ЛЕКЦИЯ №5

«Протоколирование и аудит»

по дисциплине

«Безопасность операционных систем»

Текст лекции рассмотрен и одобрен на заседании кафедры протокол № _____ от " " 201__ г.

**(Слайд 1. Титульный слайд)**

Уважаемые студенты! Сегодня вы продолжаете изучение дисциплины «Безопасность операционных систем». Лекция №6 «Протоколирование и аудит», за ней одноименное практическое занятие. Продолжительность лекции - два академических часа, практического занятия - 2 академических часа.

**Слайд 2 (вопросы занятия)**

- Протоколирование событий в современных ОС.
- Журналы событий.
- Аудит событий в современных ОС.

**Основные понятия**

**Регистрация** - механизм подотчетности системы ОБИ, фиксирующий все события, касающиеся безопасности, такие как:

- вход и выход субъектов доступа;
- запуск и завершение программ;

- выдача печатных документов;
- попытки доступа к защищаемым ресурсам;
- изменение полномочий субъектов доступа и статуса объектов доступа
- и т. д.

**Протоколирование** - сбор и накопление информации о событиях, происходящих в информационной системе.

**События**: внешние (вызванные действиями других сервисов), внутренние (вызванные действиями самого сервиса) и клиентские (вызванные действиями пользователей и администраторов).

**Аудит** – это анализ накопленной информации, проводимый оперативно, в реальном времени или периодически.

Реализация механизма регистрации и аудита преследует следующие цели:
- обеспечение подотчетности пользователей и администраторов;
- обеспечение возможности реконструкции последовательности событий;
- обнаружение попыток нарушений информационной безопасности;
- предоставление информации для выявления и анализа проблем.

## Подсистема аудита в Windows

Важный элемент политики безопасности – аудит событий в системе. ОС Windows ведет аудит событий по 9 категориям:

- Аудит событий входа в систему.
- Аудит управления учетными записями.
- Аудит доступа к службе каталогов.
- Аудит входа в систему.
- Аудит доступа к объектам.
- Аудит изменения политики.
- Аудит использования привилегий.
- Аудит отслеживания процессов.
- Аудит системных событий.

Рассмотрим более подробно, какие события отслеживает каждая из категорий.

### Аудит событий входа в систему

Аудит попыток пользователя войти в систему с другого компьютера или выйти из нее, при условии, что этот компьютер используется для проверки подлинности учетной записи.

**Аудит управления учетными записями**

Аудит событий, связанных с управлением учетными записями на компьютере: создание, изменение или удаление учетной записи пользователя или группы; переименование, отключение или включение учетной записи пользователя; задание или изменение пароля.

**Аудит доступа к службе каталогов**

Аудит событий доступа пользователя к объекту каталога Active Directory, для которого задана собственная системная таблица управления доступом (SACL).

**Аудит входа в систему**

Аудит попыток пользователя войти в систему с компьютера или выйти из нее.

**Аудит доступа к объектам**

Аудит событий доступа пользователя к объекту – например, к файлу, папке, разделу реестра, принтеру и т. п., - для которого задана собственная системная таблица управления доступом (SACL).

**Аудит изменения политики**

Аудит фактов изменения политик назначения прав пользователей, политик аудита или политик доверительных отношений.

**Аудит использования привилегий**

Аудит попыток пользователя воспользоваться предоставленным ему правом.

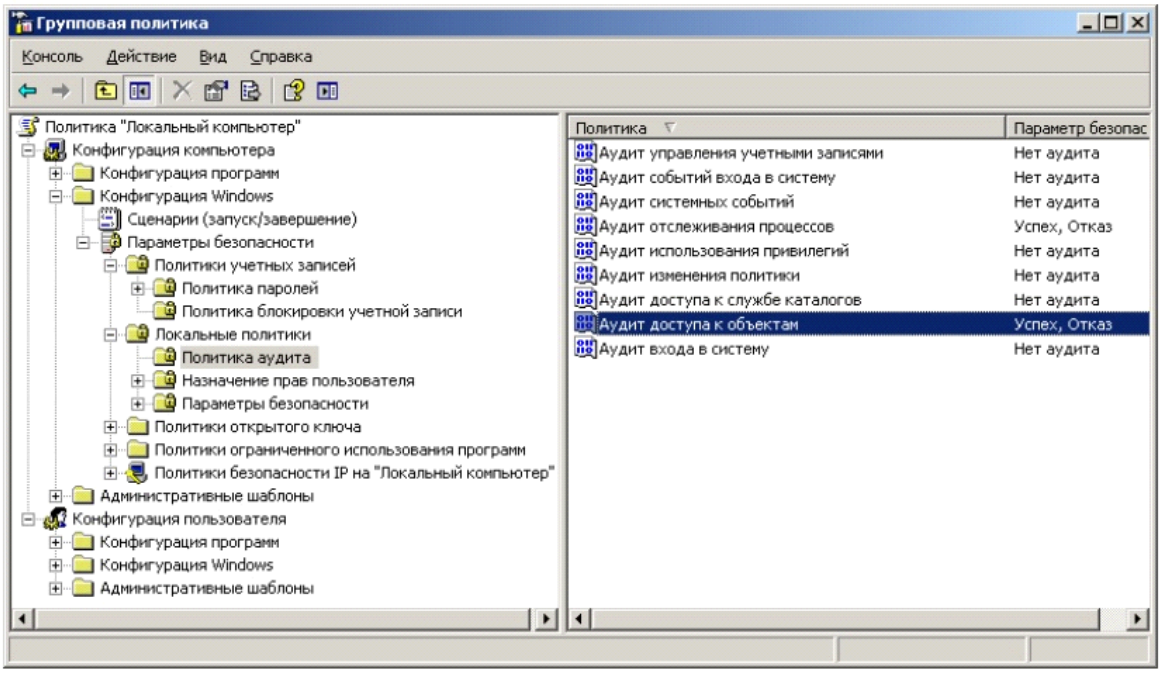
**Аудит отслеживания процессов**

Аудиту таких событий, как активизация программы, завершение процесса, повторение дескрипторов и косвенный доступ к объекту.

**Аудит системных событий**

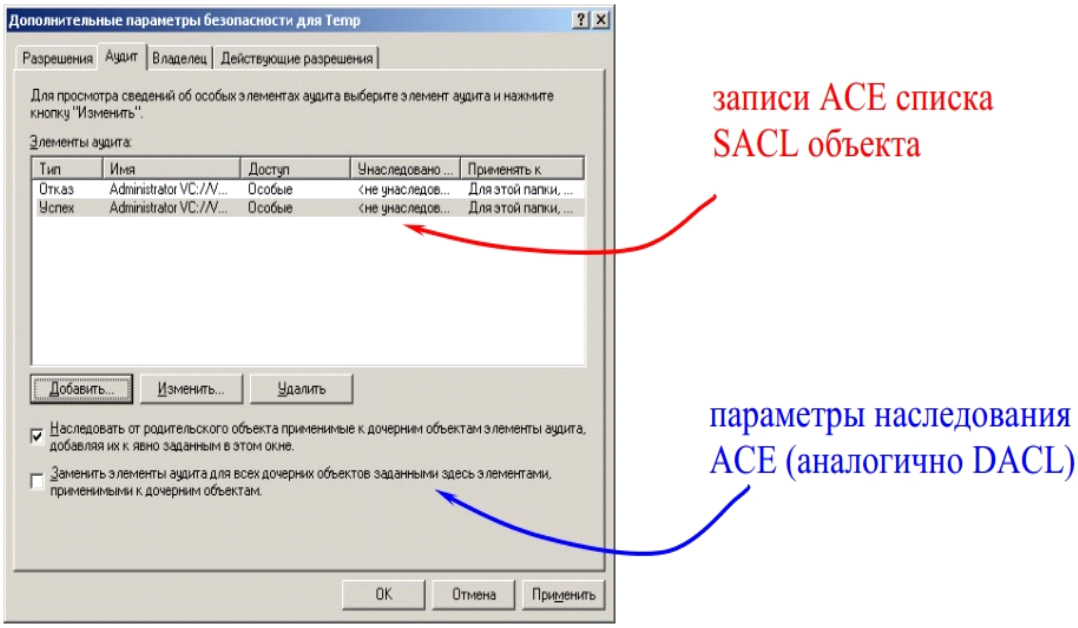
Аудит событий перезагрузки или отключения компьютера, а также событий, влияющих на системную безопасность или на журнал безопасности.

Решения об аудите конкретного типа событий безопасности принимаются в соответствии с политикой аудита локальной системы. Политика аудита, также называемая локальной политикой безопасности (local security policy), является частью политики безопасности, поддерживаемой LSASS в локальной системе, и настраивается с помощью редактора локальной политики безопасности (Оснастка gpedit.msc, Конфигурация компьютера - Конфигурация Windows – Параметры безопасности – Локальные политики – Политика аудита).




Для каждого объекта в SD содержится список SACL, состоящий из записей ACE, регламентирующих запись в журнал аудита удачных или неудачных попыток доступа к объекту. Эти ACE определяют, какие операции, выполняемые над объектами конкретными пользователями или группами, подлежат аудиту. Информация аудита хранится в системном журнале аудита. Аудиту могут подлежать как успешные, так и неудачные операции. Подобно записям ACE DACL, правила аудита объектов могут наследоваться дочерними объектами. Процедура наследования определяются набором флагов, являющихся частью структуры ACE.

Настройка списка SACL может быть осуществлена в окне дополнительных свойств объекта (пункт “Дополнительно”, закладка “Аудит”)




Для программного просмотра и изменения списков SACL можно использовать API-функции GetSecutityInfo и SetSecutityInfo.

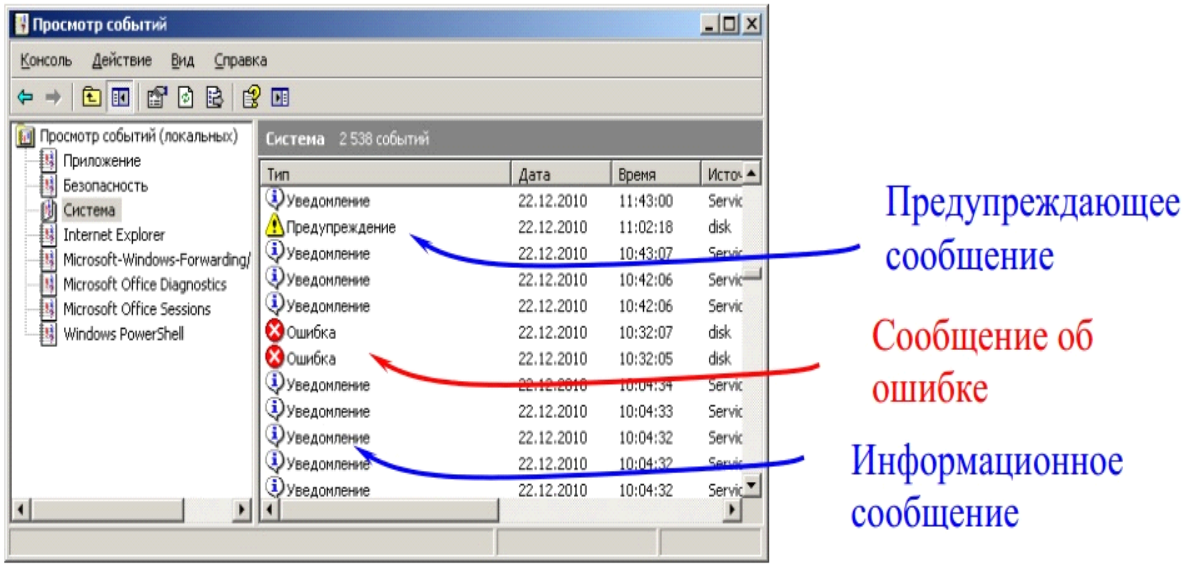
При инициализации системы и изменении политики LSASS посылает SRM сообщения, информирующие его о текущей политике аудита. LSASS отвечает за прием записей аудита, генерируемых на основе событий аудита от SRM, их редактирование и передачу Event Logger (регистратору событий). SRM посылает записи аудита LSASS через свое LPC-соединение. После этого Event Logger заносит записи в журнал безопасности.

События аудита записываются в журналы следующих типов:

- Журнал приложений. В журнале приложений содержатся данные, относящиеся к работе приложений и программ.
- Журнал безопасности. Журнал безопасности содержит записи о таких событиях, как успешные и безуспешные попытки доступа в систему, а также о событиях, относящихся к использованию ресурсов.
- Журнал системы. В журнале системы содержатся события системных компонентов Windows. Например, в журнале системы регистрируются сбои при загрузке драйвера или других системных компонентов при запуске системы.
- Журнал службы каталогов. В журнале службы каталогов содержатся события, заносимые службой каталогов Windows (на контроллере домена AD).

- Журнал службы репликации. В журнале службы репликации файлов содержатся события, заносимые службой репликации файлов Windows (на контроллере домена AD).

Просмотр журнала безопасности осуществляется в оснастке «Просмотр событий» (eventvwr.msc). Сами журналы хранятся в файлах SysEvent.evt, SecEvent.evt, AppEvent.evt в папке %WinDir%\system32\config.




В журнал записываются события 3 основных видов:

- **Информационные сообщения о событиях**.

Описывают успешное выполнение операций, таких как запуск или некоторое действие системной службы.

- **Предупреждающие сообщения о событиях**.

Описывают неожиданные действия, означающие проблему, или указывают на проблему, которая возникнет в будущем, если не будет устранена сейчас.

- **Сообщения о событиях ошибок**.

Описывают ошибки, возникшие из-за неудачного выполнения задач.

**Журнал событий (Event Log)**— в Microsoft Windows стандартный способ для приложений и операционной системы записи и централизованного хранения информации о важных программных и аппаратных событиях. Служба журналов событий сохраняет события от различных источников в едином журнале событий, программа просмотра событий позволяет пользователю наблюдать за журналом событий, программный интерфейс (API) позволяет приложениям записывать в журнал информацию и просматривать существующие записи.

Записи журнала событий хранятся в ключе реестра HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog

Данный ключ содержит подключи, называемые файлами журнала. По умолчанию имеются:

- файл журнала приложений — для событий приложений и служб;
- файл журнала безопасности — для событий системы аудита;
- файл системного журнала — для событий драйверов устройств.

## Журналирование в Linux

- Журналы хранятся в каталоге /var/log.
- Основным системным демоном логирования является syslog/rsyslog
- Другие сервисы и программы также могут размещать свои log-файлы в каталоге /var/log.
- Большинство журналов доступны для чтения только суперпользователю root, но это можно легко изменить, скорректировав права доступа к файлам.
- Журнал сообщений /var/log/messages - основной системный log-файл. Он содержит сообщения о ходе загрузки системы, а также другие сообщения о статусе работающей системы. В этом файле накапливаются сообщения об ошибках ввода/вывода (IO), проблемах с сетью и другие сообщения о системных ошибках и др. С изучения файла /var/log/messages обычно начинают выявление и устранение неполадок.
- /var/log/boot.log
- /var/log/lastlog
- /var/log/kern.log
- /var/log/mail.log
- /var/log/btmp
- /var/log/dmesg

## Аудит в Linux

Системный аудит (или аудит системных событий) - это постоянное и подробное протоколирование любых событий, происходящих в операционной системе. Аудиту могут быть подвержены такие события, как чтение/запись файлов, выполнение входа в ОС, запуск и остановка приложений, инициация сетевого соединения и многое, многое другое. Кроме самого факта возникновения события, система аудита представляет такую информацию, как дата и время возникновения события, ответственность пользователя за событие, тип события и его успешность. Сама по себе она способна лишь сообщать о произошедшем событии, тогда как процесс журналирования возлагается на плечи демона auditd.

## Подсистема аудита

Ядро Linux >= 2.6 включает в себя подсистему для проведения аудита. Она позволяет вести слежение за такими системными событиями, как:

- Запуск и завершение работы системы (перезагрузка, остановка);
- Чтение/запись или изменение прав доступа к файлам;
- Инициация сетевого соединения или изменение сетевых настроек;
- Изменение информации о пользователе или группе;
- Изменение даты и времени;
- Запуск и остановка приложений;
- Выполнение системных вызовов.

Демон auditd доступен в любом современном Linux-дистрибутиве и может быть установлен с помощью стандартного менеджера пакетов.

Подсистема аудита состоит из модуля ядра, демона auditd, демона audispd и вспомогательных утилит (auditctl, aureport, ausearch, autrace).

Используемые конфигурационные файлы:

- /etc/sysconfig/auditd — содержит настройки используемые при старте демона auditd;
- /etc/audit/auditd.conf — настройки поведения демона auditd;
- /etc/audit/audit.rules — файл содержащий правил аудита.

## Архитектура подсистемы аудита в Linux

Ни одно событие в любой операционной системе не может произойти без использования системных вызовов ядра. Запуск нового процесса, открытие файлов и работа с ними, запрос времени или типа ОС, обращение к оборудованию, создание сетевого соединения, вывод информации на экран – все эти операции производятся с помощью обращения к функциям ядра операционной системы, для краткости называемых системными вызовами. Чтобы отследить любое системное событие, достаточно просто перехватывать все обращения к системным вызовам. Именно это делает подсистема аудита. Она устанавливает триггеры до и после всех функций, ответственных за обработку системных вызовов, и ждет. Когда происходит системный вызов, триггер срабатывает, подсистема аудита получает всю информацию о вызове и его контексте, передает ее демону auditd и отдает дальнейшее управление функции, обрабатывающей системный вызов. После ее завершения срабатывает «выходной» триггер, и вся информация о системном вызове вновь поступает к подсистеме аудита и демону auditd.

## Правила аудита

Для создания, удаления и модификации правил аудита предназначена утилита auditctl. Есть три основных опции, которые принимает эта команда:

-a – добавить правило в список;

-d – удалить правило из списка;

-D – удалить все правила;

-l – вывести список заданных правил.

Если ты сейчас выполнишь команду «auditctl -l» от имени администратора, то, скорее всего, увидишь «No rules», а это значит, что они одного правила аудита еще не существует. Для добавления правил используется следующая форма записи команды auditctl:

**# auditctl -a список,действие -S имя_системного_вызова -F фильтры**

Здесь список – это список событий, в который следует добавить правило. Всего существует пять списков:

- task – события, связанные с созданием процессов;
- entry – события, происходящие при входе в системный вызов;
- exit – события, происходящие во время выхода из системного вызова;
- user – события, использующие параметры пользовательского пространства, такие как uid, pid и gid;
- exclude – используется для исключения событий.

Второй параметр опции – '-a' – это действие, которое должно произойти в ответ на возникшее событие. Их всего два: never и always. В первом случае события не записываются в журнал событий, во втором – записываются.

Далее указывается опция '-S', которая задает имя системного вызова, при обращении к которому должен срабатывать триггер (например, open, close, exit, и т.д.). Вместо имени может быть использовано числовое значение.

Необязательная опция '-F' используется для указания дополнительных параметров фильтрации события. Например, если мы хотим вести журнал событий, связанных с использованием системного вызова open(), но при этом желаем регистрировать только обращения к файлам каталога /etc, то должны использовать следующее правило:

**# auditctl -a exit,always -S open -F path=/etc/**

Чтобы еще более сузить круг поисков, сделаем так, чтобы регистрировались только те события, при которых файл открывается только на запись и изменение атрибутов:

**# auditctl -a exit,always -S open -F path=/etc/ -F perm=aw**

Здесь 'a' – изменение атрибута (то есть attribute change), а 'w' – запись (то есть write).

Также можно использовать ‘r’ – чтение (read) и ‘x’ – исполнение (execute). Другие полезные фильтры включают в себя: **pid** – события, порождаемые указанным процессом, **apid** – события, порождаемые указанным пользователем, **success** – проверка на то, был ли системный вызов успешным, **a1, a2, a3, a4** – первые четыре аргумента системного вызова. Фильтр **key** используется для указания ключа поиска, который может быть использован для поиска всех событий, связанных с этим ключом.

Для слежения за файлами в auditctl предусмотрен специальный синтаксис, при котором опцию ‘-S’ можно опустить.

Например, описанное выше правило может быть задано следующим образом (здесь опция ‘-p’ – это эквивалент фильтра perm):

**# auditctl -a exit,always -F dir=/etc/ -F perm=wa**

или

**# auditctl -w /etc/ -p wa**

## Анализ журнальных файлов

Журнальные файлы, создаваемые демоном auditd в каталоге /var/log/audit, не предназначены для чтения человеком, но хорошо подходят для анализа с помощью специальных утилит, устанавливаемых вместе с самим демоном. Самая важная из них – утилита aureport, генерирующая отчеты из лог-файлов. Вызвав ее без аргументов, мы узнаем общую статистику использования системы, включая такие параметры, как количество входов и выходов из системы, открытых терминалов, системных вызовов и т.д. Эта информация малоинтересна, поэтому лучше запросить более детальный отчет. Например, запустив команду с флагом ‘-f’, мы получим список файлов, к которым происходил доступ:

**$ sudo aureport -f**

Получив список всех попыток доступа и номера событий, каждое из них можно проанализировать индивидуально с помощью утилиты ausearch:

**$ sudo auserch -a номер_события**

Также ausearch можно использовать для поиска событий по именам системных вызовов:

**$ sudo ausearch -sc ptrace -i**

Идентификаторам пользователей:

**$ sudo ausearch -ui 2010**

Именам исполняемых файлов:

**$ sudo ausearch -x /usr/bin/nmap**

## Вывод

В данной лекции мы рассмотрели такой важный механизм безопасности как протоколирование и аудит. Изучили конкретные реализации механизмов протоколирования и аудита в ОС Linux, Windows.