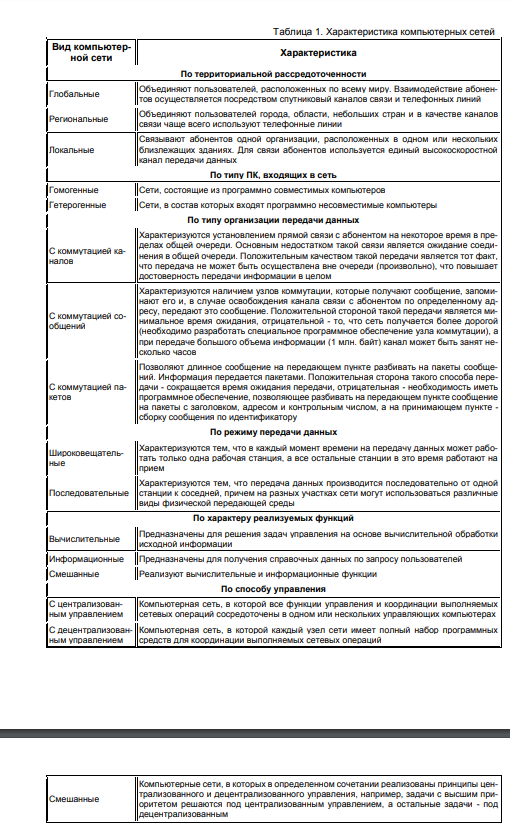
1. Компьютерная сеть – система взаимосвязанных и распределённых компьютеров, ориентированных на коллективное использование ресурсов сети, в качестве которых используются аппаратные, программные и информационные ресурсы
2. Информационные ресурсы – базы данных общего и индивидуального применения, ориентированные на решаемые в сети задачи
3. Аппаратные ресурсы сети – компьютеры различных типов, средства территориальных систем связи, аппаратура связи и согласования работы сетей одного и того же уровня или различных уровней.
4. Программные ресурсы сети - комплекс программ для планирования, организации и осуществления коллективного доступа пользователей к общесетевым ресурсам, автоматизации процессов обработки информации, динамического распределения и перераспределения общесетевых ресурсов с целью повышения оперативности и надежности удовлетворения запросов пользователей.
5. Назначение
   1. Обеспечить надёжный и быстрый доступ пользователей к ресурсам сети и организовать коллективную эксплуатацию этих ресурсов
   2. Обеспечить возможность оперативного перемещения информации на любые расстояния с целью своевременного получения данных для принятия управленческих решений
6. Возможности
   1. Организация параллельной обработки данных нескольких пк
   2. Создавать распределённые базы данных, распределяемых в памяти различных компьютеров
   3. Специализировать отдельные компьютеры для эффективного решения определённых классов задач
   4. Автоматизировать обмен информацией и программами между отдельными компьютерами и пользователями
   5. Резервировать вычислительные мощности и средства передачи данных на случай выхода из строя отдельных ресурсов сети с целью быстрого восстановления нормальной работы сети.
   6. Перераспределять вычислительные мощности между пользователями сети в зависимости от изменения потребностей и сложности решаемых задач
   7. Сочетать работу в различных режимах: диалоговом, пакетном, режиме «запрос-ответ», режиме сбора, передачи и обмена информацией.
7. Классификация компьютерных сетей
   1. По территориальной распределенности
      1. Глобальные
      2. Региональные
      3. Локальные
   2. По типу ПУ, входящих в сеть
      1. Гомогенные
      2. Гетерогенные
   3. По типу организации передачи данных
      1. С коммутацией каналов
      2. С коммутацией сообщений
      3. С коммутацией пакетов
   4. По режиму передачи данных
      1. Широковещательные
      2. Последовательные
   5. По характеру реализуемых функций
      1. Вычислительные
      2. Информационные
      3. Смешанные
   6. По способу управления
      1. С децентрализованным управлением
      2. С централизованным управлением
      3. Со смешанным управлением



1. Компоненты ЛВС. Локальная вычислительная сеть.
   1. Рабочая станция – ПК, подключённый к сети, через который пользователь получает доступ к сетевым ресурсам. Работает как локально так и в сети. Предоставляет инструментарий для решения задачи пользователем.
   2. Сервер – компьютер, выполняющий функции управления сетевыми ресурсами общего доступа: хранение, управление базами данных и т.д.
   3. Сетевой адаптер (сетевая карта) – периферийное устройство ПК, непосредственно взаимодействующее со средой передачи данных и связывает ПК с другими ПК. Также способны распознавать ошибки из-за помех, коллизий и пр. неполадок сети.
   4. Повторители и концентратор. Повторитель повторяет сигнал, улучшая электрические характеристики сигналов и их синхронность, что позволяет увеличить общую длину кабеля. Концентратор, или хаб, не только повторяет сигнал, но и позволяет объединить несколько устройств в одну сеть. Также позволяет объединить сегменты сети с различными физ. средами в один, автоматически отключать неисправные порты, поддержка резервных связей, защита передаваемых по сети данных.
   5. Мосты и коммутаторы. Оба делят общую среду передачи данных на логические сегменты, путём группировки нескольких физических сегментов в один логический. При поступлении сигнала, в отличие от повторителя, пересылает сигнал не всем, а только по одному логическому сегменту, на котором находится адресат. Мост обрабатывает кадры последовательно, коммутатор – параллельно.
   6. Маршрутизатор. Обмен информацией об изменении структуры сети, трафике и состоянии и выбирает оптимальный маршрут следования блока данных в разных сетях. Обеспечивают соединение административно независимо коммуникационных сетей
   7. Шлюз. Наиболее сложная ретрансляционная система, обеспечивающая взаимодействие с различными протоколами. Шлюзы оперируют на верхних уровнях модели OSI (сеансовом, представительском и прикладном) и представляют наиболее развитый метод подсоединения сетевых сегментов и компьютерных сетей. Необходимость возникает при объединении двух систем, имеющих разную архитектуру. Простым языком, своеобразный «переводчик» между двумя системами. Часто является отдельным компьютером
   8. Канал связи позволяет быстро и надёжно передавать информацию между различными устройствами локальной вычислительной сети.
      1. Кабельные
         1. Оптические (оптоволокно)
         2. Электрические (витая пара, коаксиль)
      2. Беспроводные (радио, связь в микроволновом диапазон, связь в ИК-диапазоне)
2. НСД – доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники (СВТ) или автоматизированными системами (АС)
3. Основные угрозы НСД
   1. Угрозы проникновения в операционную среду компьютера с использованием штатного ПО
   2. Угрозы создания нештатных режимов работы программно (аппаратных) средств за счёт преднамеренных изменений служебных данных, игнорирования предусмотренных в штатных условиях ограничений на состав и характеристики обрабатываемой информации, искажения (модификации) самих данных и т.п.;
   3. Угрозы внедрения вредоносных программ
   4. Комбинированные угрозы
4. Классификация нарушителей по времени действия.
   1. В процессе функционирования АС
   2. В период неактивности компонентов системы
   3. Как в процессе функционирования, так и нефункционирования
5. Классификация нарушителей по месту действия.
   1. без доступа на контролируемую территорию организации;
   2. с контролируемой территории без доступа в здания и сооружения;
   3. внутри помещений, но без доступа к техническим средствам АС;
   4. с рабочих мест конечных пользователей (операторов) АС;
   5. с доступом в зону данных (серверов баз данных, архивов и т.п.);
   6. с доступом в зону управления средствами обеспечения безопасности АС.
6. Злоумышленник - нарушитель, намеренно идущий на нарушение. Внешний нарушитель осуществляет НСД через автоматизированные рабочие места, подключенные к сетями общего пользования, с помощью программного воздействитя на защищаемую информацию, через элементы автоматизированной системы, которые побывали за пределами контролируемой зоны
7. Атаки в сетях на основе стека протоколов TCP/IP (перечень).
   1. Анализ сетевого трафика
   2. Сканирование сети
   3. Выявление пароля
   4. IP-spoofing или подмена доверенного объекта сети
   5. Отказ в обслуживании или Denial of Service (DoS)
   6. Атаки на уровне приложений
8. Атаки в сетях. Анализ сетевого трафика.

При нормальном режиме работы сетевой карты пакеты, у которых не совпадает MAC-адрес с MAC-адресом сетевой карты, отбрасываются. Однако при использовании программы-сниффера можно включить promiscuous mode (неразборчивый режим), при котором эти ограничения отключаются. Таким образом могут быть получены пароли при отправке данных через протоколы FTP, SMTP, POP3 и другие данные. Защититься можно сильной аутентификацией, например одноразовыми паролями, антиснифферами, коммутируемой инфраструктурой или криптографическими методами.

1. Атаки в сетях. Сканирование сети

Выявляет работающие в сети службы, открытые порты, активные сетевые сервисы, протоколы и прочую информацию о сети. Использует DNS-запросы, эхо-тестирование, сканирование портов. Контрмерой является IDS, который выявляет попытки «скана» системы и уведомляет администратора.

1. Атаки в сетях. Выявление пароля

Получение НСД путём преодоления пароля. Самый простой способ – обычный перебор пароля. Контрмера – сложные пароли, использование разных паролей, использование одноразовых паролей и криптографии.

1. Атаки в сетях. IP-spoofing или подмена доверенного объекта сети

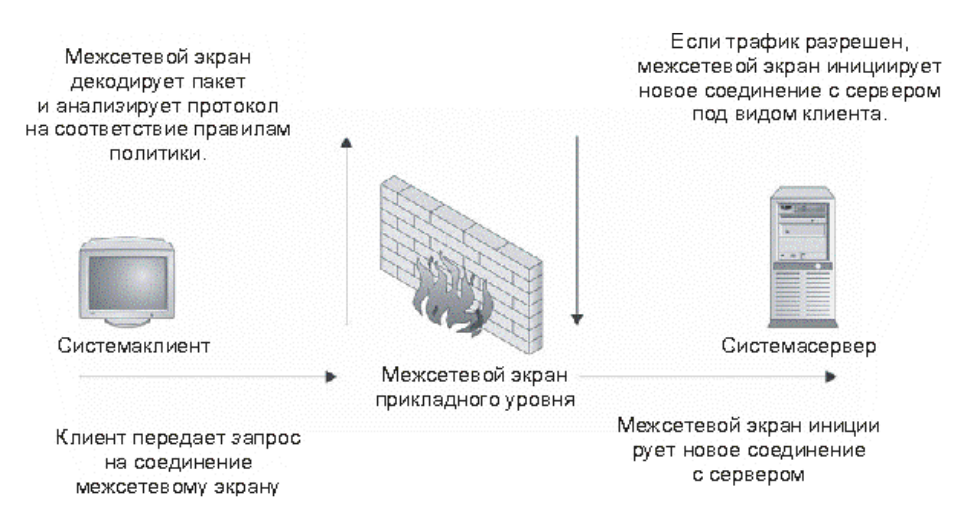
Доверенный объект – любой объект в сети, легально подключенный к серверу. Злоумышленник при таком способе выдаёт себя за доверенный объект. Для атаки такого вида можно воспользоваться IP-адресом, находящимся в пределах диапазона санкционирования. Для ослабления угрозы можно настроить контроль доступа на отсечение трафика из внешней сети, использовать фильтр RFC 2827, ввести доп. аутентификацию.

1. Атаки в сетях. Отказ в обслуживании или Denial of Service (DoS)

Атака на вычислительную систему с целью довести её до отказа. Smurf – отсылает пинг запросы по широковещательному каналу. ICMP flood – то же что и Smurf, однако без широковещательного канала. UDP flood - отправка множества UPD пакетов. TCP flood – отправка множества TCP-пакетов. TCP SYN flood – создание множества запросов на инициализация TCP соединений.

1. Атаки на уровне приложений

Использование брешей в серверном программном обеспечении, часто используются порты, которые проходят межсетевой экран (например, порт 80, используемый для отправки данных через web-server).

1. Классификация нарушителей по уровню их знаний
   1. Знает функциональные особенности АС, основные закономерности формирования в ней массивов данных и потоков запросов к ним, умеет пользоваться штатными средствами
   2. Обладает высоким уровнем знаний и опытом работы с техническими средствами системы и их обслуживания
   3. обладает высоким уровнем знаний в области программирования и вычислительной техники, проектирования и эксплуатации автоматизированных информационных систем;
   4. знает структуру, функции и механизм действия средств защиты, их сильные и слабые стороны.
2. Классификация нарушителей по уровню возможностей (используемым методам и средствам).
   1. применяющий только агентурные методы получения сведений;
   2. применяющий пассивные средства
   3. использующий только штатные средства и недостатки систем защиты для её преодоления, компактные магнитные носители информации, которые могут быть скрытно пронесены через посты охраны
   4. применяющий методы и средства активного воздействия
3. Классификация вредоносных программ.
   1. Черви
   2. Троянские кони
   3. Логические бомбы
   4. Вирусы
4. Характеристика основных вредоносных программ
   1. Черви – вредоносные программы, распространяющиеся между компьютерами
   2. Троянские кони – вредоносные программы, притворяющиеся другими программами, которые содержат вредоносный код
   3. Логические бомбы – вредоносные программы, активирующиеся по условию
   4. Вирусы – вредоносные программы, распространяющиеся в пределах информационной системы
5. Межсетевой экран (МЭ, файервол, брандмауэр) - инструмент, который фильтрует входящий и исходящий сетевой трафик. Он анализирует источник трафика, время передачи, IP-адрес, протокол, частоту сообщений и другие параметры, после чего принимает решение: пропустить или заблокировать трафик.
6. МЭ защищает от
   1. Несанкционированный доступ из интернета в защищённую сеть
   2. Неконтролируемых сетевых подключений
   3. Несанкционированной передачи из защищенной сети в интернет.
7. Виды МЭ
   1. Программно-аппаратные комплексы (ПАК), или аппаратные МЭ — специальные устройства или компоненты роутеров, на которых установлено фильтрующее программное обеспечение.
   2. Программные МЭ — программное обеспечение на сервере, которое занимается фильтрацией трафика. По сути, это то же ПО, что установлено в аппаратном МЭ, но оно устанавливается на сам сервер.
8. Типы МЭ
   1. А - аппаратные, установленные на физических границах сети.
   2. Б - программные и аппаратные, установленные на логических границах сети, например встроенные в маршрутизатор.
   3. В — программные, установленные на узлы
   4. Г — аппаратные и программные, работающие с веб-трафиком
   5. Д — аппаратные и программные с промышленными протоколами передачи данных
9. Классы МЭ
   1. 6 класс — самый простой, для работы с персональными даными 3 и 4 уровня защищ.
   2. 5 класс — для данных 2 уровня защищен.
   3. 4 класс — для данных 1 уровня защищен.
   4. 1, 2, 3 — для работы с гостайной
10. Важные положения
    1. МЭ фильтрует трафик, не пропуская трафик внутрь и из сети
    2. МЭ бывают программными и аппаратными
    3. Для работы с перс. данными и гостайной нужен мэ
    4. МЭ может сертифицироваться для гарантии защиты
    5. ФСТЭК делит межсетевые экраны на профили в зависимости от назнач. и уровня защиты
11. Прикладной уровень
12. МЭ с фильтрацией пакетов
    1. IP-адрес источника;
    2. IP-адрес отправителя;
    3. применяемый сетевой протокол (TCP, UDP, ICMP);
    4. порт источника TCP или UDP;
    5. порт назначения TCP или UDP;
    6. тип сообщения ICMP (Internet Control Message Protocol –протокол управляющих сообщений в сети Интернет), если применяется протокол ICMP.
13. Достоинства МЭ с фильтрацией пакетов
    1. Производительность
    2. Хороший способ управления трафиком
    3. Прозрачность
14. Недостатки МЭ с фильтрацией пакетов
    1. низкий уровень масштабируемости
    2. Возможность открытия больших диапазонов портов
    3. Подверженность атаки с подменой данных.