Текущий контроль №4

1. Первое лабораторное задание

Планирование и настройка политики аудита ресурсов и событий

Планирование политики аудита

Для планирования политики аудита компьютера прежде всего нужно ответить на несколько вопросов.

- Какие типы событий регистрировать?
- Регистрировать успешные, неудачные попытки или оба вида событий?

Принимая решение, руководствуйтесь правилами, описанными далее.

- Необходимо регистрировать неудачные попытки доступа к компьютеру.
- Необходимо регистрировать неавторизованный доступ к файлам, составляющим базу данных по клиентам.
- Необходимо отслеживать использование цветного принтера для подготовки счетов за его использование.
- Необходимо следить, не пытается ли кто-либо изменить аппаратную конфигурацию компьютера.
- Необходимо вести учет действий, выполняемых администратором, чтобы отследить неавторизованные изменения.
- Необходимо вести учет процедур резервного копирования для предотвращения хищения данных.
- Необходимо отслеживать неавторизованный доступ к критически важным объектам Active Directory.

Ваши решения по аудиту перечисленных действий, успешных или неудачных попыток или обоих видов событий запишите в таблице.

Регистрируемое действие	**Успех**	**Отказ**
События входа в систему		
Управление учетными записями		
Доступ к службе каталогов		
Вход в систему		
Доступ к объектам		
Изменение системной политики		
Использование привилегий		
Отслеживание процесса		
Системные события		

Настройка политики аудита

1. Войдите в систему под любой учетной записью, входящей в группу***Администраторы*** (Administrators).
2. Щелкните ***Пуск*** (Start), щелкните ***Выполнить*** (Run), в поле ***Открыть*** (Open) наберите **mmc** и щелкните ОК.
3. В окне ***Консоль 1*** (Console 1), в меню ***Консоль*** (File), щелкните ***Добавить или***

удалить оснастку (Add/Remove Snap-In).
4. В окне ***Добавить или удалить оснастку*** (Add/Remove Snap-In) щелкните кнопку ***Добавить*** (Add),
5. В диалоговом окне ***Добавить изолированную оснастку*** (Add Standalone Snap-In) выберите в списке оснастку ***Групповая политика*** (Group Policy) и щелкните кнопку ***Добавить*** (Add).
6. Убедитесь, что в поле ***Объект групповой политики*** (Group Policy Object) окна***Выбор объекта групповой политики*** (Select Group Policy Object) значится***Локальный компьютер*** (Local Computer), затем щелкните кнопку ***Готово*** (Finish).
7. В диалоговом окне ***Добавить изолированную оснастку*** (Add Standalone Snap-In) щелкните ***Закрыть*** (Close).

Заметьте, что в окне Добавить/удалить оснастку (Add/Remove Snap-In) отображается элемент Политика «Локальный компьютер» (Local Computer Policy) несмотря на то, что вы выбрали оснастку Групповая политика (Group Policy). Дело в том, что для локального компьютера Групповая политика (Group Policy) означает то же самое, что и Политика «Локальный компьютер» (Local Computer Policy).

8. В окне ***Добавить/удалить оснастку*** (Add/Remove Snap-In) щелкните кнопку***Закрыть*** (Close).
9. В дереве консоли дважды щелкните элемент ***Политика «Локальный компьютер»*** (Local Computer Policy).
10. Дважды щелкните элемент ***Конфигурация компьютера*** (Computer Configuration), затем дважды щелкните элемент ***Конфигурация Windows*** (Windows Settings).
11. Дважды щелкните элемент ***Параметры безопасности*** (Security Settings), затем дважды щелкните элементе ***Локальные политики*** (Local Policies).
12. Щелкните элемент ***Политика аудита*** (Audit Policy). В правой панели окна***Политика «Локальный компьютер»*** (Local Computer Policy) отобразятся текущие параметры политики аудита как показано на рис. 4.1.
13. Чтобы настроить политику аудита, в списке укажите ***Аудит входа в систему***(Audit Logon Events) и в меню ***Действие*** (Action) щелкните пункт ***Свойства*** (Properties), появится окно ***Свойства: аудит входа в систему*** (Audit Account Logon Events Properties), как показано на рис. 4.2. Или в правой части окна дважды щелкните каждый тип события и установите флажок ***Успех*** (Audit Successful Attempts) или ***Отказ*** (Audit Failed Attempts) согласно следующей таблице.

Событие	Успех	Отказ
События входа в систему		
Управление учетными записями	X	
Доступ к службе каталогов		
Вход в систему		X
Доступ к объектам	X	X
Изменение политики	X	

Использование привилегий	X	
Отслеживание процесса	X	X
Системные события		

14. Закройте консоль MMC и сохраните локальную групповую политику.
15. Перезапустите компьютер, чтобы изменения немедленно вступили в силу.

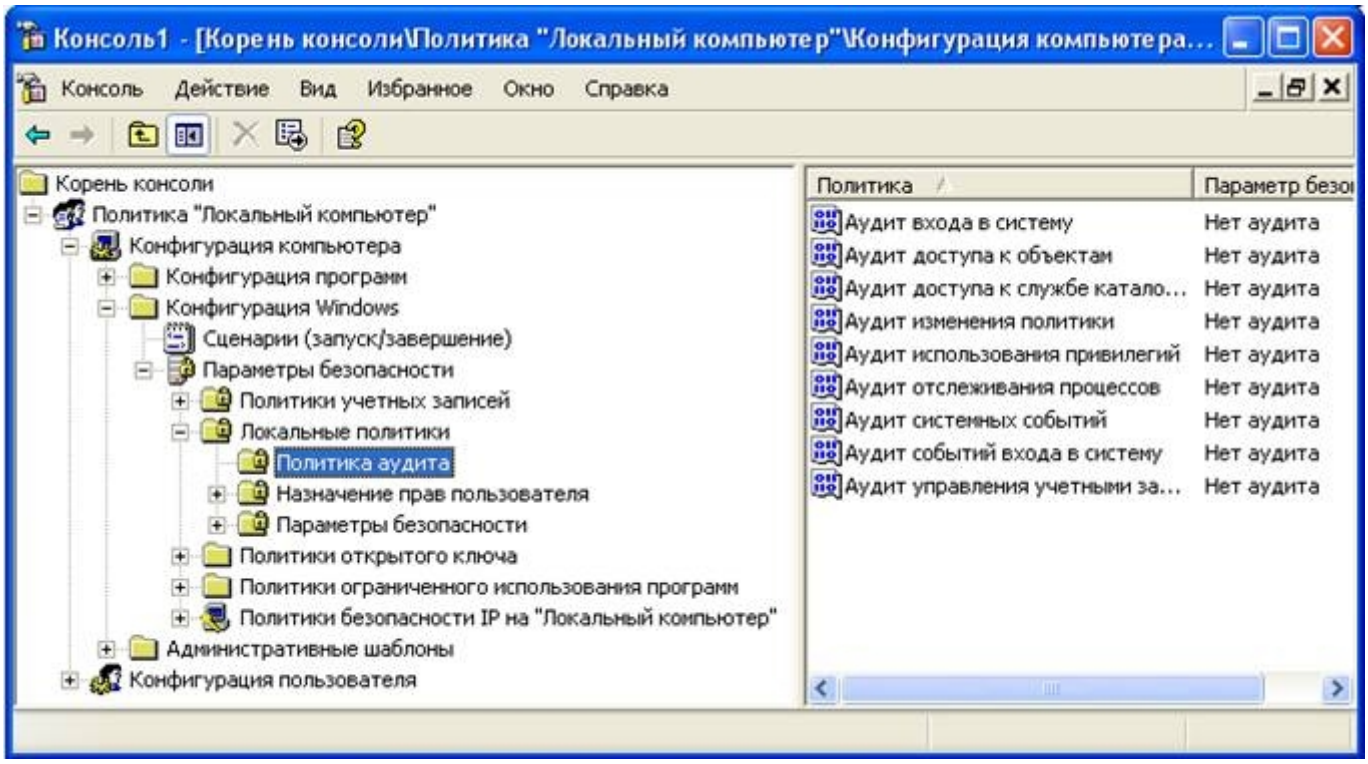

Рис. 4.1. События, для которых можно включить аудит в Windows XP Professional

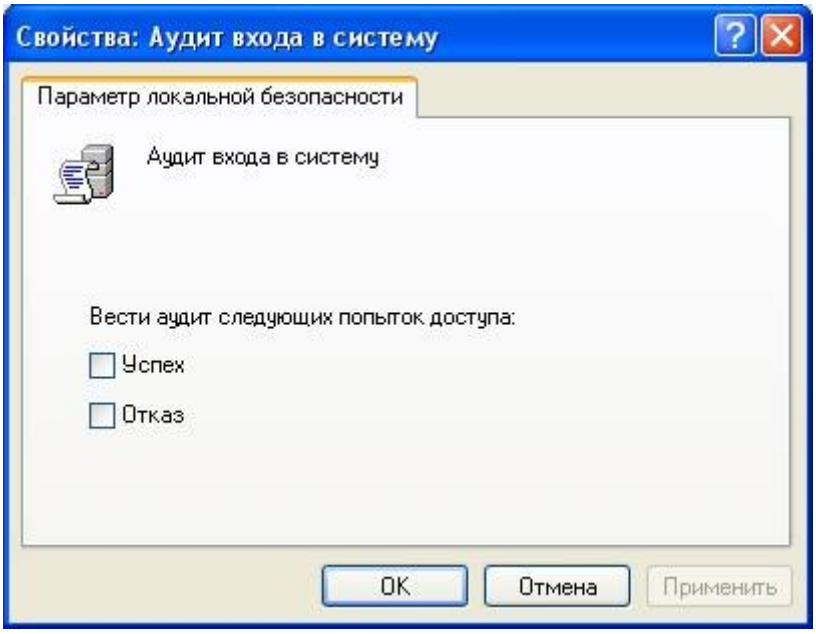

Рис. 4.2. Окно Свойства: аудит событий входа в систему

Совет: команда gpupdate позволяет обновлять параметры как локальной групповой политики, так и политики для объектов Active Directory, включая параметры безопасности. Чтобы обновить параметры на локальном компьютере, войдите в режим командной строки, наберите gpupdate и нажмите Enter. Для получения более полного описания команды gpupdate в меню Пуск (Start) щелкните Справка и поддержка (Help And Support) и используйте поиск для нахождения строки gpupdate.

4.2. Второе лабораторное задание
Настройка аудита объектов Windows XP Professional

Настройка аудита файлов

1. Войдите в систему с использованием любой учетной записи, входящей в группу***Администраторы*** (Administrators).
2. С помощью ***Проводника*** (Windows Explorer) создайте папку с именем **Audit** в корне системного диска (например, C:\Audit).
3. В папке **Audit** создайте текстовый файл с именем **AUDIT** (например, C:\Audit\Audit).
4. Щелкните правой клавишей мыши на файле **AUDIT** и выберите ***Свойства***(Properties).
5. В диалоговом окне ***Свойства*** (Properties) выберите вкладку ***Безопасность***(Security) и щелкните кнопку ***Дополнительно*** (Advanced).

Совет: Если в диалоговом окне Свойства (Properties) нет вкладки Безопасность (Security), выясните, находятся ли выбранные файлы и папки в разделе, отформатированном как NTFS? Если компьютер не входит в домен, выключен ли простой общий доступ к файлам (Simple File Sharing)? Для выключения простого общего доступа к файлам щелкните Пуск (Start), щелкните правой кнопкой мыши Мой компьютер (My Computer), затем щелкните пункт меню Проводник (Explore). В меню Сервис (Tools) выберите пункт Свойства папки (Folder Options). На вкладке Вид (View) снимите флажок Использовать простой общий доступ к файлам (Рекомендуется) [Simple File Sharing (Recommended)] и щелкните ОК.

6. В диалоговом окне ***Дополнительные параметры безопасности для*** **AUDIT**выберите вкладку ***Аудит*** (Auditing).
7. Щелкните кнопку ***Добавить*** (Add).
8. В диалоговом окне ***Выбор: пользователь или группа*** (Select User Or Group), в поле ***Имя*** (Name), укажите ***Все*** (Everyone) и щелкните ОК.
9. В диалоговом окне ***Элемент аудита для Audit.txt*** (Audit Entry For Audit.txt) установите флажки ***Успех*** (Successful) и ***Отказ*** (Failed) для каждого из следующих событий (рис. 4.4.):

- **Создание файлов/Запись данных (Create Files/Write Data);**
- **Удаление (Delete);**
- **Смена разрешений (Change Permissions);**

- **Смена владельца (Take Ownership).**

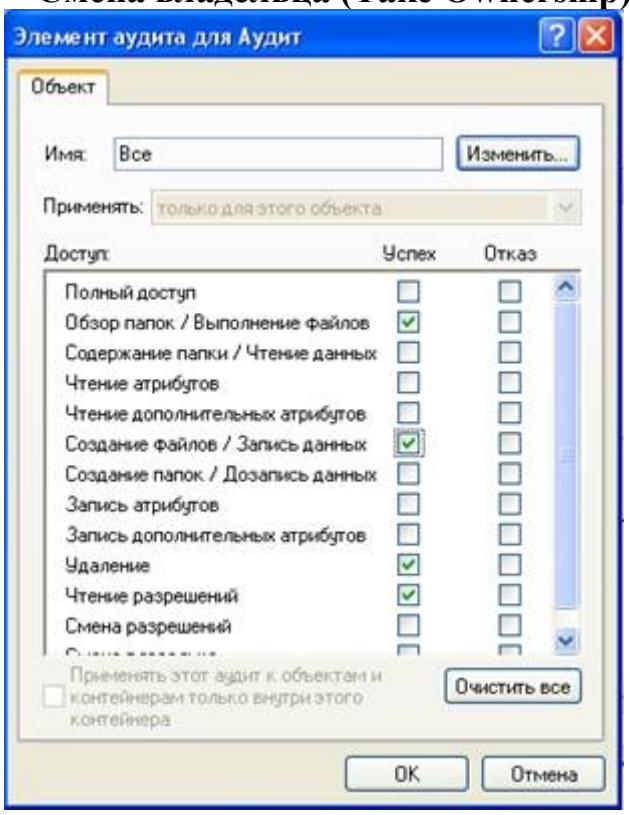

Рис. 4.4. События, аудит которых возможен для папок и файлов

10. Щелкните ОК. Windows XP Professional отобразит группу ***Все*** (Everyone) в диалоговом окне Дополнительные параметры безопасности для audit.txt (Advanced Security Settings For).
11. Для подтверждения изменений щелкните кнопку ОК.

Настройка аудита принтера

1. Щелкните ***Пуск*** (Start), затем — ***Панель управления*** (Control Panel), далее щелкните категорию ***Принтеры и другое оборудование*** (Printers And Other Hardware) и значок ***Принтеры и факсы*** (Printers And Faxes).
2. В окне ***Принтеры*** (Printers) щелкните правой кнопкой мыши значок принтера***HPColorLaserJet 4500 PS***, затем щелкните пункт меню ***Свойства*** (Properties).
3. На вкладке ***Безопасность*** (Security) щелкните кнопку ***Дополнительно***(Advanced).
4. В диалоговом окне ***Дополнительные параметры безопасности дляHPColorLaserJet 4500 PS*** , на вкладке ***Аудит*** (Auditing), щелкните кнопку***Добавить***.
5. В диалоговом окне ***Выбор: пользователь или группа*** (Select User Or Group), в поле ***Имя*** (Name), укажите ***Все*** (Everyone) и щелкните ОК.
6. В диалоговом окне ***Элемент аудита для HPColorLaserJet 4500 PS*** (Auditing Entry For HP Color LaserJet 4500 PS) установите флажок ***Успех*** (Successful) для

всех типов событий (рис.4.5.).

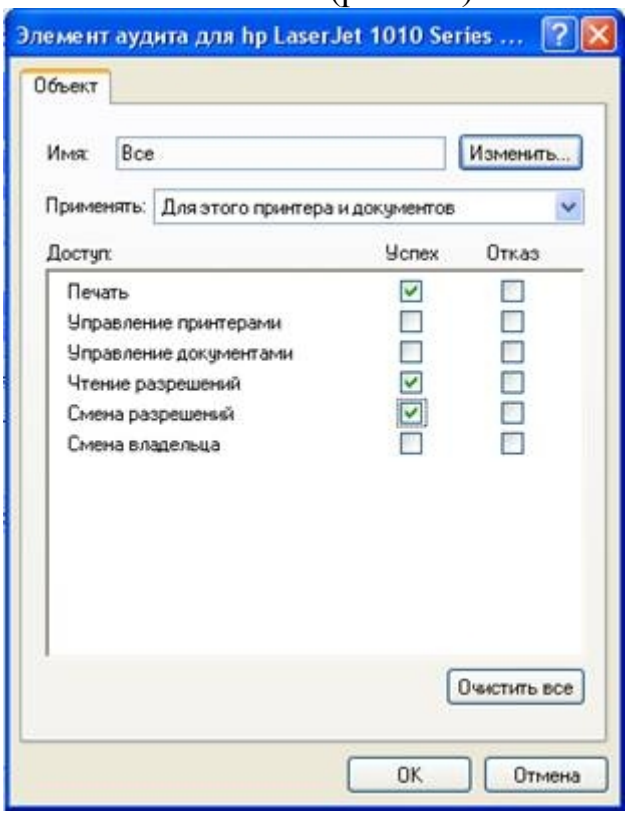

Рис. 4.5. События, аудит которых возможен для принтеров

7. Щелкните ОК. Windows XP Professional отобразит группу ***Все*** (Everyone) в диалоговом окне ***Управление доступом для HPColorLaserJet 4500 PS***(Access Control Settings For HP Color LaserJet 4500 PS).
8. Для подтверждения изменений щелкните ОК.
9. Закройте окно ***Свойства HPColorLaserJet 4500 PS*** (HP Color LaserJet 4500 PS Properties), щелкнув ОК.
10. Закройте окно ***Принтеры и факсы*** (Printers And Faxes).

Проверка правильности параметров политики аудита для файла AUDIT

1. Щелкните ***Пуск*** (Start), ***Панель управления*** (Control Panel), затем — ***Учетные записи пользователей*** (User Accounts).
2. Убедитесь, что учетная запись **User2** существует и является **ограниченной**(Limited).
3. Создайте пароль **User2** для учетной записи **User2**.
4. Закройте все окна и выйдите из системы.
5. Зарегистрируйтесь в системе под именем **User2**, используя пароль.
6. Откройте ***Проводник*** (Windows Explorer), затем откройте файл **C:\Audit\Audit**. В открывшемся окне программы ***Блокнот*** (Notepad) появится пустой файл **AUDIT**.
7. Введите следующий текст: «**Этот файл изменен пользователем User2**».
8. Попытайтесь сохранить файл. Удалось ли вам сохранить файл? Почему?
9. Закройте файл, не сохраняя его, и завершите работу с системой.

4.3. Третье лабораторное задание

Управление журналом безопасности

Просмотр журнала безопасности компьютера и отбора событий

1. Войдите в систему под любой учетной записью, входящей в группу***Администраторы*** (Administrators).
2. Щелкните ***Пуск*** (Start), ***Панель управления*** (Control Panel), категорию***Производительность и обслуживание*** (Performance And Maintenance) и***Администрирование*** (Administrative Tools), затем дважды щелкните ярлык***Просмотр событий*** (Event Viewer).
3. В дереве консоли щелкните ***приложение*** (Application Log) и просмотрите его содержимое. Просмотрите описание нескольких событий, дважды щелкнув соответствующие записи.
4. В дереве консоли щелкните ***система*** (System Log) и просмотрите его содержимое. Просмотрите описание нескольких событий, дважды щелкнув каждую их соответствующих записей (рис. 4.6.).

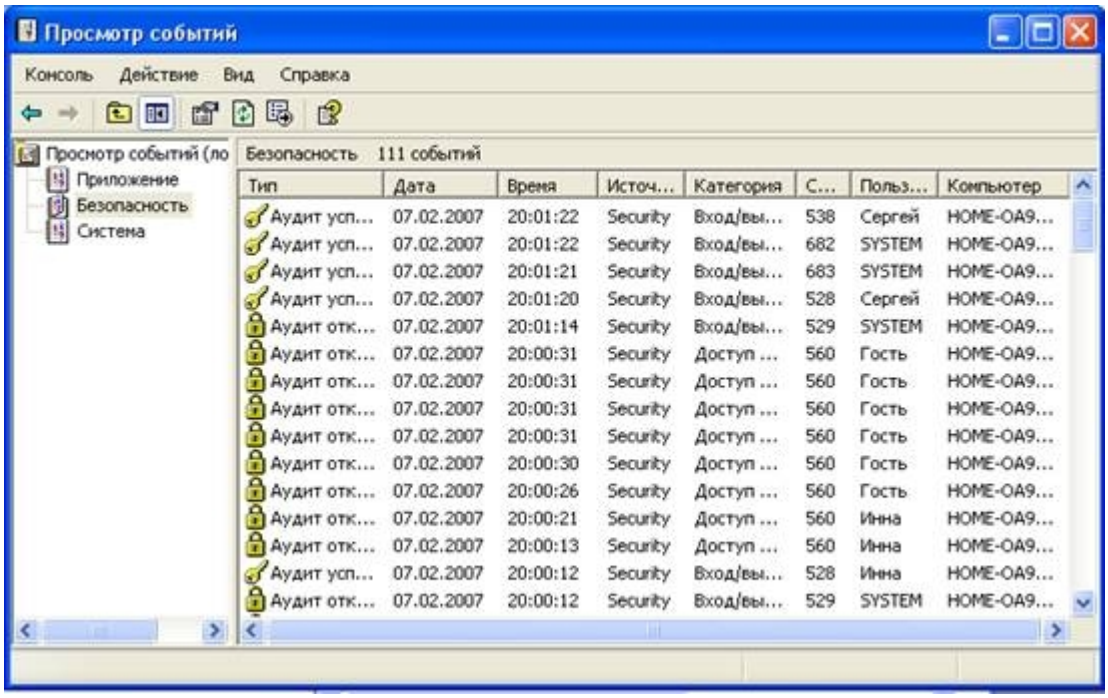

Рис. 4.6. Отображение журнала безопасности в окне утилиты Просмотр событий (Event Viewer)

Успешные попытки условно обозначены значком ключа, а неудачные — значком замка. Кроме того, указаны дата и время события, категория события и пользователь, действие которого вызвало данное событие. В колонке ***Категория***(Category) отображается тип события, например доступ к объекту, управление учетными записями, доступ к службе каталогов или попытки регистрации в системе. Типы регистрируемых событий представлены в таблице 4.8.
Чтобы просмотреть дополнительную информацию о любом событии, щелкните название события и в меню ***Действие*** (Action) щелкните пункт ***Свойства***(Properties).
5. В дереве консоли щелкните ***безопасность*** (Security Log) и просмотрите его содержимое. Просмотрите описания всех событий категории ***Отказ*** (Failure),

дважды щелкая соответствующие записи, пока не найдете попытку доступа пользователя **User2** к файлу **C:\Audit\Audit**.
6. В меню ***Вид*** (View) выберите пункт ***Фильтр*** (Filter).
На рис. 4.7 показаны параметры вкладки ***Фильтр*** (Filter).

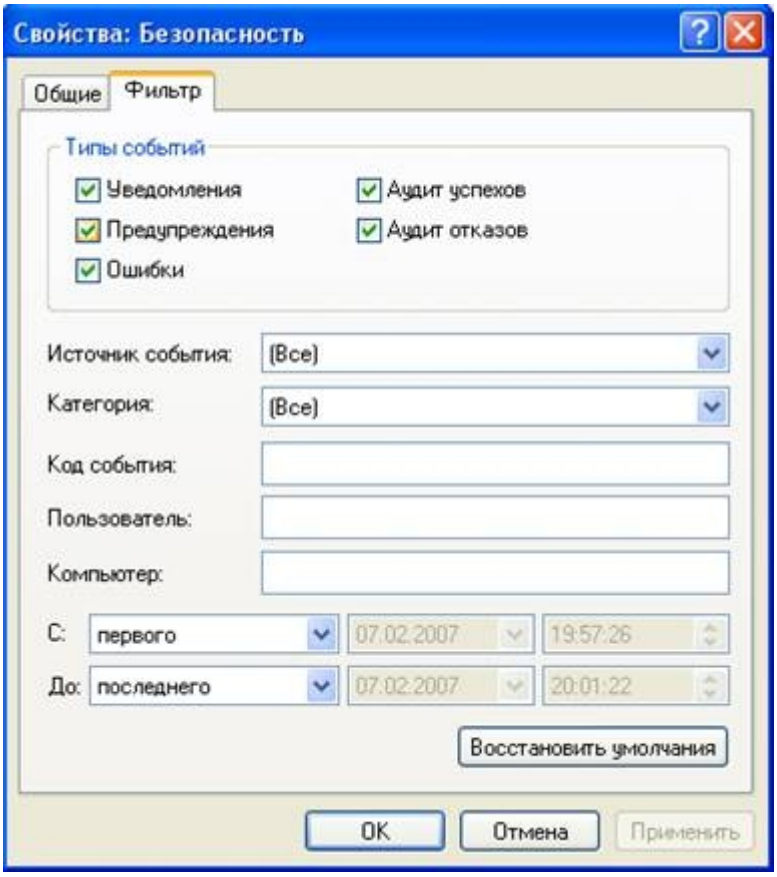

Рис. 4.7. Вкладка Фильтр (Filter) окна Свойства:Безопасность (System Properties) утилиты Просмотр событий (Event Viewer)

7. В диалоговом окне ***Свойства: Безопасность*** (Security Properties), в поле***Пользователь*** (User), введите **User2** и щелкните ОК. Применение фильтра уменьшит число событий, которые придется просмотреть, чтобы найти нужное.
8. Дважды щелкните каждое из событий. Обратите внимание, что все они относятся к пользователю **User2**.

Настройка размера и содержимого файла журнала

1. В дереве консоли выберите элемент ***Система*** (System).
2. В меню ***Действие*** (Action) щелкните пункт ***Свойства*** (Properties).
3. В диалоговом окне свойств журнала выберите ***Затирать старые события по необходимости*** (Overwrite Events As Needed).
4. В поле ***Максимальный размер журнала*** (Maximum Log Size) измените максимальный размер журнала на **2048 кбайт** и щелкните ОК. Теперь Windows XP Professional будет заполнять журнал, пока его объем не достигнет 2048 кбайт, а затем начнет затирать старые события по мере необходимости.
5. Закройте окно ***Просмотр событий*** (Event Viewer) и окно ***Администрирование***(Administrative Tools).

Типы регистрируемых событий **Таблица 4.8**

Идентификатор	Категория	Описание
512	Системное событие	Перезагрузка операционной системы
513	Системное событие	Завершение работы операционной системы (shutdown)
514	Системное событие	Загрузка пакета аутентификации
515	Системное событие	Запуск процесса аутентификации (в стандартной конфигурации WinLogon.exe)
516	Системное событие	Сбой при ретистрации одного или нескольких событий аудита1
517	Системное событие	Очистка журнала аудита
518 528	Системное событие Вход/выход пользователя \лз системы	Загрузка пакета оповещения об изменениях в списке пользователей Пользователь успешно вошел в систему
529	Вход/выход пользователя из системы	Вход пользователя в систему запрещен -имя или пароль, введенные при входе в систему, некорректны
530	Вход/выход пользователя из системы	Вход пользователя в домен в данное время запрещен
531	Вход/выход пользователя из системы	Вход пользователя в систему запрещен -учетная запись пользователя заблокирована администратором
532	Вход/выход пользователя из системы	Вход пользователя в Домен запрещен -учетная запись пользователя автоматически заблокирована по достижении определенной даты
533	Вход/выход пользователя из системы	Вход пользователя в домен с данной рабочей станции запрещен
534	Вход/выход пользователя из системы	Данный тип (интерактивный, сетевой или сервисный) входа пользователя в систему запрещен
535	Вход/выход пользователя из системы	Вход пользователя в систему запрещен -пароль пользователя устарел
536	Вход/выход пользователя из системы	Пользователь не смог войти в домен из-за сбоев сетевых сервисов
537	Вход/выход пользователя из системы	Пользователь не смог войти в систему по какой-то другой причине

538	Вход/выход пользователя из системы	Пользователь успешно вышел из системы

Продолжение табл. 4.8

Идентификатор	Категория	Описание
539	Вход/выход пользователя из системы	Вход пользователя в систему запрещен -учетная запись пользователя автоматически заблокирована из-за превышения максимально допустимого количества попыток входа в систему с неверным паролем
560	Доступ к объекту	Пользователь попытался открыть объект
561	Доступ к объекту	Пользователь закрыл объект
576	Использование опасных привилегий	В маркере доступа пользователя присутствует опасная привилегия
577	Использование опасных привилегий	Предпринята попытка использования опасной привилегии при выполнении операции, не связанной с доступом к объектам3
578	Использование опасных привилегий	Предпринята попытка использования опасной привилегии для получения доступа к объекту
592	Запуск/завершение процессов	Запуск нового процесса
593	Запуск/завершение процессов	Завершение процесса
594	Запуск/завершение процессов	Дублирование дескриптора (handle) объекта
595	Запуск/завершение процессов	Непрямой доступ к объекту
608	Изменения в политике безопасности	Субъекту предоставлена новая привилегия
609	Изменения в политике безопасности	У субъекта отнята привилегия
610	Изменения в политике безопасности	Установлены доверительные отношения с другим доменом
611	Изменения в политике безопасности	Доверительные отношения с другим доменом прекращены
612	Изменения в политике безопасности	Изменена политика аудита

624	Изменения в списке пользователей2	Создана учетная запись нового пользователя
625	Изменения в списке пользователей	Изменен тип учетной записи
626	Изменения в списке пользователей	С учетной записи пользователя снята блокировка
627	Изменения в списке пользователей	Неудачная попытка изменить пароль пользователя
628	Изменения в списке пользователей	Удачная попытка изменить пароль пользователя
629	Изменения в списке пользователей	Учетная запись пользователя заблокирована

Окончание табл. 4.8

Идентификатор	Категория	Описание
630	Изменения в списке пользователей	Учетная запись пользователя удалена
631	Изменения в списке пользователей	Создана новая глобальная группа
632	Изменения в списке пользователей	Пользователь добавлен в глобальную группу
633	Изменения в списке пользователей	Пользователь удален из глобальной группы
634	Изменения в списке пользователей	Глобальная группа удалена
635	Изменения в списке пользователей	Создана новая локальная группа
636	Изменения в списке пользователей	Пользователь добавлен в локальную группу
637	Изменения в списке пользователей	Пользователь удален из локальной группы

638	Изменения в списке пользователей	Локальная группа удалена
639	Изменения в списке пользователей	Произведены изменения в учетной записи локальной группы, не связанные с изменением членства пользователей в этой группе
640	Изменения в списке пользователей	Произведены изменения в списке пользователей, не связанные с редактированием учетных записей
641	Изменения в списке пользователей	Произведены изменения в учетной записи глобальной группы, не связанные с изменением членства пользователей в этой группе
642	Изменения в списке пользователей	Произведены изменения в учетной записи пользователя, не связанные с изменением типа учетной записи, пароля пользователя и членства пользователя в группах

5. УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ ОТЧЕТА.

Отчет должен содержать:

- название работы;
- цель работы;
- порядок действий по выполнению лабораторной работы;
- выводы по результатам проделанной работы.

6. КОНТРОЛЬНЫЕ ВОПРОСЫ ПО ВЫПОЛНЕННОЙ РАБОТЕ.

1 Какие три журнала Windows XP Professional можно просматривать средствами утилиты просмотра событий? Для чего предназначен каждый из них?
2 Как просмотреть журнал безопасности удаленного компьютера?
3 Какие два способа поиска конкретных событий есть в утилите просмотра событий? Что позволяет делать каждая из команд?
4 Размер любого из журналов может изменяться от_____кбайт до_____Гбайт, а по умолчанию он равен_____кбайт.

- Что происходит при переполнении журнала, если для него выбран параметр Не затирать события (очистка журнала вручную) (Do Not Overwrite Events)?