**Практическая работа № 9.**

**Тема:** «Настройка аудита безопасности в Windows Server 2003».

**Цель работы:** научиться проводить настройку аудита событий безопасности и использовать журналы безопасности для повышения защищенности системы.

**Теоретическое введение.**

Аудит - это процесс, позволяющий фиксировать события, происходящие в системе и имеющие отношения к безопасности. Аудит сопровождается записью информации о контролируемых событиях в специальные журналы безопасности, контролируемые администратором. Журналы позволяют контролировать поведение и использование тех ресурсов, для которых администратор назначил проведение аудита.

Аудит по умолчанию отключен, и для его настройки и введения в действие необходимо сначала активизировать аудит через настройки, управляющие политикой безопасности домена (Групповая политика) или компьютера (Локальная политика безопасности).

Затем можно выполнить настройку выбранного типа аудита применительно к объектам системы и ее пользователям.

**Указания к проведению лабораторной работы.**

Чтобы активизировать аудит на локальном компьютере или в масштабах домена, необходимо выполнить следующие действия.

Для локального компьютера на Панели управления в разделе Администрирование выберите Локальные параметры безопасности или в качестве альтернативы запустите в строке Выполнить программу secpol.msc.

В открывшейся оснастке (рисунок 1) выберите пункт Локальные политики и раскройте пункт Политика аудита. В правой части окна появится список типов действий аудита. Поначалу ни один из видов аудита не проводится и необходимо активизировать аудит.

Дважды щелкните на каждой политике, для которой необходимо активизировать аудит и затем установите флажки Успех и (или) Отказ.

Аналогичные действия при управлении доменом выполняются с помощью оснастки Групповая политика безопасности в разделе Администрирование контроллера домена.

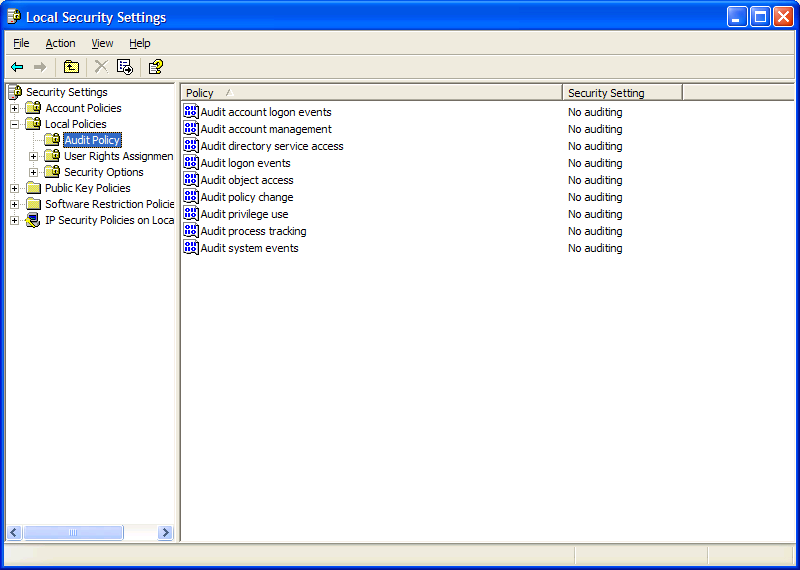


Рисунок 1 - Выбор оснастки Локальная политика безопасности

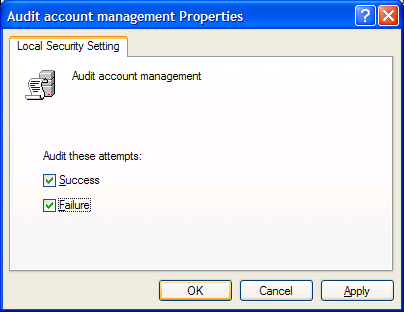


Рисунок 2 - Установка событий для аудита

Основные события, которые могут быть подвергнуты аудиту, описываются в таблице.

|  |  |
| --- | --- |
| Политика аудита | Описание политики |
| Аудит событий входа по учетной записи | Эти события возникают в контроллере домена, когда пользователь выполняет вход или выход на другом компьютере, входящем в домен |
| Аудит управления учетными записями | Эти события возникают при создании, изменении или удалении учетной записи или группы, переименовании, активизации или отключении учетной записи, когда задается или изменяется пароль |
| Аудит доступа к службе каталогов | Эти события возникают, когда выполняется доступ к объекту Active Directory |
| Аудит событий входа | Эти события возникают, когда пользователь выполняет вход или выход на рабочей станции или подсоединяется через сеть. |
| Аудит доступа к объектам | Эти события возникают, когда пользователь выполняет доступ к файлу, папке, принтеру, ключу реестра или другому объекту, для которого задан аудит |
| Аудит изменения политики | Эти события возникают, когда вносятся изменения в политики назначения прав пользователей, политики аудита |
| Аудит системных событий | Эти события возникают, когда пользователь перезагружает компьютер или завершает его работу либо при возникновении события, которое влияет на безопасность компьютера |

В практической работе выполняется настройка аудита для папок и файлов, т.е. выбирается тип аудита - Аудит доступа к объектам.

Для настройки аудита в качестве объекта аудита выберите папку или файл, в диалоговом окне Свойства используйте вкладку Безопасность и по кнопке Дополнительно перейдите в диалоговое окно Параметры управления доступом. Откройте вкладку Аудит (рисунок 3). Добавьте пользователей или группы (кнопка Добавить).

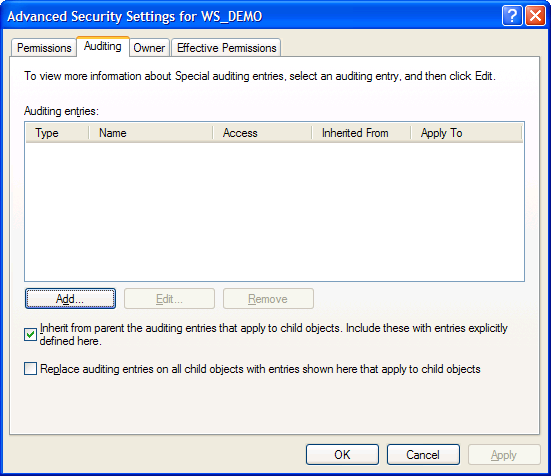


Рисунок 3 - Выбор объектов аудита

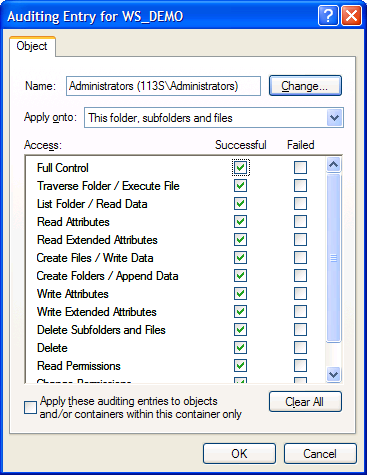


Рисунок 4 - Установка действий, контролируемых при аудите

Измените настройки существующих пользователей (кнопка Просмотр/Правка) в окне Параметры Аудита (рисунок 4).

Если устанавливаются флажки события Успех, то Windows запишет в журнал Безопасность (Security) события, их время и дату для каждой успешной попытки данного пользователя или члена группы для указанного файла или папки. Аналогичным образом, если вы устанавливаете флажок события Отказ, Windows запишет в журнал Безопасность (Security) события, их время и дату для каждой неуспешной попытки данного пользователя или члена группы для указанного файла или папки. Для просмотра зафиксированных системой событий аудита служит оснастка Просмотр Событий, доступная на локальном компьютере в разделе Администрирование Панели управления или в разделе Администрирование домена. Можно запустить оснастку командой eventvwr.msc (рисунок 5). Данная оснастка открывает доступ к трем журналам, заполняемым системой: System, Securitty, Application. При выполнении аудита заполняется журнал Security. В нем для каждого события для объектов аудита создается соответствующая запись, которую можно просмотреть, дважды щелкнув по ней, как это показано на рисунках 5 и 6.

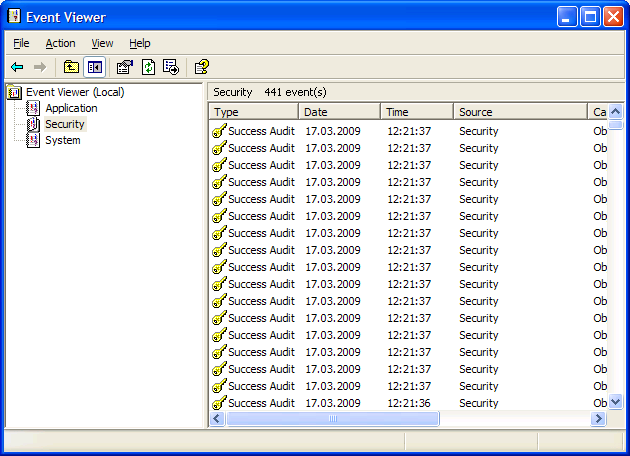


Рисунок 5 - Просмотр содержимого журнала безопасности

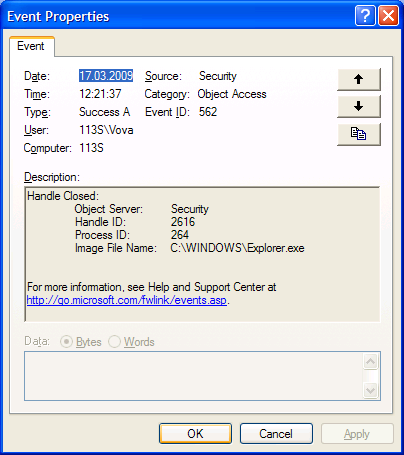


Рисунок 6 - Просмотр информации о событии безопасности

**Задание к лабораторной работе**

С целью освоения настройки аудита и его использования для повышения безопасности системы выполните следующие действия:

1. Войдите на виртуальную машину с учетной записью администратора
2. Активизируйте средствами политики безопасности аудит доступа к объекту (Успех и Отказ).
3. Создайте временную папку и текстовый файл внутри ее.
4. Выберите эту папку как объект аудита
5. Настройте аудит доступа к папке для администратора и пользователя компьютера, ограничив пользователя в возможных действиях с папкой и файлом, чтобы в ряде случаев происходило событие Отказ.
6. Выполните ряд типовых действий с папкой и файлом от имени администратора и затем от имени пользователя.
7. Прочитайте журнал событий Безопасности и найдите в нем записи, в которых отражены ваши действия с объектами как о имени администратора, так и от имени пользователя. Сделайте соответствующие выводы.
8. Результаты в виде экранов и текстов должны быть сохранены в файле отчета по лабораторной работе и представлены к защите.
9. Самостоятельно освойте настройку аудита для принтеров.

**Контрольные вопросы:**

1. Какова роль аудита в обеспечении безопасности компьютерной системы?
2. Где и каким образом формируется информация о событиях аудита?
3. Какая информация может быть получена в результате аудита?
4. Какие типы аудита вы знаете и для чего предназначен каждый из них?
5. Каким образом активизируется политика аудита?
6. Каким образом политика аудита применяется для выбранных объектов и пользователей?
7. В каких случаях целесообразно учитывать Успех, а когда целесообразно фиксировать Отказ?
8. Как пользоваться журналами безопасности?
9. Какие учетные записи дают право на настройку аудита и проверку результатов аудита?
10. Каким образом администратор может использовать информацию об аудите для повышения безопасности системы?