Угрозы
- Незащищенность данных
- Подделка данных
- Отказ от обслуживания
- Переход системы под управление вирусами

С точки зрения безопасности у компьютерных систем есть четыре основные задачи, соответствующие угрозам:
- **конфиденциальность** данных — сохранение секретности соответствующих данных. Система должна гарантировать невозможность допуска к данным лиц, не имеющих на это права. Как минимум, владелец должен иметь возможность определить, кто и что может просматривать, а система должна обеспечить выполнение этих требований, касающихся в идеале отдельных файлов.
- **целостность** данных (data integrity) - пользователи, не обладающие соответствующими правами, не должны иметь возможности изменять какие-либо данные без разрешения их владельцев (внесение в них изменений, удаление или добавление ложных данных). Если система не может гарантировать, что заложенные в нее данные не будут подвергаться изменениям, пока владелец не решит их изменить, то она потеряет свою роль информационной системы.
- **работоспособность** системы (system availability) —никто не может нарушить работу системы и вывести ее из строя. Атаки, вызывающие отказ от обслуживания (denial of service, DOS), приобретают все более распространенный характер. Например, если компьютер работает в роли интернет-сервера, то постоянное забрасывание его запросами может лишить его работоспособности, отвлекая все рабочее время его центрального процессора на изучение и отклонение входящих запросов.
- **исключение постороннего доступа** - посторонние лица могут иногда взять на себя управление чьими-нибудь домашними компьютерами (используя вирусы и другие средства) и превратить их в зомби (zombies), моментально выполняющих приказания посторонних лиц. Часто зомби используются для рассылки спама, поэтому истинный инициатор спам-атаки не может быть отслежен.

Объекты, нуждающиеся в защите: оборудование (например, центральные процессоры, сегменты памяти, дисковые приводы или принтеры) или программное обеспечение (например, процессы, файлы, базы данных или семафоры).

Большинство ОС позволяют отдельным пользователям определять, кто может осуществлять операции чтения и записи в отношении их файлов и других объектов - политика **разграничительного управления доступом** (discretional access controll). Для более жестких мер безопасности (военные организации, корпоративные патентные отделы, лечебные учреждения) – **принудительное управление доступом** (mandatory access control).

Средства защиты: брандмауэры, антивирусы, электронная подпись и др.

Механизм аутентификации

В ОС существуют учетные записи пользователей. Каждой учетной записи можно присвоить пароль. Таким образом идентификацией будет ввод имени учетной записи (логин) и ввод пароля будет аутентификацией (подтверждение того, что это именно вы). Данные процедуры предусматривают простейший вариант НСД, такой как попытка зайти в систему используя Вашу учетную запись. Этот процесс происходит локально (на Вашей рабочей станции).
При взаимодействии в сети, при подключении к какому-либо серверу, Вам может потребоваться ввести Ваши логин и пароль, для того, чтобы получить доступ к ресурсом того сервера, к которому Вы обращаетесь. Данная процедура идентификации и аутентификации происходит при помощи протокола NTLM (NT LAN Manager). Данный протокол является протоколом **сетевой аутентификации** , разработанной фирмой Microsoft для Windows NT.
Так же возможна идентификация и аутентификация в **домене Active Directory**. В сущности процедуры идентичны простой локальной идентификации и аутентификации, но в данном случае, при регистрации в домене, обмен данными между рабочей станцией и сервером

происходит по протоколу Kerberos v5 rev6 (более надежный за счет обоюдной аутентификации, более быстрое соединение и др.)
Процесс регистрации пользователя состоит из таких элементов, как клиент, сервер, центр распределения ключей (KDC) и билеты Kerberos (как “документы” для аутентификации и авторизации). Весь процесс происходит следующим образом:

- Пользователь делает запос регистрационных данных Local Security Authority System (LSASS - часть операционной системы отвечающей за авторизацию локальных пользователей отдельного компьютера)
- LSASS получет билет длял пользователя на контроллере домена
- LSASS посылает запрос на сервер (по протоколу Kerberos v5 rev6), для получения билета для рабочей станции пользователя
- Kerberos Service посылает билет на рабочую станцию
- LSASS формирует ключ доступа для рабочей станции пользователя
- Ключ доступа прикрепляется к пользователю до окончания сеанса работы

IP Security

IPsec (IP Security) - набор протоколов обеспечивающий защиту данных, передаваемых по протоколу IP, что позволяет осуществлять подтверждение подлинности и (или) шифрование IP-пакетов. Так же IPsec включает в себя протоколы для защищённого обмена ключами в сетях общего доступа (Интернет).
Протоколы IPsec работают на 3м - сетевом уровне (модели OSI). Другие протоколы сети, например, SSL и TLS, работают на 4м - транспортном уровне. Протокол IPsec более гибкий, поскольку может использоваться для защиты любых протоколов основаных на TCP и UDP. Также увеличивается его сложность из-за невозможности использовать протокол TCP для надёжной передачи данных.
IPsec можно разделить на два класса: протоколы обеспечивающие **защиту потока передаваемых пакетов** и протоколы **обмена криптографическими ключами**. Протокол обмена криптографическими ключами — IKE (Internet Key Exchange); два протокола, защищающих передаваемый поток: ESP (Encapsulating Security Payload — инкапсуляция зашифрованных данных, а так же обеспечение целостности и конфиденциальности данных) и AH (Authentication Header — аутентифицирующий заголовок, гарантирующий только целостность потока, данные не шифруются).
Протокол IPSec состоит из следующих компонентов:

- AH, отвечающий за подпись неизменяемой части заголовка и данные IP-пакета при помощи алгоритмов уселения криптостойкости HMAC-MD5 и HMAC-SHA, но не производящий шифрования данных
- ESP - протокол шифрования сетевого трафика, отвечающий за шифрацию всего пакета данных, за исключением заголовков IP и ESP, при помощи алгоритмов шифрования DES-CBC и Triple-DES, а так же подписывает зашифрованные данные вместе со своим заголовком

IPSec представлен следующими компанентами:

- IPSec Driver, обеспечивает обрабатку пакетов
- IPSec Filter, указывает, какие пакеты и как нужно обрабатывать
- IPSec Policy, отвечает за определение параметров IP Security для компьютеров

IKE, организующий переговоры между хостами при помощи протокола ISAKMP/Oakley