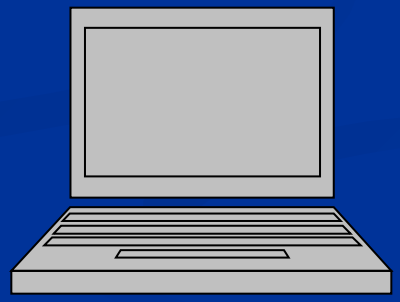
Понятие о необходимости встроенных средств защиты на уровне ОС

Подготовила:
Студентка гр.И-411
Сартакова Е.Л.

Всеобщая осведомленность в необходимости обеспечения безопасности компьютерных систем растет по мере того, как очень важные сервисы все больше и больше становятся зависимыми от взаимодействия компьютерных систем.

Операционная система обеспечивает защиту механизмов прикладного уровня от неправильного использования, обхода или навязывания ложной информации .

Потребность в защищенных операционных системах особенно важна в современных компьютерных средах.

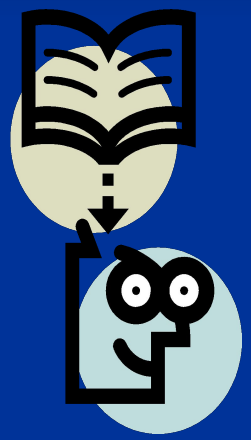


Мандатная безопасность

Мандатная политика безопасности *- любая политика, логика и присвоение атрибутов безопасности которой строго контролируются системным администратором политики безопасности.*

С помощью мандатной безопасности можно реализовать политики безопасности на уровне предприятия.

Дискреционная политика безопасности



Дискреционная политика безопасности *- любая политика, в которой обычные пользователи могут принимать участие в определении функций политики и/или присвоении атрибутов безопасности.*


Мандатная политика
политика контроля доступа
политика использования подсистемы идентификации
политика использования криптографической подсистемы

Надежный путь доступа

Надежный путь доступа *- механизм, посредством которого пользователь может взаимодействовать с доверенным ПО напрямую, и который может быть активирован либо пользователем либо доверенным ПО, но не может быть воспроизведен каким либо другим ПО.*

Надежный сетевой канал

Надежный сетевой канал *(Trusted Network Interface - TNI) представляет концепцию надежного(безопасного) канала связи между доверенным ПО на различных узлах сети.*

Контроль доступа

Механизмы контроля доступа прикладного уровня могут быть разбиты на две компоненты:

- перехватывающую и

- решающую

Когда субъект пытается осуществить доступ к объекту, защищенному этим механизмом, перехватывающая компонента должна вызвать решающую компоненту, передав ей соответствующие входные параметры для принятия решения в соответствии с политикой безопасности, и должна претворить в жизнь принятое решение.

Криптография

Анализ криптографической защиты на прикладном уровне может быть разбит на:

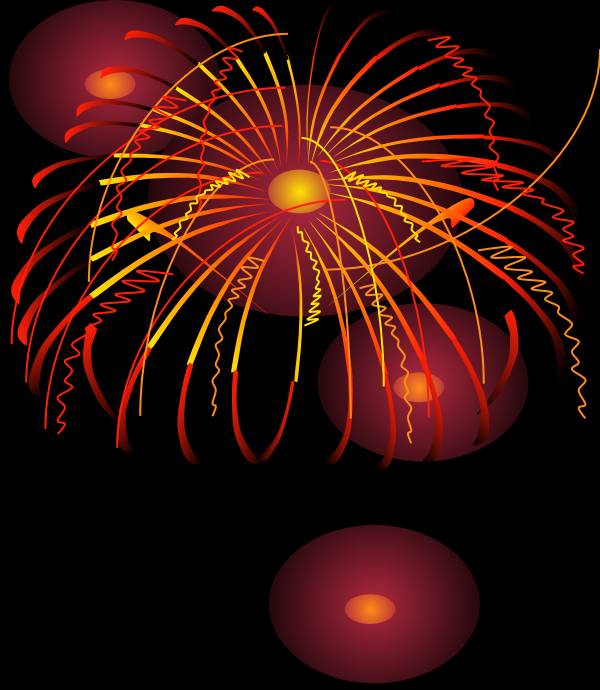
- *анализ вызова механизма криптографической защиты и*
- *анализ самого механизма*

Сетевые протоколы обеспечения безопасности

Сетевые протоколы обеспечения безопасности IPSEC используются для предоставления сервисов аутентификации, конфиденциальности и целостности на уровне протокола IP.

Средства защиты, встроенные в ОС, занимают особое место. Их основной задачей является защита информации, определяющей конфигурацию системы, и уже затем — пользовательских данных.

Угрозы, создаваемые современными компьютерными средами, не могут быть нейтрализованы без использования защищенных операционных систем.



Всем

спасибо

за внимание!