Проблема информационной безопасности

Выполнили: ученицы 11 класса
Чекамасова Карина
Лысенко Валентина
Ластовская Яна
Стадник Екатерина

Содержание

1.Понятие информационной безопасности

2.Проблемы информационной безопасности

3.Угрозы информационной безопасности

4.Свойства информации

5. Примеры реализации угрозы нарушения конфиденциальности

6.Примеры реализации угрозы нарушения целостности данных

7.Вредоносное программное обеспечение

8.Понятие атаки на информационную систему

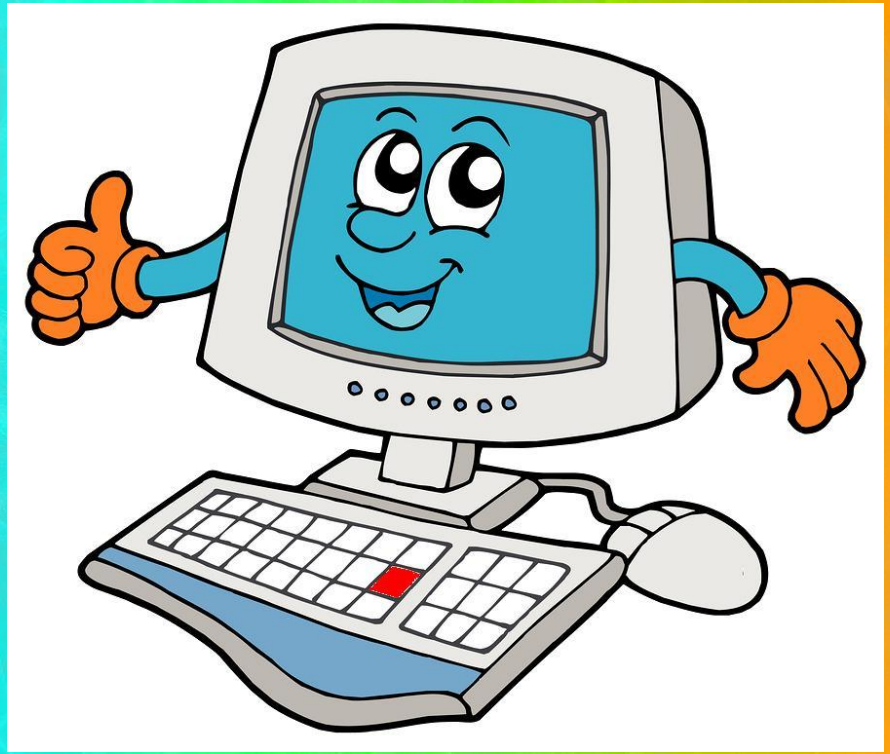
9.Классификация атак

10.Сетевые атаки

11.Средства защиты информационных систем

Понятие информационной безопасности

Под информационной безопасностью понимается защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений.



Проблемы информационной безопасности

Информационная безопасность является одним из важнейших аспектов интегральной безопасности. Иллюстрациями являются следующие факты: В Доктрине информационной безопасности РФ защита от НСД к информационным ресурсам, обеспечение безопасности информационных и телекоммуникационных систем выделены в качестве важных составляющих национальных интересов;В 1995 году было похищено 250 миллиардов рублей. По сведениям ФБР ущерб от компьютерных преступлений в США в 1997 г. составил 136 миллионов долларов.

Угрозы информационной безопасности

Угроза информационной безопасности (ИБ) – потенциально возможное событие, действие, процесс или явление, которое может привести к нанесению ущерба чьим-либо интересам. Попытка реализации угрозы называется атакой. Классификацию угроз ИБ можно выполнить по нескольким критериям: по аспекту ИБ (доступность, целостность, конфиденциальность); по компонентам ИС, на которые угрозы нацелены (данные, программа, аппаратура, поддерживающая инфраструктура); по способу осуществления (случайные или преднамеренные действия природного или техногенного характера); по расположению источника угроз (внутри или вне рассматриваемой ИС).

Свойства информации

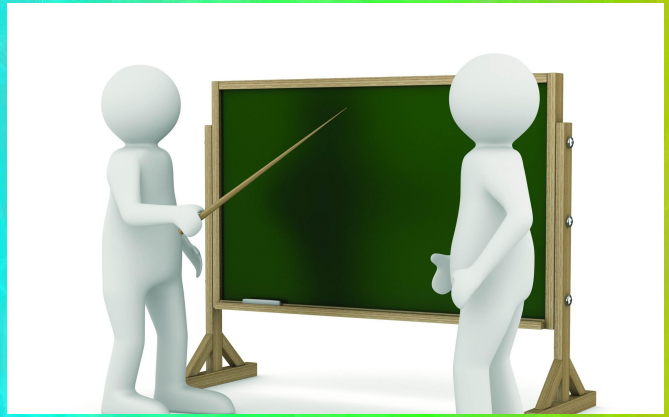
Вне зависимости от конкретных видов угроз информационная система должна обеспечивать базовые свойства информации и систем ее обработки: доступность – возможность получения информации или информационной услуги за приемлемое время; целостность – свойство актуальности и непротиворечивости информации, ее защищенность от разрушения и несанкционированного изменения; конфиденциальность – защита от несанкционированного доступа к информации.

Примеры реализации угрозы нарушения конфиденциальности

Часть информации, хранящейся и обрабатываемой в ИС, должна быть сокрыта от посторонних. Передача данной информации может нанести ущерб как организации, так и самой информационной системе. Конфиденциальная информация может быть разделена на предметную и служебную. Служебная информация (например, пароли пользователей) не относится к определенной предметной области, однако ее раскрытие может привести к несанкционированному доступу ко всей информации. Предметная информация содержит информацию, раскрытие которой может привести к ущербу (экономическому, моральному) организации или лица. Средствами атаки могут служить различные технические средства (подслушивание разговоров, сети), другие способы (несанкционированная передача паролей доступа и т.п.). Важный аспект – непрерывность защиты данных на всем жизненном цикле ее хранения и обработки. Пример нарушения – доступное хранение резервных копий данных.

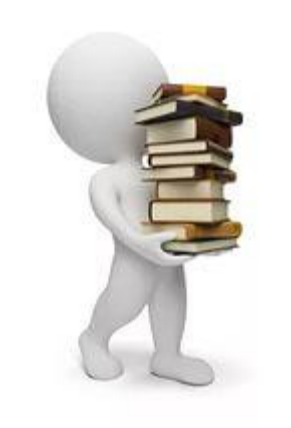
Примеры реализации угрозы нарушения целостности данных

Одними из наиболее часто реализуемых угроз ИБ являются кражи и подлоги. В информационных системах несанкционированное изменение информации может привести к потерям. Целостность информации может быть разделена на статическую и динамическую. Примерами нарушения статической целостности являются: ввод неверных данных; несанкционированное изменение данных; изменение программного модуля вирусом; Примеры нарушения динамической целостности: нарушение атомарности транзакций; дублирование данных; внесение дополнительных пакетов в сетевой трафик.



Вредоносное программное обеспечение

Одним из способов проведения атаки является внедрение в системы вредоносного ПО. Данный вид программного обеспечения используется злоумышленниками для: внедрения иного вредоносного ПО; получения контроля над атакуемой системой; агрессивного потребления ресурсов; изменение или разрушение программ и/или данных. По механизму распространения различают: вирусы – код, обладающий способностью к распространению путем внедрения в другие программы; черви – код, способный самостоятельно вызывать распространение своих копий по ИС и их выполнение.



Понятие атаки на информационную систему

Атака – любое действие или последовательность действий, использующих уязвимости 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 атак

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);

Сетевые атаки

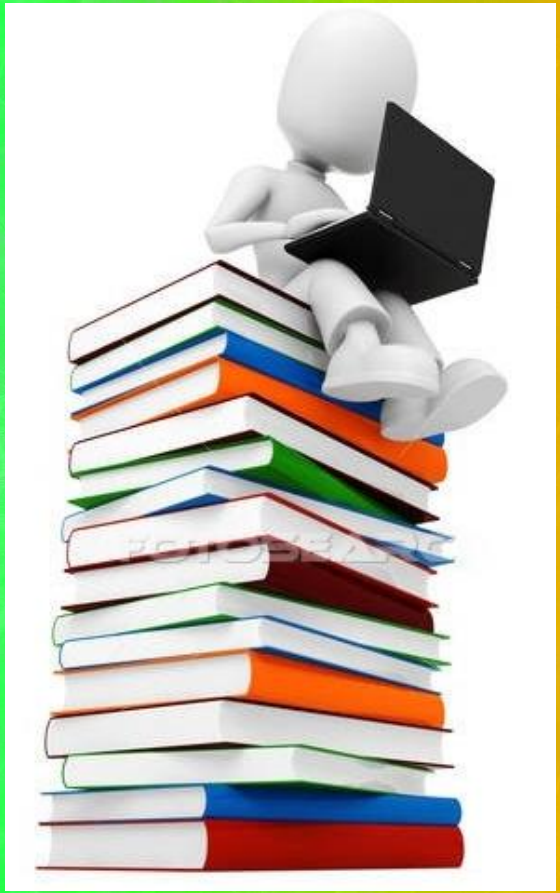
-Пассивная атака

-Активная атака

-Модификация потока данных

-Создание ложного потока(фальсификация)

-Повторное использование



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.

Активная атака

Активной называется такая атака, при которой противник имеет возможность модифицировать передаваемые сообщения и вставлять свои сообщения. Отказ в обслуживании - DoS-атака (Denial of Service) 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.

Модификация потока данных

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

Создание ложного потока(фальсификация)

(нарушение аутентичности) означает попытку одного субъекта выдать себя за другого .

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.

Средства защиты информационных систем

Такие средства могут быть классифицированы по следующим признакам: 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.

Спасибо за внимание!