**Лабораторная работа № 2.**

Управление политикой безопасности в операционной системе windows

1.Постановка задачи:

Цель работы – освоения средств администратора и аудитора операционной системы Windows.

Ответить на вопросы

Результат выполненной работы:

Вопросы:

1)Какие события безопасности должны фиксироваться в журнале аудита?

В Журнале событий фиксируются следующие виды событий:

* Вход в систему
* Управление учетной записью
* Доступ к службе каталогов
* Доступ к объектам
* Изменения политики
* Использования привилегий
* Отслеживание процессов
* Системных событий
* Событий входа в систему

Количество событий, которые записываются в журнал, очень велико, поэтому анализ журнала событий может быть довольно трудоемкой задачей. Для этого разработаны специальные утилиты, помогающие выявлять подозрительные события. Кроме того, можно фильтровать журнал по задаваемым критериям.

2) Какие параметры определяют политику аудита?

* Аудит вход в систему
* Аудит управление учетной записью
* Аудит доступ к службе каталогов
* Аудит доступ к объектам
* Аудит изменения политики
* Аудит использования привилегий
* Аудит отслеживание процессов
* Аудит системных событий
* Аудит событий входа в систему

3) целесообразно ли с точки зрения безопасности компьютерной системы разрешать анонимный доступ к ее информационным ресурсам?

- Нет, поскольку в таком случае можно получить доступ ко данным, имея всего лишь физическую возможность взаимодействия с системой.

4) как должен передаваться по сети (с точки зрения безопасности компьютерной системы) пароль пользователя?

- В зашифрованном виде, чтобы снизить вероятность того, что эта информация попадет к злоумышленникам.

5) нужно ли ограничивать права пользователей по запуску прикладных программ?

- Да, чтобы избежать технических проблем, вызванных отсутствием компетенции у неопытного пользователя.

1. В чем уязвимость с точки зрения безопасности информации принимаемой по умолчанию реакции системы на превышение размера журнала аудита?

- Когда журнал безопасности переполнится, Windows перестанет отвечать на запросы и будет выведено сообщение "Неудачная попытка аудита". Чтобы восстановить после остановки Windows, необходимо очистить журнал безопасности.

2. Какое из дополнительных правил ограниченного использования программ кажется Вам наиболее эффективным и почему?

- Выбор уровня безопасности для указанного пути. Доступны следующие уровни безопасности: неограниченный, позволяющий запускать программное обеспечение с полным набором прав зарегистрированного пользователя, и запрещенный, не позволяющий запускать программное обеспечение.

3. Из каких этапов состоит построение политики безопасности для компьютерной системы?

- определение, какие данные и насколько серьезно необходимо защищать,

- определение кто и какой ущерб может нанести фирме в информационном аспекте,

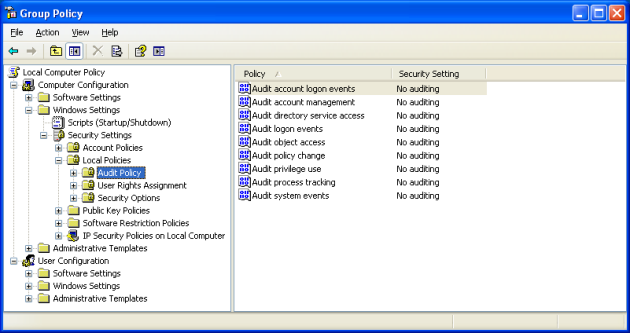
- вычисление рисков и определение схемы уменьшения их до приемлемой величины.

4. К чему может привести ошибочное определение политики безопасности?

- К утечке, потере или повреждению данных и(или) системы.

Применение Аудита Windows для отслеживания деятельности пользователей:

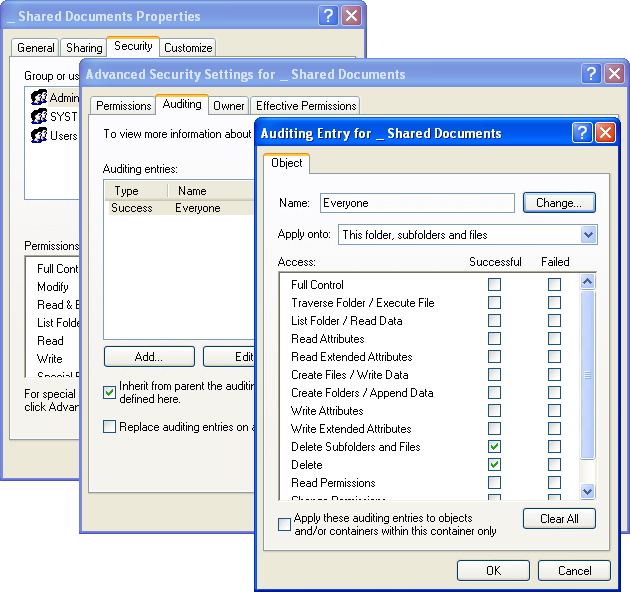
Для включения аудита зайдите с правами администратора в компьютер, предоставляющий доступ к общим документам, и выполните команду **Start**→**Run**→**gpedit.msc.** В разделе Computer Configuration раскройте папку **Windows Settings → Security Settings → Local Policies → Audit Policies:**

[](http://windowsntlv.files.wordpress.com/2011/08/audit_policy.png)

Дважды щёлкните по политике **Audit object access (Аудит доступа к объектам)** и выберите галочку **Success.** Этот параметр включает механизм слежения за успешным доступом к файлам и реестру. Действительно, ведь нас интересуют только удавшиеся попытки удаления файлов или папок. Включите Аудит только на компьютерах, непосредственно на которых хранятся отслеживаемые объекты.

        Простого включения политики Аудита недостаточно, мы также должны указать, доступ к каким именно папкам требуется отслеживать. Обычно такими объектами являются папки общих (разделяемых) документов и папки с производственными программами или базами данных (бухгалтерия, склад и т.п.) — то есть, ресурсы, с которыми работают несколько человек.

        Заранее угадать, кто именно удалит файл, невозможно, поэтому слежение и указывается за Всеми (Everyone). Удавшиеся попытки удаления отслеживаемых объектов любым пользователем будут заноситься в журнал. Вызовите свойства требуемой папки (если таких папок несколько, то всех их по очереди) и на закладке **Security (Безопасность) → Advanced (Дополнительно) → Auditing (Аудит)** добавьте слежение за субъектом **Everyone (Все),** его успешными попытками доступа **Delete (Удаление)** и **Delete Subfolders and Files (Удаление подкаталогов и файлов):**

[](http://windowsntlv.files.wordpress.com/2011/08/audit_files.png)

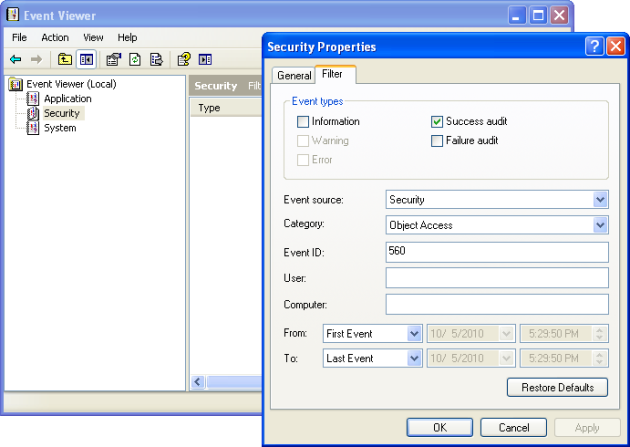
        Событий может журналироваться довольно много, поэтому также следует отрегулировать размер журнала **Security (Безопасность)**, в который они будут записываться. Для  
этого выполните команду **Start → Run → eventvwr.msc.** В появившемся окне вызовите свойства журнала Security и укажите следующие параметры:

* Maximum Log Size = **65536 KB** (для рабочих станций) или **262144 KB** (для серверов)
* Overwrite events as needed.

        На самом деле, указанные цифры не являются гарантированно точными, а подбираются опытным путём для каждого конкретного случая.

 Нажмите **Start → Run → eventvwr.msc** и откройте для просмотра журнал **Security (Безопасность).**Журнал может быть заполнен событиями, прямого отношения к проблеме не имеющими. Щёлкнув правой кнопкой по журналу Security, выберите команду **View → Filter** и отфильтруйте просмотр по следующим критериям:

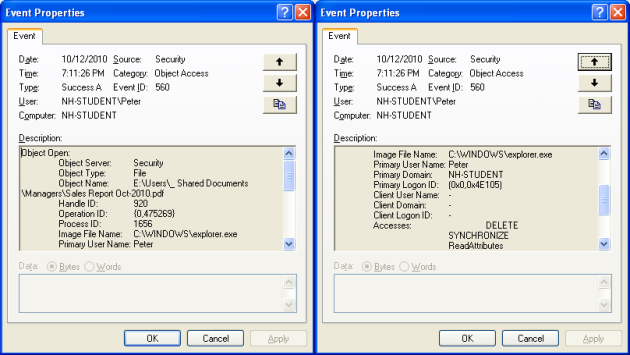
* Event Source:Security;
* Category:         Object Access;
* Event Types:      Success Audit;
* Event ID:         560;

**[](http://windowsntlv.files.wordpress.com/2011/08/audit_events2003.png)**

Просмотрите список отфильтрованных событий, обращая внимание на следующие поля внутри каждой записи:

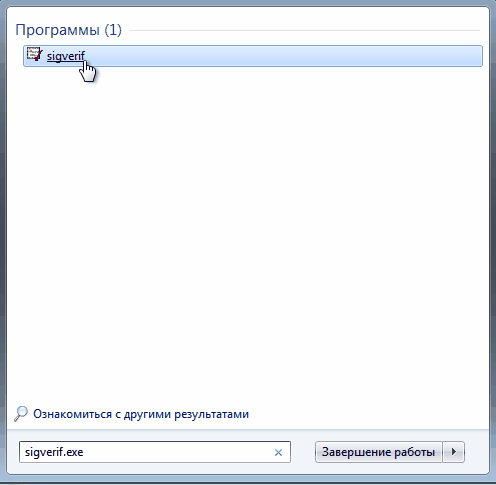
* **Object Name.** Название искомой папки или  файла;
* **Image File Name.** Имя программы, с помощью которой удалили файл;
* **Accesses.** Набор запрашиваемых прав.

Программа может запрашивать у системы сразу несколько типов доступа — например, **Delete+Synchronize**или **Delete+Read\_Control.** Значимым для нас правом является **Delete.**

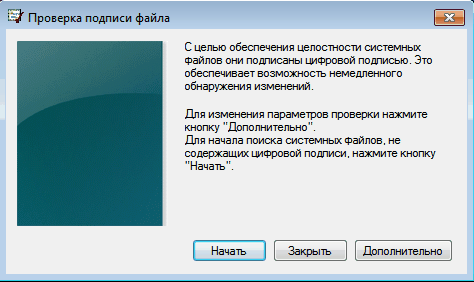
**[](http://windowsntlv.files.wordpress.com/2011/08/audit_details2003.png)**

### Проверка цифровой подписи

В Windows 7 для проверки цифровой подписи есть специальная утилита sigverif.exe. Для ее запуска нужно в поисковой строке меню Пуск набрать sigverif.exe и нажать Ввод

[](https://windowsnotes.ru/wp-content/uploads/2012/02/sig1.gif)

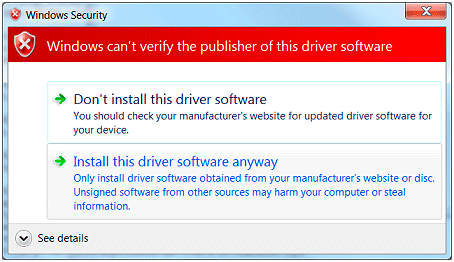
В окне программы жмем начать, и она автоматически проверяет системные файлы на наличие подписей.

[](https://windowsnotes.ru/wp-content/uploads/2012/02/sig2.gif)

Результат проверки сохраняется в текстовый файл sigverif.txt. Хранится он в папке Общие документы, также его можно посмотреть прямо из окна программы, щелкнув по кнопке Дополнительно.

### Отключение проверки цифровой подписи

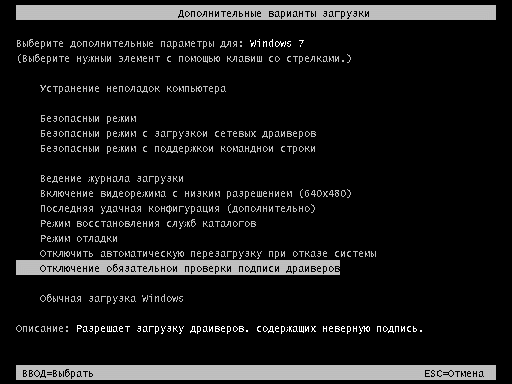
В Windows 7 требования к устанавливаемым драйверам существенно ужесточены, и любой устанавливаемый драйвер должен иметь цифровую подпись, проверенную и сертифицированную Microsoft. Перед загрузкой и установкой драйвера устройства Windows проверит его цифровую подпись, и если драйвер не подписан, выдаст предупреждение

[](https://windowsnotes.ru/wp-content/uploads/2012/02/sig7.gif)

Можно это предупреждение проигнорировать и установить драйвер, однако работать он не будет все равно. При установке неподписанного драйвера в диспетчере устройств данное устройство будет помечено восклицательным знаком и содержать сообщение об ошибке.

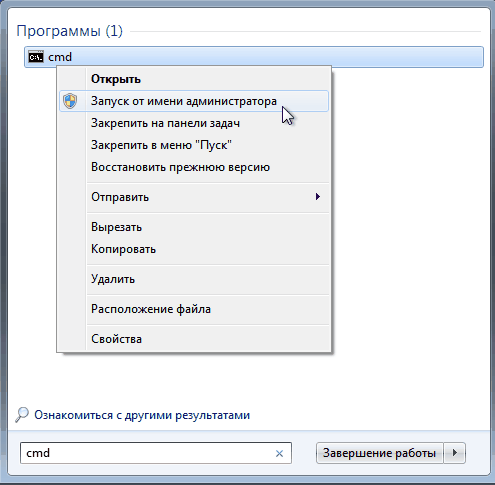
Политика проверки цифровой подписи драйверов призвана улучшить надежность и стабильность операционной системы, но иногда возникает необходимость установить неподписанный драйвер. К счастью, в Windows 7 можно отключить проверку цифровой подписи. Для этого есть несколько способов:

Отключить поверку цифровой подписи драйверов при загрузке через загрузочное меню. Для этого при загрузке ОС жмем клавишу F8. Для загрузки без проверки цифровых подписей нужно выбрать пункт «Отключение обязательной проверки подписи драйверов»

[](https://windowsnotes.ru/wp-content/uploads/2012/02/sig5.gif)

Дальше можно загружаться и устанавливать необходимые драйвера. Однако данный режим предназначен исключительно для тестирования и при следующей загрузке в обычном режиме установленный драйвер работать не будет.

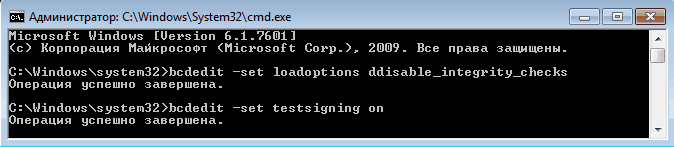
Для постоянной загрузки в тестовом режиме можно воспользоваться утилитой командной строки bcdedit. Для этого открываем командную строку с правами администратора

[](https://windowsnotes.ru/wp-content/uploads/2012/02/sig8.gif)

И последовательно вводим 2 команды:

bcdedit -set loadoptions DDISABLED\_INTEGRITY\_CHECKS

bcdedit  -set TESTSIGNING ON

[](https://windowsnotes.ru/wp-content/uploads/2012/02/sig9.gif)

После выполнения каждой команды должно появиться сообщение об успешном выполнении.  Теперь можно перезагрузить компьютер и установить необходимые драйвера.

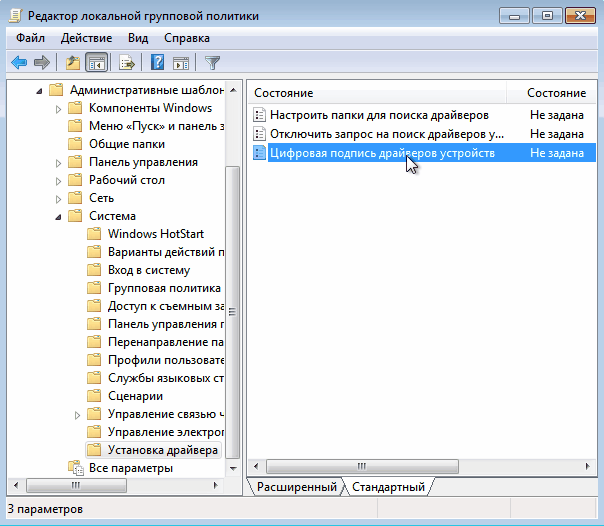
Для отключения тестового режима нужно ввести в командной строке команды:

bcdedit -set loadoptions ENABLE\_INTEGRITY\_CHECKS

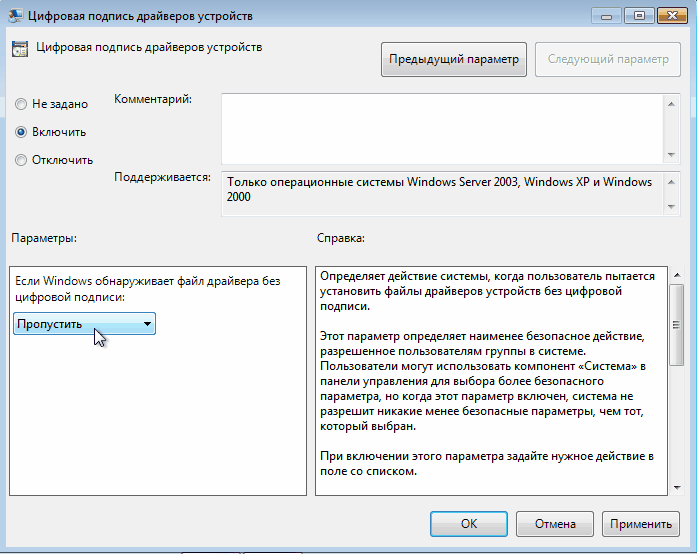
bsdedit -set loadoptions TESTSIGNING ON

**Важно**: если выдается сообщение о том, что команда неизвестна, то вместо дефиса (-) ключи можно писать через слеш (/).

Ну и наконец можно просто отключить проверку цифровых подписей драйверов через групповую политику. Для запуска оснастки групповой политики вводим в меню Пуск в строке поиска команду gpedit.msc и жмем Ввод. В меню политик идем в Конфигурация пользователя\Административные шаблоны\Система\Установка драйверов и выбираем политику «Цифровая подпись драйверов устройств».

[](https://windowsnotes.ru/wp-content/uploads/2012/02/sig10.gif)

В появившемся окне включаем политику и указываем параметр пропустить в качестве действия системы при обнаружении неподписанных драйверов.

[](https://windowsnotes.ru/wp-content/uploads/2012/02/sig11.gif)

После перезагрузки политика применится и можно будет загружать и устанавливать любые, в том числе и неподписанные драйвера