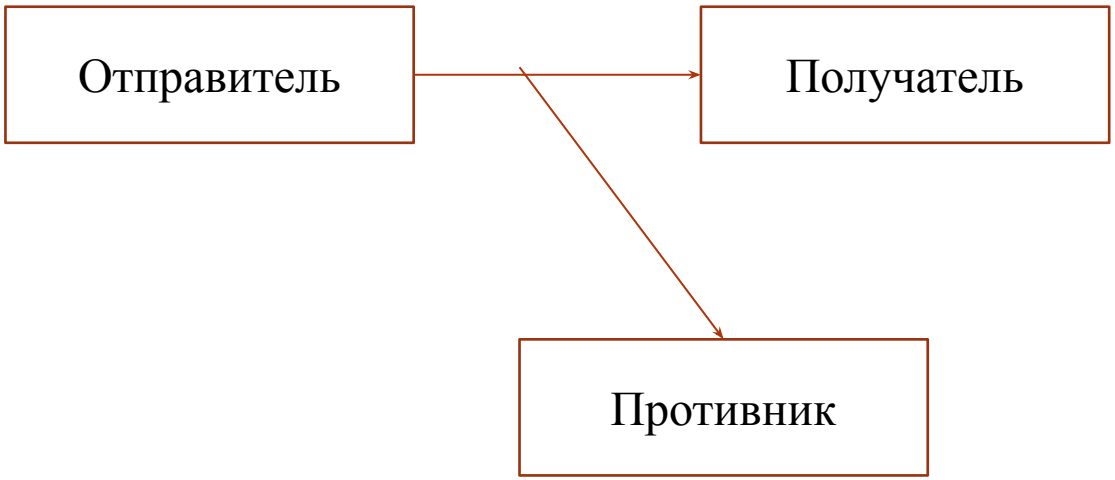
в) Создание ложного потока (фальсификация)

г) Повторное использование

Сетевые атаки

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.



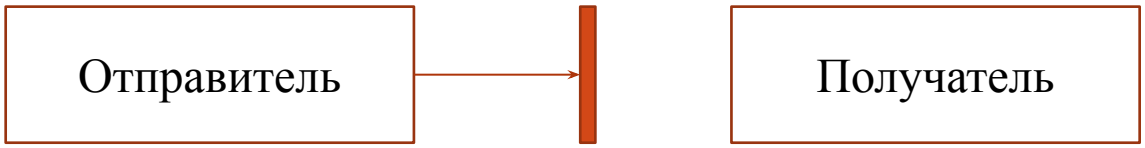
Сетевые атаки

II. Активная атака

- 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)*

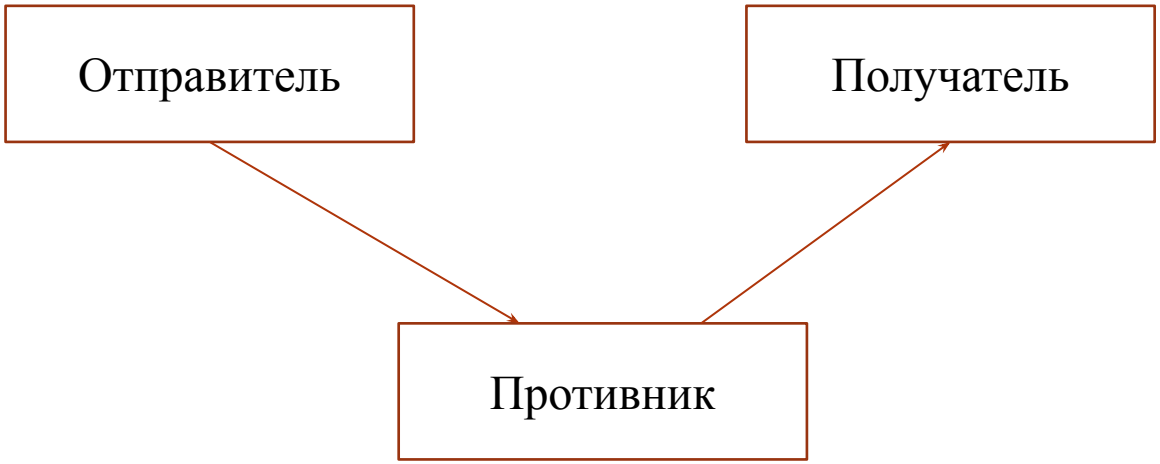
- Отказ в обслуживании нарушает нормальное функционирование сетевых сервисов. *Противник* может перехватывать все сообщения, направляемые определенному адресату. Другим примером подобной *атаки* является создание значительного трафика, в результате чего сетевой сервис не сможет обрабатывать запросы законных 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.



Сетевые атаки

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

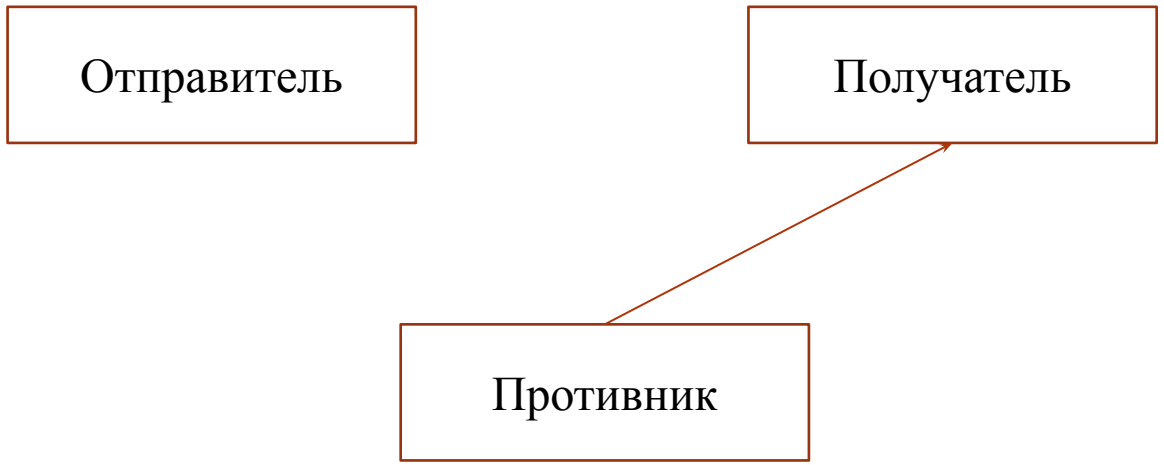
- Модификация потока данных означает либо изменение содержимого пересылаемого сообщения, либо изменение порядка сообщений.



Сетевые атаки

3) Создание ложного потока (фальсификация)

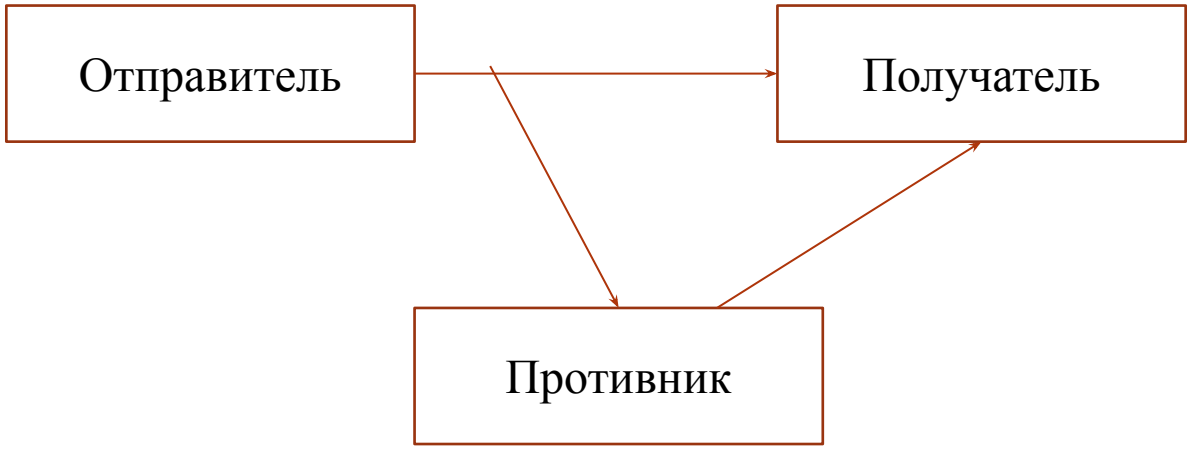
- *Фальсификация* (нарушение аутентичности) означает попытку одного субъекта выдать себя за другого



Сетевые атаки

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*.



Сервисы безопасности

- ***Конфиденциальность;***
- ***Аутентификация;***
- ***Целостность;***
- ***Невозможность отказа;***
- ***Контроль доступа;***
- ***Доступность.***

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

Задачи 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

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.

Методы обеспечения ИБ

- **препятствие** – метод физического преграждения пути злоумышленнику к информации;
- **управление доступом** – метод защиты с помощью регулирования использования информационных ресурсов системы;
- **маскировка** – метод защиты информации путем ее криптографического преобразования;
- **регламентация** – метод защиты информации, создающий условия автоматизированной обработки, при которых возможности несанкционированного доступа сводится к минимуму;
- **принуждение** – метод защиты, при котором персонал вынужден соблюдать правила обработки, передачи и использования информации;
- **побуждение** – метод защиты, при котором пользователь побуждается не нарушать режимы обработки, передачи и использования информации за счет соблюдения этических и моральных норм.

Средства защиты информационных систем

- **технические средства** – различные электрические, электронные и компьютерные устройства;
- **физические средства** – реализуются в виде автономных устройств и систем;
- **программные средства** – программное обеспечение, предназначенное для выполнения функций защиты информации;
- **криптографические средства** – математические алгоритмы, обеспечивающие преобразования данных для решения задач информационной безопасности;
- **организационные средства** – совокупность организационно-технических и организационно-правовых мероприятий;
- **морально-этические средства** – реализуются в виде норм, сложившихся по мере распространения ЭВМ и информационных технологий;
- **законодательные средства** – совокупность законодательных актов, регламентирующих правила пользования ИС, обработку и передачу информации.