Занятие 16. Лекция

Тема: Принципы защиты информации от несанкционированного доступа

ПРИНЦИП ОБОСНОВАННОСТИ ДОСТУПА. Данный принцип заключается в обязательном выполнении двух основных условий: пользователь должен иметь достаточную «форму допуска» для получения информации требуемого им уровня конфиденциальности, и эта информация необходима ему для выполнения его производственных функций.

ПРИНЦИП ДОСТАТОЧНОЙ ГЛУБИНЫ КОНТРОЛЯ ДОСТУПА. Средства защиты информации должны включать механизмы контроля доступа ко всем видам информационных и программных ресурсов системы, которые с принципом обоснованности доступа следует разделять между пользователями.

ПРИНЦИП РАЗГРАНИЧЕНИЯ ПОТОКОВ ИНФОРМАЦИИ. Для предупреждения нарушения безопасности информации, которое, например, может иметь место при записи секретной информации на несекретные носители и несекретные файлы, ее передаче программам и процессам, не предназначенным для обработки секретной информации, а также при передаче секретной информации по незащищенным каналам и линиям связи, необходимо осуществлять соответствующее разграничение потоков информации.

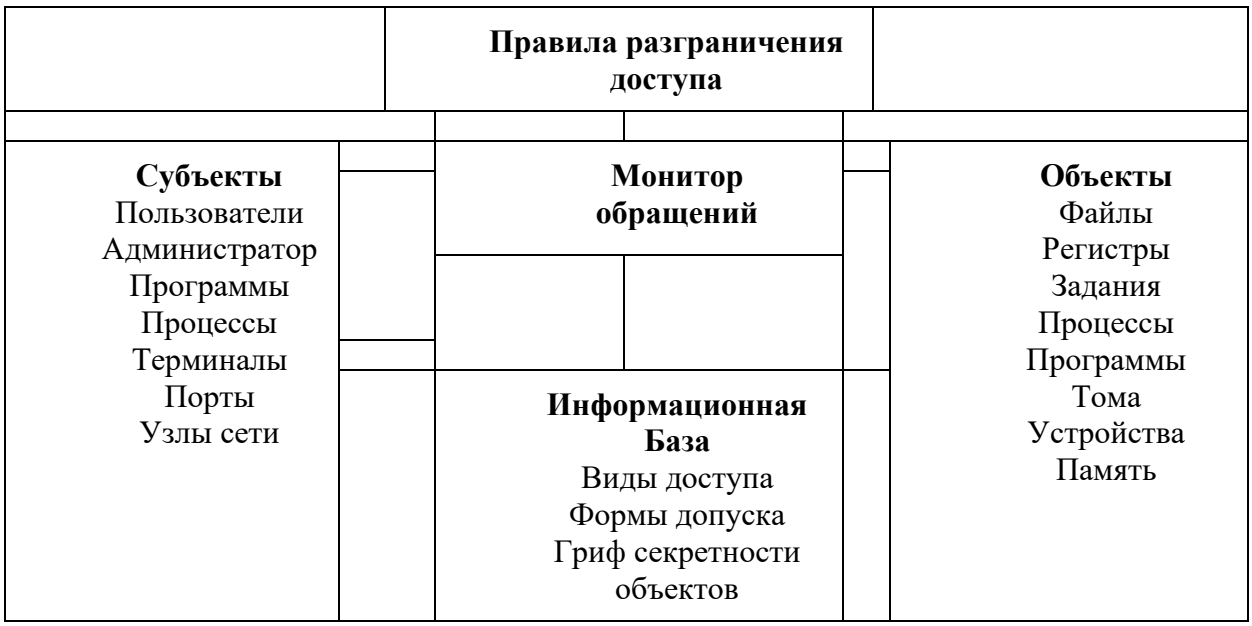
ПРИНЦИП ЧИСТОТЫ ПОВТОРНО ИСПОЛЬЗУЕМЫХ РЕСУРСОВ. Данный принцип заключается в очистке ресурсов, содержащих конфиденциальную информацию, при их удалении или освобождении пользователем до перераспределения этих ресурсов другим пользователям.

ПРИНЦИП ПЕРСОНАЛЬНОЙ ОТВЕТСТВЕННОСТИ. Каждый пользователь должен нести персональную ответственность за свою деятельность в системе, включая любые операции с конфиденциальной информацией в системе и возможные нарушения ее защиты, т.е. какие-либо случайные или умышленные действия, которые приводят или могут привести к несанкционированному ознакомлению с конфиденциальной информацией, ее искажению или уничтожению, или делают такую информацию недоступной для ее законных пользователей.

ПРИНЦИП ЦЕЛОСТНОСТИ СРЕДСТВ ЗАЩИТЫ. Данный принцип подразумевает, что средства защиты информации в системе должны точно выполнять свои функции в соответствии с перечисленными принципами и быть изолированными от пользователей, а для своего сопровождения должны включать специальный защищенный интерфейс для средств контроля, сигнализации о попытках нарушения защиты информации и воздействия на процессы в системе.

Реализация перечисленных принципов осуществляется с помощью так называемого «монитора обращений», контролирующего любые запросы к данным или программам со стороны пользователей по установленным для них видам доступа к этим данным или программам (рисунок).

Практическое создание монитора обращений предполагает разработку конкретных правил разграничения доступа в виде так называемой модели защиты информации.


Правила разграничения доступа
Субъекты
Пользователи
Администратор
Программы
Процессы
Терминалы
Порты
Узлы сети
Монитор обращений
Информационная База
Виды доступа
Формы допуска
Гриф секретности объектов
Объекты
Файлы
Регистры
Задания
Процессы
Программы
Тома
Устройства
Память