Программно-аппаратные средства защиты информации

Программно-аппаратные средства защиты информации — это сервисы безопасности, встроенные в сетевые операционные системы.

К сервисам безопасности относятся:

- Идентификация и аутентификация;
  - Управление доступом;
- Протоколирование и аудит;
  - Криптография;
- Экранирование.

ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ

Идентификация предназначена для того, чтобы пользователь или вычислительный процесс, действующий по команде определенного пользователя, могли идентифицировать себя путем сообщения своего имени.

С помощью аутентификации вторая сторона убеждается, что пользователь, пытающийся войти в операционную систему, действительно тот, за кого себя выдает.

УПРАВЛЕНИЕ ДОСТУПОМ

Средства управления доступом позволяют специфицировать и контролировать действия, которые пользователи и вычислительные процессы могут выполнять над информацией и другими компьютерными ресурсами, то есть речь идет о логическом управлении доступом, который реализуется программными средствами.

ЛОГИЧЕСКОЕ УПРАВЛЕНИЕ ДОСТУПОМ

Логическое управление доступом обеспечивает конфиденциальность и целостность объектов путем запрещения обслуживания неавторизированных пользователей.

Контроль прав доступа осуществляется посредством различных компонент программной среды — ядром сетевой операционной системы, дополнительными средствами безопасности, системой управления базами данных, посредническим программным обеспечением.

ПРОТОКОЛИРОВАНИЕ

Протоколированием называется процесс сбора и накопления информации о событиях, происходящих в информационной системе предприятия. Возможные события принято делить на три группы:

- внешние события, вызванные действиями других сервисов;
- внутренние события, вызванные действиями самого сервиса;
- клиентские события, вызванные действиями пользователей и администраторов.

АУДИТ

Аудитом называется процедура анализа накопленной в результате протоколирования информации. Этот анализ может осуществляться оперативно в реальном времени или периодически.

ЭКРАНИРОВАНИЕ

Экран - это средство разграничения доступа клиентов из одного сетевого множества к серверам, принадлежащим другому сетевому множеству. Функция экрана заключается в контроле всех информационных потоков между двумя множествами систем.

Примерами экранов являются межсетевые экраны (бранд- мауары (firewalls)), устанавливаемые для защиты локальной сети организации, имеющей выход в открытую среду.

КРИПТОГРАФИЯ

Метод криптографии — одно из наиболее мощных средств обеспечения конфиденциальности и контроля целостности информации. Основной элемент криптографии – шифрование.

В состав криптографической системы входят: один или нескольких алгоритмов шифрования, ключи, используемые этими алгоритмами шифрования, подсистемы управления ключами, незашифрованный и зашифрованный тексты.