**Лекции №12: Аудит и журналы безопасности**

**Цель:** познакомить студентов с понятием и методами проведения аудита информационной безопасности, а также с важностью ведения журналов безопасности для мониторинга, анализа и обнаружения угроз. Рассмотреть, как эффективное использование журналов безопасности помогает в предотвращении атак и повышении общей защиты системы.

Отслеживание событий является обычной и необходимой частью работы системных администраторов (или менеджеров веб-сайтов). Для этого в *Windows* 2000 и *IIS* используются журналы и *аудит*. Процедуры управления сайтом включают в себя регулярную проверку, *анализ* и просмотр зафиксированной информации для выявления неудавшихся или успешных атак, направленные на *сайт*. При обнаружении проблемы следует выполнить *аудит безопасности* для определения нанесенного ущерба и способа проникновения в систему.

В любой политике безопасности имеются процедуры и стандартные приемы для этих случаев. Даже и не думайте о работе сайта, если такая политика еще не разработана. В лекции рассказывается о том, как настраивать журнал, осуществлять *аудит*, создавать резервные копии и производить восстановление. Все эти действия необходимы для обеспечения безопасной и надежной работы сервера и веб-сайта.

### Отслеживание событий сайта

События, происходящие на веб-сервере *Windows* 2000/*IIS*, отслеживаются при помощи просмотра и анализа журнала, в который отправляются сообщения от других служб, приложений или операционной системы. Эти сообщения учитывают события, происходящие в системе: выключение, *запуск*, создание новой учетной записи и т.д. *IIS* дополнительно отслеживает события собственного набора служб, например, запросы от посетителей сайта, отправленные на *сервер* для осуществления анонимного входа.

В *Windows* 2000 имеются журналы шести различных типов. Если вы имеете *опыт* системного администрирования *Windows* 2000, то уже знакомы с некоторыми из них. *IIS* ведет свой собственный отдельный журнал. Ниже приведен полный перечень журналов, работающих на сервере.

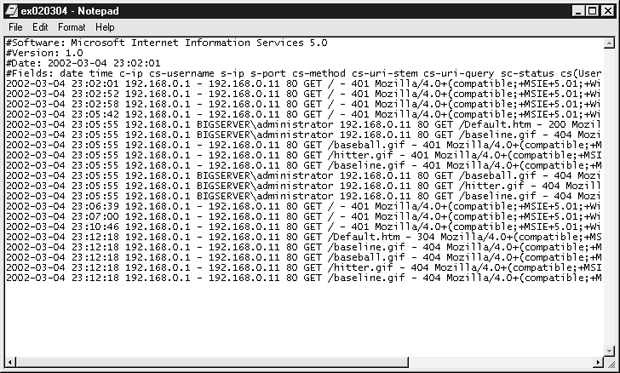
* **Системный журнал**. Фиксирует события компонентов: остановку и запуск службы или возникновение ошибки.
* **Журнал безопасности**. Записывает события, связанные с безопасностью: вход пользователей и использование ресурсов, например, создание, открытие и удаление файлов.
* **Журналы приложений**. Фиксируют события, связанные с приложениями, выполняемыми на сервере.
* **Журнал службы каталогов**. Фиксирует информацию о работе службы Active Directory, например, проблемы с подключением к глобальному каталогу.
* **Журнал сервера DNS**. Записывает события, связанные с работой службы Windows 2000 DNS в Active Directory.
* **Журнал службы репликации файлов**. Фиксирует значимые события, происходящие при попытке контроллера домена обновить другие контроллеры домена.
* **Журнал IIS**. Фиксирует события, происходящие при работе служб IIS (WWW, FTP и т.д.).

Для веб-сервера *IIS* не требуется работа всех без исключения журналов, например, не нужны журналы сервера *DNS* и службы репликации файлов. Журнал службы каталогов включается, если *сервер* является частью домена *Windows* *Active Directory*, причем ведется он на другом сервере. Веб-*сервер* работает с системным журналом, журналом приложений, журналом безопасности и журналом *IIS*.

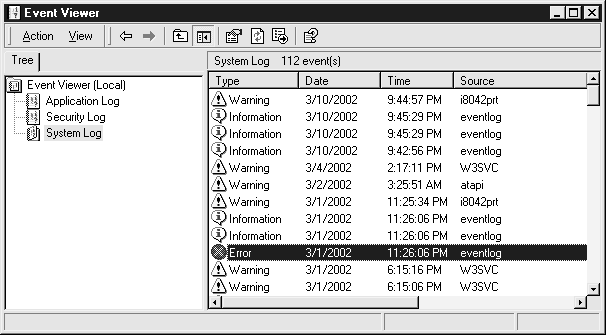
*Системный журнал* *Windows* 2000 и журнал приложений активируются по умолчанию при установке *IIS* для автоматического фиксирования *системных событий* и событий приложений. Остальные журналы запускаются только после их непосредственной настройки и/или запуска. При выполнении *IIS* Lockdown автоматически активируется журнал безопасности *Windows* 2000 и *IIS*.

#### Информация журналов событий

Журналы Windows 2000 и IIS можно настроить на запись большого числа различных событий и действий. IIS по умолчанию сохраняет файлы журнала в текстовом формате, их можно просматривать в любом приложении, поддерживающем этот формат. Обычно файлы анализируются посредством их загрузки в программу генерации отчетов, которая осуществляет фильтрацию, сортировку и управление данными. На рисунке приведен пример содержимого файла журнала IIS.

[](https://www.intuit.ru/EDI/27_04_15_5/1430086749-14056/tutorial/221/objects/5/files/05_01.gif)

*Системный журнал* Windows 2000 по умолчанию хранится в специальном формате в файлах с расширением .evt. Программа Event Viewer (Просмотр событий) Windows 2000, доступная в консоли MMC в папке Administration Tools (Администрирование), позволяет просматривать сообщения в журналах Windows 2000 и упорядочивать их по дате, времени, источнику, степени значимости и по другим переменным. Event Viewer используется также для преобразования файлов журнала в текстовый формат для просмотра в другой программе. На рисунке показана консоль программы Event Viewer.

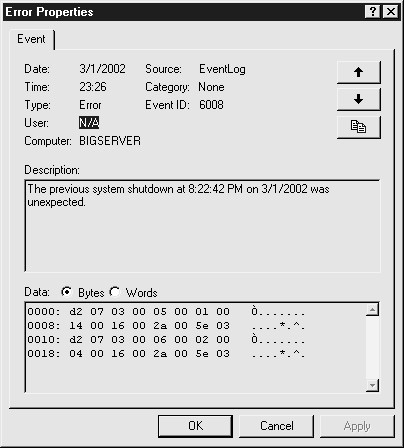


Анализ аспектов безопасности при помощи файлов журналов требует некоторых навыков. Следует различать типы сообщений и понимать, что они означают. Когда ваш сервер начнет свою работу, внимательно следите за ним в течение некоторого времени и фиксируйте признаки нормальной работы, чтобы выявлять впоследствии отклонения от нормы.

Каждая из пяти категорий записей журналов имеет свой собственный значок. Каждое сообщение содержит идентификатор события ID, дату, время, объект, имя компьютера, категорию и тип номера события сообщения. Ниже приведены категории сообщений и их назначение.

* **Информационные сообщения о событиях**. Описывают успешное выполнение операций, таких как запуск 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.
* **Сообщения о событиях успешного выполнения той или иной операции**. Описывают события безопасности, выполненные Windows 2000 согласно запросу.
* **Сообщения о событиях неудачного выполнения операции**. Описывают события безопасности, не выполненные Windows 2000 согласно запросу.

На [рисунке 5.1](https://www.intuit.ru/studies/courses/1002/122/lecture/3525?page=1" \l "image.5.1) приведен пример сообщения об ошибке в системном журнале Windows 2000, зафиксировавшего неожиданное отключение сервера. Это событие выходит за рамки нормальной работы и его необходимо исследовать. По идентификационному номеру ID события его можно найти в базе данных *Microsoft Knowledge Base*, если не понятно, что оно означает.



**Рис. 5.1.**Сообщение системного журнала Windows 2000, информирующее о неожиданном отключении

#### Аудит

В Windows 2000 и IIS имеется специальная функция по отслеживанию безопасности – аудит, фиксирующая в журнале безопасности события, связанные с ресурсами IIS и Windows 2000 либо с объектами управления системой. Аудит является сложным процессом, использующим средства для анализа собранной информации и диагностики событий сайта, связанных с безопасностью.

Windows 2000 предоставляет три типа возможностей по аудиту объектов и ресурсов, свои функции имеются и в IIS (см. [табл. 5.1](https://www.intuit.ru/studies/courses/1002/122/lecture/3525?page=1" \l "table.5.1)).

|  |  |
| --- | --- |
| Таблица 5.1. Типы аудита в Windows 2000 и IIS | |
| **Тип аудита** | **Системы, в которых применяется аудит** |
| Система и реестр | Windows 2000 и IIS. |
| Файловая система | Windows 2000 и IIS. |
| Учетная запись пользователя | Windows 2000 и IIS. |
| Посетители домашней страницы | Только IIS. |
| Авторство | Только IIS. |

При аудите отслеживаются события согласно правилам аудита, определенным в локальной политике безопасности сервера и/или *параметрах веб*-сайта. Осуществляется аудит событий, входящих в следующие девять категорий.

* **События системы**. События, связанные с безопасностью, такие как отключение системы и ее перезапуск; события, влияющие на журнал безопасности.
* **Отслеживание процесса**. Детализированное отслеживание вызова процесса, дубликатов процессов, непрямого доступа к объектам и уничтожения процесса.
* **Изменение политики**. Изменение политики безопасности, включая присвоение привилегий, модификацию политики аудита и параметров доверия.
* **Использование привилегий**. Использование привилегий, присвоение специальных привилегий.
* **Управление учетной записью**. Создание, изменение, удаление пользователей и групп; изменение паролей.
* **Доступ к службе каталогов**. Отслеживание доступа к Active Directory. Включается для разрешения аудита определенных объектов каталога, работает только на контроллерах домена.
* **События входа в учетную запись**. Аутентификация на локальном компьютере в консоли или через сеть.
* **События входа**. Интерактивный вход или сетевые подключения к локальному компьютеру; генерируются в том месте, где происходит вход.
* **Доступ к объектам**. Попытки доступа к определенным объектам: файлам, каталогам, учетным записям пользователей и параметрам реестра.

Событие, для которого выполнен аудит, имеет два значения: успех и неудача. Для каждой категории событий возможен аудит успешных, неудачных или обоих типов событий. Тревожным признаком является высокая концентрация событий в журнале или необычная последовательность событий. Например, большое число событий ввода неправильного пароля означает, что сервер подвергся атаке на взлом пароля.

### Регистрация процедур настройки и поддержки в журнале

*Совместная работа* журналов и аудита отслеживает работу системы, однако этого недостаточно для аудита безопасности. Для надежного аудита безопасности имеются процедуры просмотра файлов журнала для обеспечения их сохранности, архивного состояния и правильного функционирования. Только при правильной настройке журналов, их включении и регулярном обслуживании *аудит безопасности* осуществляется конфиденциально и с высокой *степенью доверия*. Журналы помогут восстановить цепь событий при нарушении безопасности, послужат официальными доказательствами в суде по искам в области информационной безопасности.

Ведение журналов и *аудит* в *Windows* 2000 и *IIS* настраиваются на фиксирование определенного числа событий. При настройке системы на *запись* слишком большого количества информации журналы событий быстро заполняются. Какой смысл записывать данные, которые никогда не понадобятся? С другой стороны, при фиксировании малого числа событий можно утерять важную информацию. Решение о записи тех или иных событий является очень ответственным и должно быть тщательно обдумано.

#### Цели и задачи аудита

Планирование, политика и поддержка являются ключевыми моментами для сбора важной информации, которая пригодится в критической ситуации. При четкой постановке целей легче определить тип фиксируемой информации и настроить журналы на запись необходимого количества данных. Параметры запуска IIS Lockdown и/или шаблона Hisecweb.inf обеспечивают надежную базовую политику. Их настройки можно изменить для фиксирования дополнительной информации.

Нужно решить, для каких ресурсов и объектов управления необходим аудит, затем для каждого класса ресурсов или объектов выявить отслеживаемые события. В [таблице 5.2](https://www.intuit.ru/studies/courses/1002/122/lecture/3525?page=2" \l "table.5.2) приведена информация из официального издания " *Security Auditing in Windows 2000* " ("*Аудит безопасности* в Windows 2000"), расположенного на веб-сайте Microsoft Technet ([http://www.Microsoft.com/technet](http://www.microsoft.com/technet" \t "_blank)). Таблица содержит примеры событий, связанных с безопасностью различных ресурсов и объектов. Она показывает использование целенаправленного подхода к аудиту, но он может и не подойти вашей организации. Необходимо самостоятельно принять решение о необходимости аудита ресурсов и отслеживаемых событий. Например, при выполнении атаки на объект лучшими индикаторами будут события ошибок, так как они зафиксируют попытки доступа пользователя, не имеющего соответствующего разрешения.

|  |  |  |
| --- | --- | --- |
| Таблица 5.2. События, помогающие идентифицировать проблемы безопасности | | |
| **Потенциальная угроза** | **Тип аудита** | **Результирующие события** |
| Взлом пароля с использованием генератора случайных паролей | Учетная запись пользователя | Неудача процедуры аудита для событий входа/выхода из системы. Большое число событий означает повторяющиеся попытки входа, часто являющиеся результатом систематической атаки. |
| Вход с использованием украденного пароля | Учетная запись пользователя | Успешный аудит событий входа/выхода для идентификации пользователей системы с целью определения места, откуда инициировано вторжение. |
| Несанкционированный доступ к секретным файлам | Файловая система | Успех и неудача аудита для событий доступа к файлам и объектам в сильно защищенных ресурсах. Успех и неудача аудита доступа для чтения/записи секретных файлов подозреваемыми пользователями или группами. |
| Злоупотребление привилегиями | Файловая система и реестр | Успешный аудит прав пользователей, управления пользователями и группами, изменения политики безопасности, перезапуска, выключения и *системных событий* для выявления пользователей, внесших изменения, и определения этих изменений. |

#### Управление журналами

Каждый файл журнала Windows 2000 имеет свои параметры конфигурации. Они позволяют изменять объем пространства, отводимого для файлов журналов на диске, и указывать действие, выполняемое после заполнения журнала. Эти параметры приведены ниже.

* **Максимальный размер файла журнала**. Настраивается при помощи приложения Event Viewer (Просмотр событий), значение по умолчанию – 512 Кб.
* **Перезапись файла журнала после его заполнения**. Имеет три значения: перезапись событий при необходимости, перезапись событий, возраст которых превышает определенное число дней, и запрет перезаписи.
* **Отключение сервера при ошибке аудита**. Вызывает остановку сервера в случае заполнения журнала безопасности при отсутствии перезаписи событий. В материалах Microsoft он называется "CrashOnAuditFail" и соответствует значению, устанавливаемому политикой безопасности в системном реестре.

IIS имеет аналогичные параметры файла журнала, но они отличаются от рассмотренных выше. Параметры файла журнала IIS следующие.

* Разрешение неограниченного размера файла журнала.
* Создание нового файла журнала по достижении файлом определенного размера.
* Создание нового файла журнала по прошествии определенного периода времени (час, день, неделя, месяц).

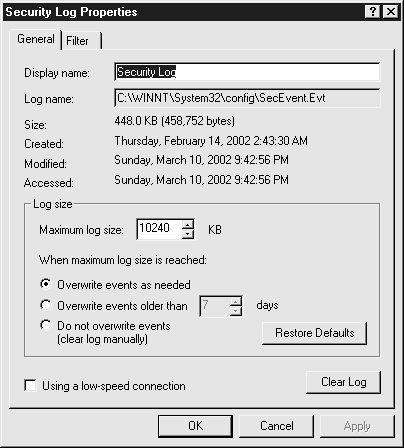
При управлении файлами журнала укажите для этих параметров соответствующие значения и действия. Убедитесь в их защищенности и обеспечьте периодическую архивацию для освобождения пространства под новые файлы и записи истории событий.

##### Настройка параметров журнала

Для отображения информации журнала, для установки и управления его параметрами используется программа Windows 2000 Event Viewer (Просмотр событий). Event Viewer позволяет устанавливать размер файла журнала, выбирать действие по перезаписи, включать и выключать параметр "CrashOnAuditFail". Для управления файлами журнала IIS используется консоль MMC Internet Services Manager (Диспетчер служб интернета).

**Настройка размера и перезаписи файла журнала Windows 2000**. Процедуры настройки размера файла журнала и параметров его перезаписи в Windows 2000 одинаковы для всех типов журнала.

1. Откройте программу Event Viewer (Просмотр событий) в окне Administrative Tools (Администрирование).
2. В левом окне консоли Event Viewer щелкните правой кнопкой мыши на записи *Security Log* (Журнал безопасности) и выберите Properties (Свойства). Откроется окно *Security Log* Properties (Свойства журнала безопасности) (см. [рис. 5.2](https://www.intuit.ru/studies/courses/1002/122/lecture/3525?page=2" \l "image.5.2)).
3. На вкладке General (Общие) укажите размер файла журнала в области Log Size (Размер журнала). Значением по умолчанию является 1024 Кб. Введите нужное значение в зависимости от размера диска или раздела сервера, от объема получаемого сайтом трафика. Можете в течение некоторого времени отслеживать размер файла журнала, чтобы выяснить величину этого размера.



**Рис. 5.2.**Настройка свойств журнала безопасности в окне Security Log (Журнал безопасности)

1. Определите параметр перезаписи файла посредством выбора одной из опций. Выбор опции зависит от периодичности, с которой планируется проводить архивацию данных журнала. При высоком уровне доступности сайта безопаснее всего использовать опцию *Overwrite* events as needed (Перезапись событий по мере надобности) и запретить заполнение журнала до отказа, так как в этом случае можно потерять данные.
2. Нажмите на OK после выбора опции, чтобы сохранить изменения и закрыть окно.

вопросов для закрепления материала

1. **Что такое аудит информационной безопасности и какую роль он играет в защите системы?**
2. **Какие журналы событий существуют в Windows 2000, и какие из них используются для веб-сервера IIS?**
3. **Какие типы событий фиксируются в системном журнале Windows 2000 и журнале IIS?**
4. **Какие типы сообщений могут быть записаны в журналы событий? Приведите примеры для каждого типа.**
5. **Что такое журнал безопасности в Windows 2000, и какие события в нем фиксируются?**
6. **Что такое аудит в контексте безопасности, и как он работает в Windows 2000 и IIS?**
7. **Какие типы аудита можно настроить в Windows 2000 и IIS?**
8. **Какой процесс должен быть выполнен при обнаружении проблемы на сервере через журнал событий?**
9. **Какие категории событий отслеживаются в процессе аудита?**
10. **Какую информацию можно получить из файлов журналов и каким образом ее можно анализировать?**
11. **Как можно использовать консоль Event Viewer для работы с журналами событий?**
12. **Какие шаги предпринимаются для настройки журналов и аудита в IIS и Windows 2000?**
13. **Какой роль в мониторинге безопасности выполняют журналы приложений и журнал службы каталогов?**
14. **Что такое политика безопасности сервера, и как она связана с настройкой аудита?**
15. **Как эффективное использование журналов безопасности может помочь предотвратить атаки и повысить защиту системы?**