Лабораторная работа № 2.

Управление политикой безопасности в операционной системе Windows

Подготовительные определения понятий

Политика безопасности организации – совокупность документированных руководящих принципов, правил, процедур и практических приёмов в области безопасности, которые регулируют управление, защиту и распределение ценной информации

Аудит – процесс, позволяющий фиксировать события, происходящие в операционной системе и имеющие отношение к безопасности

Журнал аудита – запись в хронологическом порядке действий системы, содержащей достаточно сведений для того, чтобы реконструировать, проанализировать и проверить последовательность сред и действий, окружающих каждое событие или ведущих к каждому событию по ходу операции от ее начала до выдачи окончательных результатов

Цифровая подпись – последовательность символов, полученная в результате криптографического преобразования электронных данных. ЭЦП добавляется к блоку данных и позволяет получателю блока проверить источник и целостность данных и защититься от подделки

Подготовительные вопросы

1. Какие события безопасности должны фиксироваться в журнале аудита?
   1. Вход в систему
   2. Управление учетной записью
   3. Доступ к службе каталогов
   4. Доступ к объектам
   5. Изменения политики
   6. Использования привилегий
   7. Отслеживание процессов
   8. Системных событий
2. Какие параметры определяют политику аудита?
   1. Аудит вход в систему
   2. Аудит управление учетной записью
   3. Аудит доступ к службе каталогов
   4. Аудит доступ к объектам
   5. Аудит изменения политики
   6. Аудит использования привилегий
   7. Аудит отслеживание процессов
   8. Аудит системных событий
3. Целесообразно ли с точки зрения безопасности компьютерной системы разрешать анонимный доступ к ее информационным ресурсам?

Нет, в таком случае любой человек сможет получить данныеск этой компьютерной системы.

1. Как должен передаваться по сети (с точки зрения безопасности компьютерной системы) пароль пользователя?

В зашифрованном виде

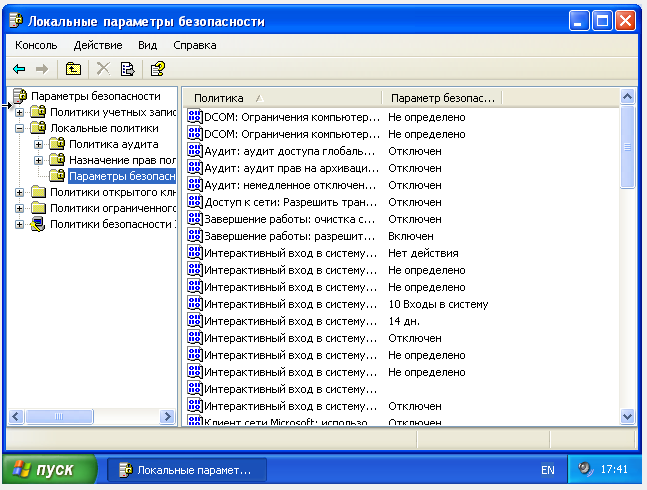
1. Нужно ли ограничивать права пользователей по запуску прикладных программ?

Да, как минимум, чтобы ограничить использование компьютера неопытным пользователем.

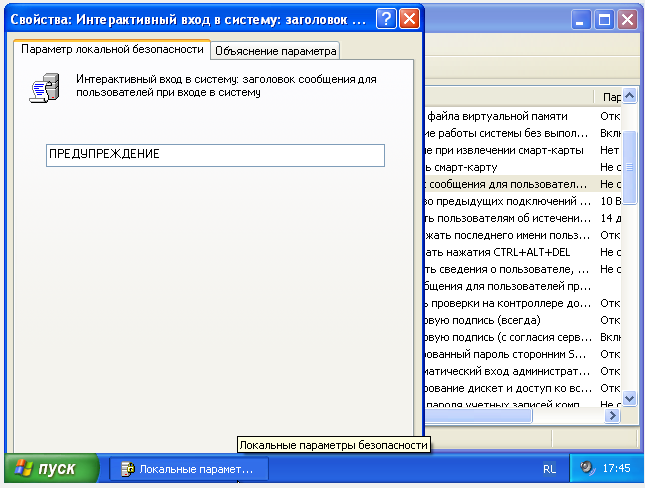
Выполнение работы

Освоить средства определения политики безопасности:

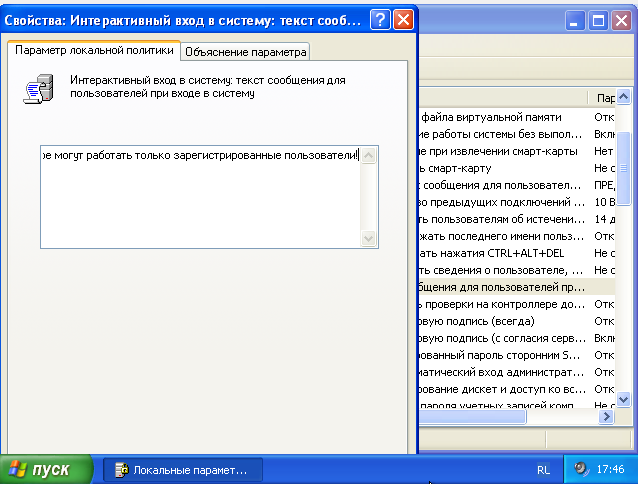
• открыть окно определения параметров политики безопасности (Панель управления | Администрирование | Локальная политика безопасности | Локальные политики | Параметры безопасности);



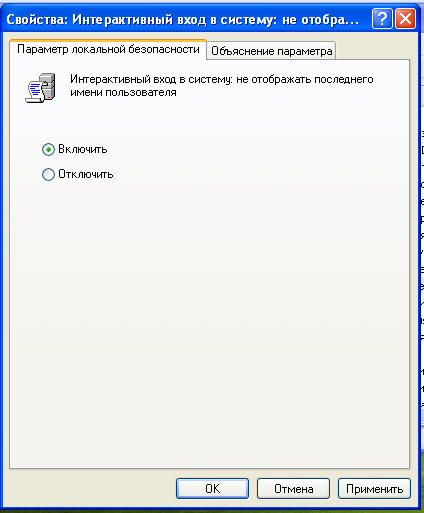
• установить заголовок «ПРЕДУПРЕЖДЕНИЕ» в качестве значения параметра «Интерактивный вход в систему: заголовок сообщения для пользователей при входе в систему»;



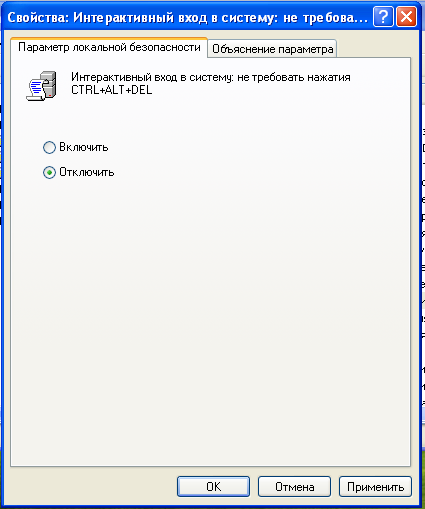
• установить текст «На этом компьютере могут работать только зарегистрированные пользователи!» в качестве значения параметра «Интерактивный вход в систему: текст сообщения для пользователей при входе в систему»;



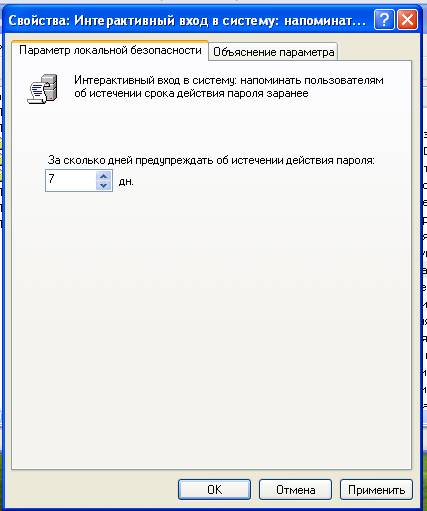
• установить значение «Включен» для параметра «Интерактивный вход в систему: не отображать последнего имени пользователя»;



• установить значение «Отключен» для параметра «Интерактивный вход в систему: не требовать нажатия CTRL+ALT+DEL»;



• установить значение «7 дней» для параметра «Интерактивный вход в систему: напоминать пользователям об истечении срока действия пароля заранее»;



• включить в отчет о лабораторной работе сведения о порядке назначения параметров политики безопасности, относящихся к интерактивному входу, и ответ на вопрос о смысле этих параметров;

1. Интерактивный вход в систему: поведение при извлечении смарт-карты.  
   Этот параметр безопасности определяет, что происходит при извлечении смарт-карты пользователя, вошедшего в систему, из устройства чтения смарт-карт.

Возможны следующие варианты:

* Нет действия
* Блокировка рабочей станции
* Принудительный выход из системы
* Отключение в случае удаленного сеанса служб терминалов

Если в диалоговом окне "Свойства" данной политики выбрать вариант "Блокировка рабочей станции", станция при извлечении смарт-карты будет заблокирована; таким образом, пользователь может уйти с рабочего места, взяв с собой смарт-карту, - доступ к его сеансу останется под защитой.

Если в диалоговом окне "Свойства" этой политики выбрать вариант "Принудительный выход из системы", при извлечении смарт-карты произойдет автоматическое завершение сеанса работы пользователя.

Если выбрать вариант "Отключение в случае удаленного сеанса служб терминалов", при извлечении смарт-карты произойдет отключение сеанса без выхода пользователя из системы. Это позволяет пользователю позже вставить смарт-карту и восстановить сеанс или использовать другой терминал, оборудованный устройством чтения смарт-карт, без необходимости повторного выполнения входа.

По умолчанию: нет действия.

1. Интерактивный вход в систему: заголовок сообщения для пользователей при входе в систему  
   Этот параметр безопасности позволяет указать заголовок окна, содержащего сообщение, указанное в параметре "Интерактивный вход: текст сообщения для пользователей при входе в систему".

По умолчанию: сообщение отсутствует.

1. Интерактивный вход в систему: количество предыдущих подключений к кэшу (в случае отсутствия доступа к контроллеру домена)  
   Сведения о предыдущих входах пользователей в систему кэшируются локально, чтобы обеспечить последующий вход в систему в случае отсутствия доступа к контроллеру домена. При отсутствии доступа к контроллеру домена и кэшировании сведений о входах пользователей в систему пользователь получает следующее сообщение:

“Не удалось установить связь с сервером и получить параметры входа в систему. Вход выполнен с помощью локально сохраненной информации об учетной записи. Если эта информация была изменена со времени последнего входа в систему на этом компьютере, то изменения не будут отражены во время текущего сеанса.”

При отсутствии доступа к контроллеру домена и отсутствии кэширования данных о входах пользователей в систему пользователь получает следующее сообщение:

“Подключение к системе сейчас невозможно, так как домен <ИМЯ\_ДОМЕНА> недоступен.”

Значение этого параметра "0" отключает кэширование данных входа. При любом значении большем 50 кэшируется только 50 попыток входа в систему.

По умолчанию: 10

1. Интерактивный вход в систему: напоминать пользователям об истечении срока действия пароля заранее  
   Определяет, за сколько дней до истечения срока действия пароля следует предупреждать об этом пользователей. Если пользователя заблаговременно предупредить, он успеет подготовить новый достаточно надежный пароль.

По умолчанию: 14 дней.

1. Интерактивный вход в систему: не отображать последнее имя пользователя  
   Этот параметр безопасности определяет, будет ли на экране входа в систему показано имя последнего пользователя, выполнившего вход.

Если этот параметр включен, в диалоговом окне входа в Windows не будет отображаться имя последнего пользователя, выполнившего вход.

Если этот параметр отключен, будет показано имя последнего пользователя, выполнившего вход.

По умолчанию: "Отключен".

1. Интерактивный вход в систему: не требовать нажатия CTRL+ALT+DEL  
   Этот параметр безопасности определяет, должен ли пользователь, прежде чем войти в систему, нажать клавиши CTRL+ALT+DEL.

Если эта политика включена на компьютере, пользователь не должен для входа в систему нажимать CTRL+ALT+DEL. В таком случае компьютер становится уязвимым для атак, основанных на перехвате паролей пользователей. Если потребовать нажатия клавиш CTRL+ALT+DEL перед входом в систему, то пользователям будет гарантирован надежно защищенный канал передачи паролей.

Если эта политика отключена, то любой пользователь должен будет перед входом в Windows нажимать CTRL+ALT+DEL (если только он не входит в систему с помощью смарт-карты).

По умолчанию:

Выключен на рабочих станциях и серверах домена.

Включен на автономных рабочих станциях.

1. Интерактивный вход в систему: отображать сведения о пользователе, если сеанс заблокирован  
   Этот параметр безопасности определяет, будут ли отображаться такие сведения, как адрес электронной почты или домен \ имя пользователя, на экране входа в систему.

Настройка конфиденциальности по умолчанию отключена, что скрывает сведения.

1. Интерактивный вход в систему: текст сообщения для пользователей при входе в систему  
   Этот параметр безопасности задает текстовое сообщение, показываемое пользователям при входе в систему.

В такие сообщения часто включаются сведения юридического характера, например предупреждения о последствиях неправомерного использования корпоративных данных или о возможном аудите выполняемых пользователями действий.

По умолчанию: сообщение отсутствует.

1. Интерактивный вход в систему: требовать проверки на контроллере домена для отмены блокировки  
   Для снятия блокировки с компьютера необходимо предоставить сведения, используемые при входе в систему. Для учетных записей домена данный параметр безопасности определяет, нужно ли для снятия блокировки обращаться на контроллер домена. Если этот параметр отключен, пользователь может разблокировать компьютер, используя учетные данные из кэша. Если параметр включен, контроллер домена должен проверить подлинность учетной записи домена, используемой для снятия блокировки с компьютера.

По умолчанию: "Отключен".

1. Интерактивный вход в систему: требовать смарт-карту  
   Этот параметр безопасности требует использования смарт-карты для входа пользователя на компьютер.

Возможны следующие варианты:

* Включен. Пользователи могут войти на компьютер только с использованием смарт-карт.
* Отключен. Пользователи могут войти на компьютер, используя любой метод.

По умолчанию: "Отключен".

• с помощью раздела Справки Windows «Параметры безопасности» включить в отчет о лабораторной работе пояснения отдельных параметров локальной политики безопасности компьютерной системы и их возможных значений (в соответствии с номером варианта и приложением). Вариант 10

**Системные объекты: усилить разрешения по умолчанию для внутренних системных объектов (например, символических ссылок)**

Определяет уровень строгости стандартной избирательной таблицы управления доступом (DACL) для объектов.

Служба Active Directory ведет глобальный список общих системных ресурсов, таких как имена устройств DOS, мьютексы и семафоры. Благодаря этому можно отыскивать нужные объекты и предоставлять их в общий доступ различным процессам. При создании объекта создается стандартная таблица DACL, соответствующая данному типу объектов; в ней указано, кто имеет доступ к объекту и какие предоставляются разрешения.

Если данная политика включена, стандартная таблица DACL становится более строгой: пользователям, не являющимся администраторами, разрешается читать содержимое общих объектов, но запрещается изменять общие объекты, созданные другими пользователями.

**Сетевой доступ: разрешить применение разрешений для всех к анонимным пользователям**

Определяет, может ли анонимный пользователь запрашивать атрибуты идентификатора безопасности (SID) другого пользователя.

Если эта политика включена, пользователь, зная идентификатор безопасности администратора, может связаться с компьютером, на котором действует данная политика, и получить имя администратора по этому идентификатору.

По умолчанию: отключен на рабочих станциях; включен на серверах.

**Сетевой доступ: разрешать анонимный доступ к именованным каналам**

Определяет, каким сеансам связи (каналам) будут назначаться атрибуты и разрешения, допускающие анонимный доступ.

По умолчанию нет.

**Интерактивный вход в систему: количество предыдущих подключений к кэшу (в случае отсутствия доступа к контроллеру домена)**

Определяет, сколько раз пользователь может войти в домен Windows, используя учетные данные из кэша.

Сведения из учетных записей домена, используемые при входе в систему, могут помещаться в локальный кэш, чтобы в случае, если при очередной попытке входа связаться с контроллером домена не удастся, пользователь все равно мог бы войти в систему. Данный параметр задает число уникальных пользователей, для которых сведения, необходимые для входа в систему, заносятся в локальный кэш.

Если контроллер домена недоступен и учетные данные пользователя содержатся в кэше, пользователь получает следующее сообщение:

Не удалось подключиться к контроллеру вашего домена. Вход выполнен с использованием учетных данных, сохраненных в кэше. Изменения в профиле, внесенные с момента последнего входа в систему, могут быть недоступны.

Если контроллер домена недоступен и учетных данных пользователя в кэше нет, пользователь получает следующее сообщение:

Не удалось выполнить вход в систему, поскольку домен <ИМЯ\_ДОМЕНА> недоступен.

По умолчанию 10.

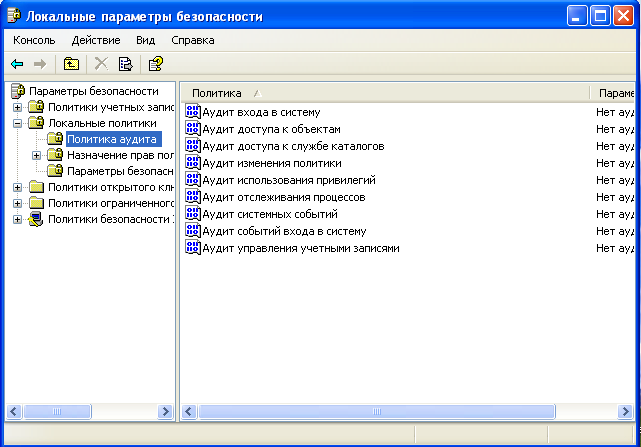
**Интерактивный вход в систему: требовать проверки на контроллере домена для отмены блокировки**

Для снятия блокировки с компьютера необходимо предоставить сведения, используемые при входе в систему. Для учетных записей домена данный параметр определяет, нужно ли для снятия блокировки обращаться на контроллер домена. Если этот параметр отключен, пользователь может разблокировать компьютер, используя учетные данные из кэша. Если параметр включен, контроллер домена должен проверить подлинность учетной записи домена, используемой для снятия блокировки с компьютера.

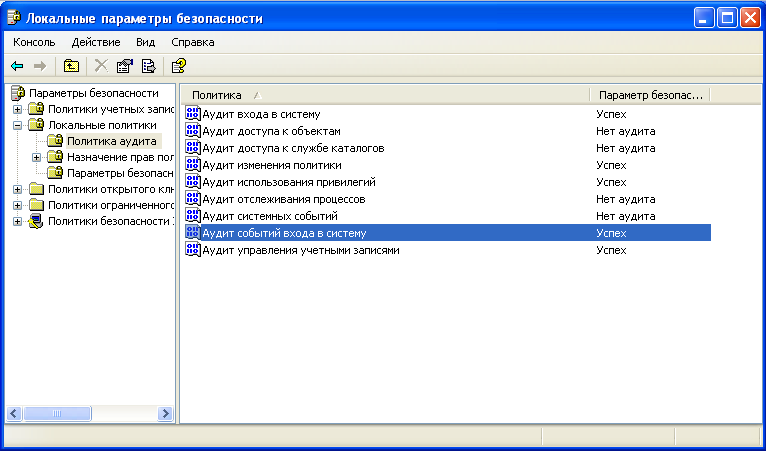
По умолчанию отключен.

Освоить средства определение политики аудита:

• открыть окно определения параметров политики аудита (Панель управления | Администрирование | Локальная политика безопасности | Локальные политики | Политика аудита);



• с помощью параметров политики аудита установить регистрацию в журнале аудита успешных и неудачных попыток: входа в систему; изменения политики; использования привилегий; событий входа в систему; управления учетными записями;



• открыть окно просмотра журнала аудита событий безопасности (Панель управления | Администрирование | Просмотр событий | Безопасность), выполнить команду «Свойства» контекстного меню (или команду Действие | Свойства) и включить в отчет о лабораторной работе ответы на вопросы:

• какие еще параметры политики аудита могут быть изменены;

1. Аудит входа в систему  
   Этот параметр безопасности определяет, подлежит ли аудиту каждая попытка пользователя войти в систему с компьютера или выйти из нее. События входа в систему формируются контроллерами домена в процессе проверки учетных записей домена и локальными компьютерами при работе с локальными учетными записями. Если включены обе категории политик - учетных записей и аудита при входе в систему, - входы в систему с использованием учетной записи домена формируют событие входа или выхода на рабочей станции или сервере и событие входа в систему на контроллере домена. Кроме того, интерактивные входы на рядовой сервер или рабочую станцию с использованием учетной записи домена формируют событие входа на контроллере домена, в то время как при входе пользователя производится поиск сценариев входа и политик. Дополнительные сведения о событиях входа в систему см. в разделе "Аудит событий входа в систему".

Если этот параметр политики определен, можно задать аудит успехов или отказов либо вообще отключить аудит событий данного типа. Аудит успехов означает создание записи аудита для каждой успешной попытки входа в систему. Аудит отказов означает создание записи аудита для каждой неудачной попытки входа.

Чтобы установить значение "Нет аудита", в диалоговом окне "Свойства" данного параметра политики установите флажок "Определить следующие параметры политики" и снимите флажки "Успех" и "Отказ".

По умолчанию: "Успех".

1. Аудит доступа к объектам  
   Этот параметр безопасности определяет, подлежит ли аудиту событие доступа пользователя к объекту - например к файлу, папке, разделу реестра, принтеру и т. п., - для которого задана собственная системная таблица управления доступом (SACL).

Если этот параметр политики определен, можно задать аудит успехов или отказов либо вообще отключить аудит событий данного типа. Аудит успехов означает создание записи аудита при каждом успешном доступе пользователя к объекту, для которого определена соответствующая таблица SACL. Аудит отказов означает создание записи аудита при каждой неудачной попытке доступа пользователя к объекту, для которого определена таблица SACL.

Чтобы установить значение "Нет аудита", в диалоговом окне "Свойства" данного параметра политики установите флажок "Определить следующие параметры политики" и снимите флажки "Успех" и "Отказ".

Следует отметить, что системную таблицу управления доступом для объекта файловой системы можно установить на вкладке "Безопасность" диалогового окна "Свойства" этого объекта.

По умолчанию: "Нет аудита".

1. Аудит доступа к службе каталогов  
   Этот параметр безопасности определяет, подлежит ли аудиту событие доступа пользователя к объекту каталога Active Directory, для которого задана собственная системная таблица управления доступом (SACL).

По умолчанию эта политика отменяет аудит для объекта групповой политики "Стандартный контроллер домена" и не определена для рабочих станций и серверов, на которых она не имеет смысла.

Если этот параметр политики определен, можно задать аудит успехов или отказов либо вообще отключить аудит событий данного типа. Аудит успехов означает создание записи аудита при каждом успешном доступе пользователя к объекту Active Directory, для которого определена таблица SACL. Аудит отказов означает создание записи аудита при каждой неудачной попытке доступа пользователя к объекту Active Directory, для которого определена таблица SACL. Чтобы установить значение "Нет аудита", в диалоговом окне "Свойства" данного параметра политики установите флажок "Определить следующие параметры политики" и снимите флажки "Успех" и "Отказ".

Следует отметить, что системную таблицу управления доступом для объекта Active Directory можно установить на вкладке "Безопасность" диалогового окна "Свойства" этого объекта. Данная политика аналогична политике "Аудит доступа к объектам", только она применяется к объектам Active Directory, а не к объектам файловой системы и реестра.

По умолчанию:

"Успех" - на контроллерах домена.

Не определен для рядового компьютера домена.

1. Аудит изменения политики  
   Этот параметр безопасности определяет, подлежит ли аудиту каждый факт изменения политик назначения прав пользователей, политик аудита или политик доверительных отношений.

Если этот параметр политики определен, можно задать аудит успехов или отказов либо вообще отключить аудит событий данного типа. Аудит успехов означает создание записи аудита при каждом успешном изменении политик назначения прав пользователей, политик аудита или политик доверительных отношений. Аудит отказов означает создание записи аудита при каждой неудачной попытке изменения политик назначения прав пользователей, политик аудита или политик доверительных отношений.

Чтобы установить значение "Нет аудита", в диалоговом окне "Свойства" данного параметра политики установите флажок "Определить следующие параметры политики" и снимите флажки "Успех" и "Отказ".

По умолчанию:

"Успех" - на контроллерах домена.

"Нет аудита" - на рядовых серверах.

1. Аудит использования привилегий  
   Этот параметр безопасности определяет, подлежит ли аудиту каждая попытка пользователя воспользоваться предоставленным ему правом.

Если этот параметр политики определен, можно задать аудит успехов или отказов либо вообще отключить аудит событий данного типа. Аудит успехов означает создание записи аудита для каждого успешного применения права пользователя. Аудит отказов означает создание записи аудита для каждого неудачного применения права пользователя.

Чтобы установить значение "Нет аудита", в диалоговом окне "Свойства" данного параметра политики установите флажок "Определить следующие параметры политики" и снимите флажки "Успех" и "Отказ".

По умолчанию: "Нет аудита".

1. Аудит отслеживания процессов  
   Этот параметр безопасности определяет, подлежат ли аудиту такие события, как активизация программы, завершение процесса, повторение дескрипторов и косвенный доступ к объекту.

Если этот параметр политики определен, можно задать аудит успехов или отказов либо вообще отключить аудит событий данного типа. Аудит успехов означает создание записи аудита для каждого успешного события, связанного с отслеживаемым процессом. Аудит отказов означает создание записи аудита для каждого неудачного события, связанного с отслеживаемым процессом.

Чтобы установить значение "Нет аудита", в диалоговом окне "Свойства" данного параметра политики установите флажок "Определить следующие параметры политики" и снимите флажки "Успех" и "Отказ".

По умолчанию: "Нет аудита".

1. Аудит системных событий  
   Этот параметр безопасности определяет, подлежат ли аудиту события перезагрузки или отключения компьютера, а также события, влияющие на системную безопасность или на журнал безопасности.

Если этот параметр политики определен, можно задать аудит успехов или отказов либо вообще отключить аудит событий данного типа. Аудит успехов означает создание записи аудита для каждого успешного системного события. Аудит отказов означает создание записи аудита для каждого неудачного завершения системного события.

Чтобы установить значение "Нет аудита", в диалоговом окне "Свойства" данного параметра политики установите флажок "Определить следующие параметры политики" и снимите флажки "Успех" и "Отказ".

По умолчанию:

"Успех" - на контроллерах домена. "Нет аудита" - на рядовых серверах.

1. Аудит событий входа в систему  
   Этот параметр безопасности определяет, подлежит ли аудиту каждая попытка пользователя войти в систему с другого компьютера или выйти из нее, при условии что этот компьютер используется для проверки подлинности учетной записи. События входа в систему формируются при проверке подлинности учетной записи пользователя домена, выполняемой контроллером домена. Событие регистрируется в журнале безопасности контроллера домена. Событие входа в систему создается при проверке подлинности локального пользователя на локальном компьютере. Событие регистрируется в локальном журнале безопасности. События выхода из системы не формируются.

Если этот параметр политики определен, можно задать аудит успехов или отказов либо вообще отключить аудит событий данного типа. Аудит успехов означает создание записи аудита для каждой успешной попытки входа в систему. Аудит отказов означает создание записи аудита для каждой неудачной попытки входа в систему.

Чтобы установить значение "Нет аудита", в диалоговом окне "Свойства" данного параметра политики установите флажок "Определить следующие параметры политики" и снимите флажки "Успех" и "Отказ".

Если аудит успешных попыток входа в систему включен на контроллере домена, в журнал будет заноситься запись о каждом пользователе, прошедшем проверку на этом контроллере домена, несмотря на то, что пользователь на самом деле входит в систему на рабочей станции домена. По умолчанию: "Успех".

1. Аудит управления учетными записями  
   Этот параметр безопасности определяет, подлежат ли аудиту все события, связанные с управлением учетными записями на компьютере. К таким событиям относятся, в частности, следующие:

* создание, изменение или удаление учетной записи пользователя или группы;
* переименование, отключение или включение учетной записи пользователя;
* задание или изменение пароля.

Если этот параметр политики определен, можно задать аудит успехов или отказов либо вообще отключить аудит событий данного типа. Аудит успехов означает создание записи аудита для каждого успешного события управления учетными записями. Аудит отказов означает создание записи аудита для каждого неудачного события управления учетными записями.

Чтобы установить значение "Нет аудита", в диалоговом окне "Свойства" данного параметра политики установите флажок "Определить следующие параметры политики" и снимите флажки "Успех" и "Отказ".

По умолчанию:

"Успех" - на контроллерах домена.

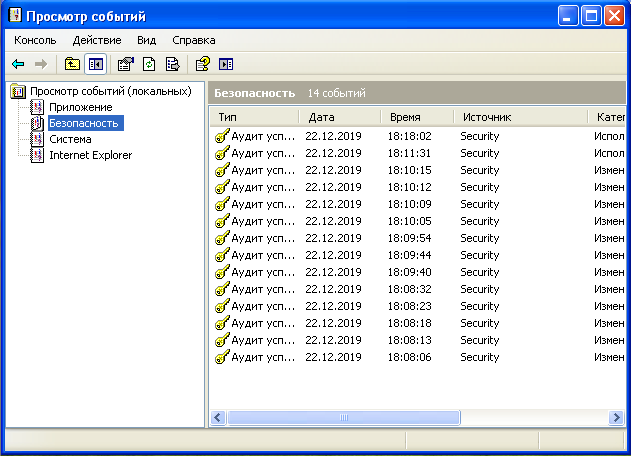
"Нет аудита" - на рядовых серверах.

• где расположен журнал аудита событий безопасности;

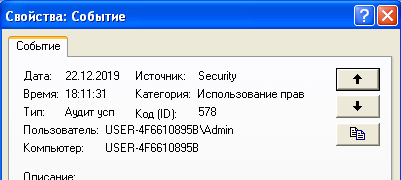
C:\WINDOWS\System32\config\SecEvent.Evt

Освоить средства просмотра журнала аудита событий безопасности:

• открыть окно просмотра журнала аудита событий безопасности (Панель управления | Просмотр событий | Безопасность);



• включить в отчет о лабораторной работе копии экранных форм с краткой и полной информацией о просматриваемом событии безопасности;



• с помощью буфера обмена Windows и соответствующей кнопки в окне свойств события включить в отчет о лабораторной работе полную информацию о нескольких событиях безопасности.

1. Изменение политики аудита:

Новая политика:

Успех Отказ

+ + Вход/выход

- - Доступ к объектам

+ + Использование прав

+ + Управление учетными записями

+ + Изменение политики

- - Системные события

- - Подробное слежение

- - Доступ к службе каталогов

+ + Вход через учетную запись

Исполнитель:

Пользователь: Admin

Имя домена: USER-4F6610895B

Код входа: (0x0,0x9D23)

1. Изменение политики аудита:

Новая политика:

Успех Отказ

+ + Вход/выход

- - Доступ к объектам

+ + Использование прав

+ - Управление учетными записями

+ + Изменение политики

- - Системные события

- - Подробное слежение

- - Доступ к службе каталогов

+ + Вход через учетную запись

Исполнитель:

Пользователь: Admin

Имя домена: USER-4F6610895B

1. Изменение политики аудита:

Новая политика:

Успех Отказ

+ + Вход/выход

- - Доступ к объектам

+ + Использование прав

+ - Управление учетными записями

+ + Изменение политики

- - Системные события

- - Подробное слежение

- - Доступ к службе каталогов

+ - Вход через учетную запись

1. Изменение политики аудита:

Новая политика:

Успех Отказ

+ + Вход/выход

- - Доступ к объектам

+ - Использование прав

+ - Управление учетными записями

+ + Изменение политики

- - Системные события

- - Подробное слежение

- - Доступ к службе каталогов

+ - Вход через учетную запись

Исполнитель:

Пользователь: Admin

Имя домена: USER-4F6610895B

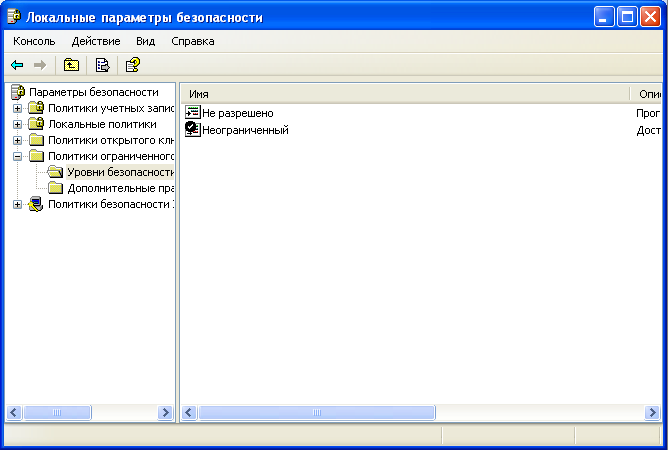
Исполнитель:

Пользователь: Admin

Имя домена: USER-4F6610895B

Освоить средства определения политики ограниченного использования программ:

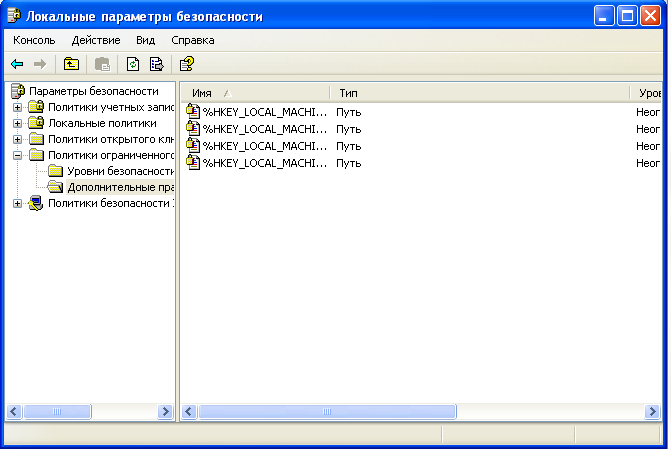
• открыть окно определения уровней безопасности политики ограниченного использования программ (Панель управления | Администрирование | Локальная политика безопасности | Политики ограниченного использования программ | Уровни безопасности);



• включить в отчет о лабораторной работе пояснения к возможным уровням безопасности при запуске программ и копии соответствующих экранных форм;

* Уровень безопасности “Не разрешено”. Программное обеспечение запускаться не будет, вне зависимости от прав доступа пользователя.
* Уровень безопасности “Неограниченный”. Доступ программ к ресурсам определяется правами пользователя.

• открыть окно определения дополнительных правил политики ограниченного использования программ (Панель управления | Администрирование | Локальная политика безопасности | Политики ограниченного использования программ | Дополнительные правила);



• включить в отчет о лабораторной работе ответы на вопросы, какие дополнительные правила для работы с программами могут быть определены (с помощью команд контекстного меню или меню «Действие») и в чем их смысл, а также копии соответствующих экранных форм.

Можно создать правила:

1. Правила для сертификатов.

Политики ограниченного использования программ могут также обнаруживать программное обеспечение по его сертификату подписи. Можно создать правило для сертификата, которое определяет программу, а потом разрешает или запрещает ее запуск в зависимости от уровня безопасности. Например, с помощью правил для сертификатов можно автоматически считать доверенным программное обеспечение из доверенного источника в домене, не запрашивая пользователя. С помощью правил для сертификатов также можно запускать файлы в запрещенных областях операционной системы. По умолчанию правила для сертификатов не включены.

При создании правил для домена с помощью групповая политика необходимо иметь разрешения на создание или изменение объекта групповая политика. При создании правил для локального компьютера необходимы административные учетные данные на этом компьютере.

1. Правило для хеша.   
   Когда для программы создается правило хэширования, политики ограниченного использования программ вычисляют хэш программы. Когда пользователь пытается открыть программу, ее хэш сравнивается с существующими правилами хэширования для политик ограниченного использования программ. Хэш программы остается неизменным независимо от ее расположения на компьютере. Однако если программа каким-либо образом меняется, то ее хэш также меняется и перестает совпадать с хэшем в правиле хэширования для политик ограниченного использования программ.
2. Правило для зоны интернета.   
   Правила для зон Интернета применяются только к пакетам установщика Windows. Правило для зоны может определять программу из зоны, заданной в Internet Explorer. Это зоны "Интернет", "Локальная интрасеть", "Опасные сайты", "Надежные сайты" и "Мой компьютер". Правило зоны Интернета предназначено для предотвращения загрузки и установки программного обеспечения пользователями.
3. Правило для пути.   
   Правило для пути определяет программу по пути к ее файлу. Например, даже если для компьютера задан уровень безопасности по умолчанию Запрещено, можно предоставить каждому пользователю неограниченный доступ к определенной папке. Можно создать правило для пути с помощью пути к файлу и задать в правиле для пути уровень безопасности Не ограничено. Для этого типа правила часто используются пути %userprofile%, %windir%, %appdata%, %programfiles% и %temp%. Также можно создавать правила для пути в реестре, где путем служит раздел реестра для программы.

Контрольные вопросы

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.

1. 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.

1. Из каких этапов состоит построение политики безопасности для компьютерной системы?
   1. Определение, какие данные и насколько серьезно необходимо защищать.
   2. Определение, кто и какой ущерб может нанести фирме в информационном аспекте.
   3. Вычисление рисков и определение схемы уменьшения их до приемлемой величины.
2. К чему может привести ошибочное определение политики безопасности?

К утечке, потере или повреждению данных .