Безопасность операционных систем

БОБКОВА ЕКАТЕРИНА, П17.1

Классификация угроз безопасности операционной системы

Единой и общепринятой классификации угроз безопасности операционной системы не существует. Однако классифицировать эти угрозы можно по способу их реализации.

Классификация угроз по цели:

- Несанкционированное чтение информации
- Несанкционированное изменение информации
- Несанкционированное уничтожение информации
- Полное или частичное уничтожение ОС (от кратковременного вывода из строя программных модулей до физического стирания их с диска системных файлов)

Классификация угроз по принципу воздействия на ОС:

- Использование известных (легальных) каналов получения информации, например, несанкционированного чтения пользователя которому доступ ограничен
- Использование скрытых каналов получения информации, например, угроза использования злоумышленником недокументированных возможностей ОС
- Создание новых каналов получения информации с помощью программных закладок

Классификация угроз по принципу воздействия на ОС

Активное воздействие несанкционированные действия злоумышленника в системе

Пассивное воздействие несанкционированные наблюдения злоумышленника за процессами происходящими в системе

Классификация угроз по типу используемой злоумышленником слабости защиты:

Неадекватная политика безопасности, в том числе ошибки администратора системы

Ошибки и недокументированные возможности программного обеспечения ОС, в том числе и так называемые люки – случайно или преднамеренно встроенные в систему «служебные входы» , позволяющие обходить систему

Классификация угроз по способу воздействия на объект атаки:

- непосредственное воздействие
- превышение пользователем своих полномочий
- работа от имени другого пользователя
- использование результатов работы другого пользователя (например, несанкционированный перехват информационных потоков, инициированных другим пользователем)

Классификация угроз по способу действия злоумышленника:

- В интерактивном режиме (вручную)
- В пакетном режиме (с помощью специально написанной программы)

Классификация угроз по объекту атаки:

- Операционная система в целом
- Объекты ОС
- Каналы передачи данных

Классификация угроз по используемым средствам атаки:

- Штатные средства ОС без использования дополнительного программного обеспечения
- ПО третьих фирм (к этому классу ПО относятся как компьютерные вирусы так и другие вредоносные программы.)
- Специально разработанное ПО

Классификация угроз по состоянию атакуемого объекта ОС на момент атаки:

Хранение

Передача

Обработка

Типичные атаки на ОС

- СКАНИРОВАНИЕ ФАЙЛОВОЙ СИСТЕМЫ
- КРАЖА КЛЮЧЕВОЙ ИНФОРМАЦИИ
- ПОДБОР ПАРОЛЯ
- СБОРКА МУСОРА
- ПРОГРАММНЫЕ ЗАКЛАДКИ
- ЖАДНЫЕ ПРОГРАММЫ
  - Жадными называются программы, преднамеренно захватывающие значительную часть ресурсов компьютера

Понятие защищенной ОС

- Защищенной называется ОС, если она предусматривает средства защиты от основных классов угроз
- Частично защищенной называется ОС которая предусматривает защиту не от всех классов угроз , а только от некоторых
- Политикой безопасности называется набор норм, правил и практических приемов, регулирующих порядок хранения и обработки ценной информации
- Адекватной политикой безопасности называется такая политика безопасности, которая обеспечивает достаточный уровень защищенности ОС.

Основные функции подсистемы защиты ОС

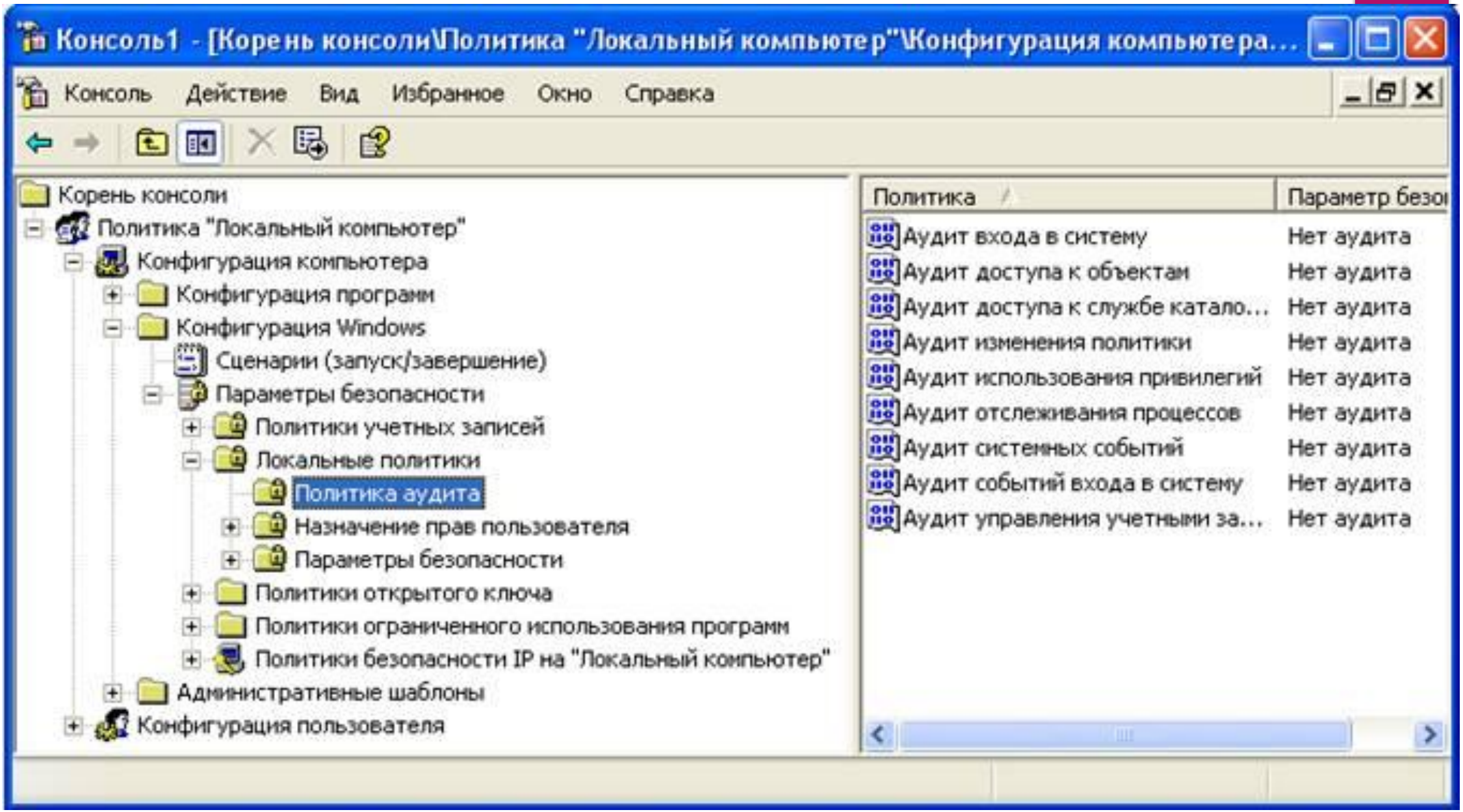
- Разграничение доступа
- Идентификация и аутентификация
- Аудит
- Управление политикой безопасности
- Криптографические функции
- Сетевые функции

Идентификация, аутентификация, аудит и авторизация субъектов доступа

- Идентификация субъекта доступа заключается в том, что субъект сообщает ОС идентифицирующую информацию о себе и таким образом идентифицирует себя
- Аутентификация субъекта доступа заключается в том, что субъект предоставляет ОС помимо идентифицирующей информации подтверждающая, что он действительно является тем субъектом доступа, к которому относится идентифицирующую информация
- Авторизация субъекта доступа происходит после успешной идентификации и аутентификации

Идентификация, аутентификация, аудит и авторизация субъектов доступа

Процедура аудита применительно к ОС заключается в регистрации в специальном журнале, называемом журналом аудита или журналом безопасности , событий, которые могут представлять опасность для ОС. Пользователи системы, обладающие правом чтения этого журнала, называются аудиторами


Консоль1 - [Корень консоли\Политика "Локальный компьютер"\Конфигурация компьютера...
Консоль
Действие
Вид
Избранное
Окно
Справка
Корень консоли
Политика "Локальный компьютер"
Конфигурация компьютера
Конфигурация программ
Конфигурация Windows
Сценарии (запуск/завершение)
Параметры безопасности
Политики учетных записей
Локальные политики
Политика аудита
Назначение прав пользователя
Параметры безопасности
Политики открытого ключа
Политики ограниченного использования программ
Политики безопасности IP на "Локальный компьютер"
Административные шаблоны
Конфигурация пользователя
Политика
Параметр безо
Аудит входа в систему
Нет аудита
Аудит доступа к объектам
Нет аудита
Аудит доступа к службе катало...
Нет аудита
Аудит изменения политики
Нет аудита
Аудит использования привилегий
Нет аудита
Аудит отслеживания процессов
Нет аудита
Аудит системных событий
Нет аудита
Аудит событий входа в систему
Нет аудита
Аудит управления учетными за...
Нет аудита

Требования к аудиту

Подсистема аудита ОС должна удовлетворять следующим требованиям:

- Только сама ОС может добавлять записи в журнал аудита
- Ни один субъект доступа, в том числе и сама ОС, не имеет возможности редактировать или удалять отдельные записи в журнал аудита
- Только пользователи-аудиторы, обладающие соответствующей привилегией, могут просматривать журнал аудита
- Только пользователи-аудиторы могут очищать журнал аудита
- При переполнении журнала аудита ОС аварийно завершает работу («зависает»)

Требования к аудиту

Политика аудита - это совокупность правил, определяющих то, какие события должны регистрироваться в журнале аудита

Для обеспечения надежной защиты ОС в журнале должны обязательно регистрироваться следующие события

- Политика входа/выхода пользователей из системы
- Попытки изменения списка пользователей
- Попытки изменения политики безопасности, в том числе и политике аудита

СПАСИБО ЗА ВНИМАНИЕ!