Лабораторная работа 13. Аудит событий безопасности операционной системы

Цель лабораторной работы: ознакомление с интерфейсом управления подсистемой аудита безопасности и параметрами политики аудита на примере операционной системы Windows.

Задачи лабораторной работы:
1. Политика аудита
2. Аудит входа/выхода пользователей
3. Аудит событий, связанных с администрированием
4. Аудит событий, связанных с работой операционной системы
5. Аудит доступа пользователей к ресурсам
6. Управление журналом аудита

Задание
Контрольные вопросы

Содержание лабораторной работы:

1. Политика аудита

Политика аудита определяет, какие категории сообщений о событиях отслеживаются и сохраняются в журнале безопасности. Настройка политики происходит при помощи оснастки «Локальная политика безопасности».

Войдите в операционную систему под учётной записью «Администратор». Откройте оснастку «Локальная политика безопасности» («Пуск - Панель управления - Администрирование»). Выберите раздел «Локальные политики - Политика аудита» (рис. 1).

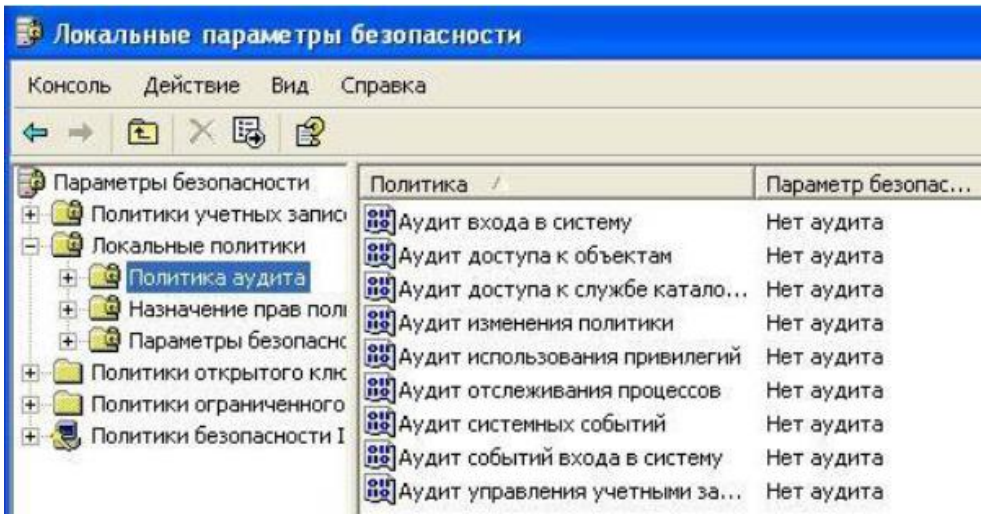

Рис. 1 - Политика аудита Windows XP

В политике аудита представлен набор параметров, соответствующих различным категориям событий безопасности. В «Свойствах» каждого из параметров возможно включение фиксации событий, относящихся к соответствующей категории. Откройте параметр политики аудита «Аудит входа в систему» (рис.2). Включение аудита происходит по следующим типам событий:

- *«Успех» - фиксируются события, осуществление которых было разрешено пользователю;*

- *«Отказ» - фиксируются события, осуществление которых было запрещено пользователю.*

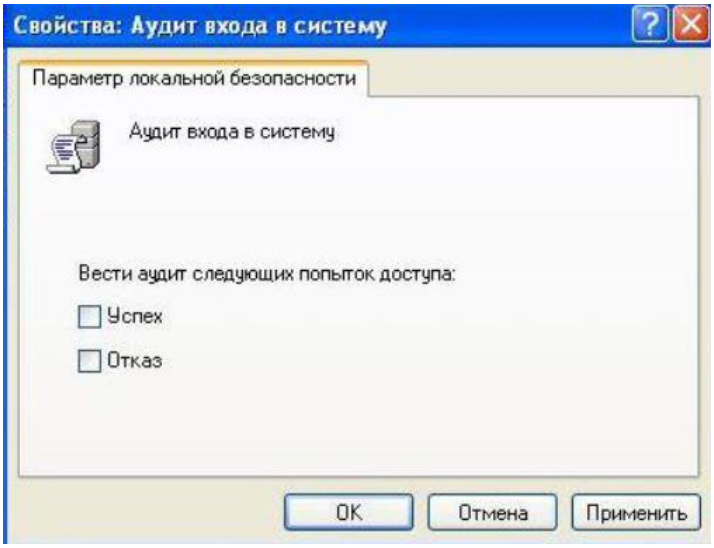

Рис. 2 - Настройки параметра «Аудит входа в систему»

2. Аудит входа/выхода пользователей

Параметр «Аудит входа в систему» включает фиксацию каждой попытки входа пользователя в систему или выхода из неё на данном компьютере. Включите оба типа событий («Успех» и «Отказ») для параметра «Аудит входа в систему».

Включите оба типа событий («Успех» и «Отказ») для параметра «Аудит событий входа в систему». Параметр «Аудит событий входа в систему» включает фиксацию каждой проверки данным компьютером учётных данных (в т.ч. контроллером домена при входе в домен на рабочей станции).

Завершите сеанс текущего пользователя. Введите неверный пароль при входе в операционную систему, чтобы сгенерировать событие типа «Отказ».

Войдите под учётной записью «Администратор». Откройте журнал «Безопасность» оснастки «Просмотр событий» (рис. 3).

Рис. 3 - Журнал «Безопасность»

Записи журнала «Безопасность» включают в себя следующую информацию о событии: время и дата события; имя учётной записи пользователя, сгенерировавшего событие; имя компьютера, на котором произошло событие; категорию и тип события; код события; дополнительную информацию в зависимости от категории события.

В журнале «Безопасность» откройте запись категории «Вход/выход» типа «Аудит отказов». Данная запись описывает событие, сгенерированное при вводе неправильного пароля (рис. 4). Так как пользователь ещё не прошёл аутентификацию, событие было сгенерировано от имени пользователя «System». В записи о событии указывается имя пользователя, использовавшееся при осуществлении неудачной попытки входа в систему, и тип входа. Код данного события - 529.

Рис. 4 - Запись аудита об отказе входа в операционную систему

Откройте запись категории «Вход/выход» типа «Аудит успехов» с кодом 528. Данная запись описывает событие, сгенерированное при удачном входе в операционную систему (рис. 5).

В обеих записях (аудита успехов и отказов) указан тип входа в систему - 2. Этот тип означает интерактивный вход в систему. Типы входа в систему, фиксируемые в Windows XP, приведены в табл. 1.

Рис. 5 - Запись аудита об успешном входе в операционную систему

Таблица 1. Описание типов входа в систему

Тип входа	***Название типа входа***	***Описание***
2	Интерактивный	Локальный вход пользователя на компьютер.
3	Сеть	Пользователь вошёл на данный компьютер через сеть.
4	Пакетный	Пакетный тип входа используется пакетными серверами.
5	Служба	Служба запущена Service Control Manager.
7	Разблокирование	Эта рабочая станция разблокирована.
8	NetworkCleartext	Пользователь вошёл на данный компьютер через сеть. Пароль пользователя передан в нехэшированной форме.
9	NewCredentials	Посетитель клонировал свой текущий маркер и указал новые учётные записи для исходящих соединений.
10	RemoteInteractive	Пользователь выполнил удалённый вход на этот компьютер, используя службу терминалов или удаленный рабочий стол.
11	CachedInteractive	Пользователь вошёл на этот компьютер с сетевыми учётными данными, которые хранились локально на компьютере.

Откройте запись категории «Вход/выход» типа «Аудит успехов» с кодом 551. Данная запись содержит информацию, связанную с успешным выходом пользователя из операционной системы.

Откройте записи категории «Вход учётной записи» (рис. 6, 7). Оба типа события («Успех» и «Отказ») имеют один код события - 680. Дополнительно в записи указывается механизм аутентификации - Microsoft Authentication Package.

Рис. 6 - Запись аудита об отказе входа учётной записи

Рис. 7 - Запись аудита об успешном входе учётной записи

3. Аудит событий, связанных с администрированием

Параметр «Аудит управления учётными записями» включает фиксацию событий, связанных с управлением учётными записями пользователей и групп пользователей. Включите тип событий «Успех» для «Аудита управления учётными записями».

Измените пароль пользователю «user», создайте нового пользователя «user1». Записи категории «Аудит управления учётными записями» содержат как имя учётной

записи, у которой были проведены изменения, так и имя учётной записи пользователя, изменявшего настройки.

Откройте в журнале «Безопасность» запись категории «Учётные записи» с кодом события 628 (при отсутствии записи обновите журнал). Данная запись содержит информацию об изменении пароля учётной записи (рис. 8). В записи аудита представлены имена учётных записей обоих пользователей - у которого пароль был изменён («user») и от имени которой он изменялся («Администратор»).

Рис. 8 - Запись аудита об успешном изменении пароля учётной записи

Откройте запись категории «Учётные записи» с кодом события 626. Данная запись содержит информацию о включении (создании новой) учётной записи пользователя (рис. 9).

При создании нового пользователя автоматически происходит его добавление в группу. Откройте запись категории «Учётные записи» с кодом события 636. Данная запись содержит информацию о добавлении учётной записи пользователя в существующую группу (рис. 10). В записи указаны имя учётной записи пользователя, производившего добавление, имя учётной записи добавляемого пользователя и имя группы, в которую добавляется пользователь.

Рис. 9 - Запись аудита о включении учётной записи

Рис. 10 - Запись аудита о добавлении учётной записи в группу

Параметр «Аудит изменения политики» включает фиксацию событий, связанных с изменением политики аудита, назначения прав пользователям и т.д. Включите тип событий «Успех» для «Аудита изменения политики».

Откройте раздел «Локальные политики - Назначение прав пользователя» в «Локальной политике безопасности». Предоставьте пользователю «user» право «Архивирование файлов и каталогов», удалите право «Локальный вход в систему» у учётной записи «Гость».

Записи категории «Аудит изменения политики» содержат имя учётной записи, производившей изменение какой-либо политики, название изменяемой привилегии или настройки. Если происходило изменение привилегии учётной записи пользователя, то указывается имя этой учётной записи.

Откройте запись категории «Изменение политики» с кодом 608 (рис. 11). Данная запись содержит информацию о предоставлении пользователю права на резервное копирование информации (SeBackupPrivelege).

Рис. 11 - Запись аудита о присвоении пользователю прав

Откройте запись категории «Изменение политики» с кодом 622 (рис. 12). Данная запись содержит информацию об удалении права локального входа пользователя в систему (SeInteractiveLogonRight).

Откройте запись категории «Изменение политики» с кодом 612 (рис. 13). Данная запись содержит информацию об изменении политики аудита. Зафиксировано включение аудита «Успехов» в категории «Изменение политики».

Рис. 12 - Запись аудита об удалении прав у пользователя

Рис. 13 - Запись аудита об изменении политики безопасности

Параметр «Аудит использования привилегий» включает фиксацию событий, связанных с применением пользователем выданных ему привилегий. Включите тип событий «Успех» для «Аудита использования привилегий».

Измените системное время. Завершите сеанс пользователя. Войдите под учётной записью «Администратор».

Откройте запись категории «Использование прав» с кодом 577 (рис. 14). Данная запись содержит информацию об использовании привилегии изменения системного времени (SeSystemtimePrivelege) с указанием пользователя, применившего привилегию.

Рис. 14 - Запись аудита о применении привилегии на изменение системного времени

Откройте запись категории «Использование прав» с кодом 576 (рис. 15). Данная запись содержит информацию о предоставлении пользователю набора привилегий при входе в операционную систему.

Откройте запись категории «Использование прав» с кодом 578 (рис. 16). Данная запись содержит информацию об операции с привилегированным объектом - открытие журнала аудита (EventLog).

Рис. 15 - Запись аудита о присвоении привилегий пользователю при входе в систему

Рис. 16 - Запись аудита о работе с журналом аудита

4. Аудит событий, связанных с работой операционной системы

Параметр «Аудит системных событий» включает фиксацию событий, связанных со следующими системными событиями: изменение системного времени; запуск и отключение элементов системы безопасности и др. Включите тип событий «Успех» для «Аудита системных событий».

Очистите журнал аудита (например, через контекстное меню журнала). Перезагрузите операционную систему.

Откройте запись категории «Системное событие» с кодом 517 (рис. 17). Данная запись содержит информацию о времени очистки журнала аудита и имя учётной записи пользователя, очистившего журнал.

Рис. 17 - Запись аудита об очистке журнала аудита

Откройте запись категории «Системное событие» с кодом 520 (рис. 18). Данная запись содержит информацию об изменении системного времени. Это событие может генерироваться как от имени учётной записи «System» при синхронизации времени с сервером, так и от имени пользователя. В записи указывается предыдущее и новое время.

Рис. 18 - Запись аудита об изменении системного времени

Параметр «Аудит отслеживания процессов» включает фиксацию событий, связанных с работой процессов (создание, завершение, дублирование и т.п.). Включите тип событий «Успех» для «Аудита отслеживания процессов».

Запустите какое-нибудь приложение и закройте его.

Откройте записи категории «Подробное отслеживание» с кодом 592 и 593 (рис. 19, 20). Эти записи содержат информацию о создании нового процесса и его завершении. В информацию о событии включается полное имя исполняемого файла, инициировавшего процесс.

5. Аудит доступа пользователей к ресурсам

Параметр «Аудит доступа к объектам» включает фиксацию событий, связанных с доступом к файлам, каталогам, ключам реестра, принтерам и т.д. Возможен аудит различных типов доступа: чтения, изменения, удаления, печати и др.

Включите оба типа событий («Успех» и «Отказ») для параметра «Аудит доступа к объектам».

Рис. 19 - Запись аудита о запуске приложения (создании процесса)

Рис. 20 - Запись аудита о завершении приложения (выходе из процесса)

Аудит доступа к ресурсам возможен только на логических дисках с файловой системой NTFS. Аудиту подвергаются только те объекты, для которых явно указана необходимость фиксации событий. Таким образом, включение аудита доступа происходит в два этапа: включение «Аудита доступа к объектам» в политике аудита и включение аудита для каждого контролируемого объекта.

Создайте текстовый файл. Перейдите на вкладку «Аудит» в «Свойствах» созданного файла («Свойства - Безопасность - Дополнительно - Аудит»). Включите тип событий «Успех» на тип доступа «Изменение разрешений» для пользователя «Администратор» и тип событий «Отказ» на все типы доступа для пользователя «user» (рис. 21). Во вкладке «Безопасность» свойств созданного файла запретите пользователю «user» доступ на «Запись».

Рис. 21 - Параметры аудита доступа к файлу

Откройте запись категории «Доступ к объекту» с кодом 560 (рис. 22, 23). Данная запись содержит информацию об успешной смене разрешений на доступ к объекту (тип доступа - WRITE_DAC). Кроме типа доступа, в записи указывается информация об объекте доступа: имя и тип (File). О субъекте доступа указывается следующая информация: имя учётной записи, осуществлявшей доступ, и полное имя исполняемого файла процесса, при помощи которого осуществлялся доступ.

Рис. 22 - Запись аудита о доступе к объекту для изменении прав доступа

Рис. 23 - Запись аудита о доступе к объекту для изменении прав доступа (окончание)

Войдите под учётной записью «user». Попытайтесь удалить созданный файл, попытайтесь изменить разрешения на доступ к файлу.
Войдите под учётной записью «Администратор». Откройте записи журнала «Безопасность» категории «Доступ к объекту» с кодом 560, произведённой от имени учётной записи «user». Одна из записей содержит информацию о неуспешной (Аудит отказов) попытке удаления файла (тип доступа - DELETE, рис. 24). Другая запись содержит информацию о неуспешной (Аудит отказов) попытке изменения разрешений на доступ к файлу (рис. 25).

Рис. 24 - Запись аудита о неуспешной попытке доступа к объекту для его удаления

Откройте «Свойства» принтера doPDF («Пуск - Настройка - Принтеры и факсы»). Для принтеров возможен аудит следующих специфичных действий: печать, управление принтерами, управление документами.

Включите тип аудита «Успех» типа доступа «Управление документами» принтера doPDF для пользователя «Администратор» (применить «Для этого принтера и докуентов», рис.26). Напечатайте текстовый документ.

Рис. 25 - Запись аудита о неуспешной попытке доступа к объекту для изменения прав доступа к нему

Рис. 26 - Параметры аудита доступа к принтеру

Просмотрите записи категории «Доступ к объекту» с кодом 560. К печати документа имеют отношение записи с типом объекта Printer (рис. 27) и Document (рис. 28). В записи для принтера указан тип доступа «Печать». В записи для документа указано имя напечатанного документа.

Рис. 27 - Запись аудита об использовании принтера

Рис. 28 - Запись аудита об управлении документом

6. Управление журналом аудита

Войдите под учётной записью «user». Попытайтесь открыть журнал аудита. Группе «Пользователи», в которую входит «user», по умолчанию запрещена работа с журналом аудита, поэтому операционная система сгенерирует ошибку доступа (рис.29).

Рис. 29 - Ошибка доступа к журналу аудита

Запустите от имени учётной записи «Администратор» оснастку «Локальная политика безопасности». Добавьте пользователя «user» в перечень учётных записей параметра «Управление аудитом и журналом безопасности» («Локальные политики - Назначение прав пользователей», рис. 30). Под учётной записью «user» проверьте наличие прав для работы с журналом аудита.

Рис. 30 - Параметр управления доступом к журналу безопасности

Войдите под учётной записью «Администратор». В меню журнала аудита выберите «Вид» - «Фильтр». Настройте фильтр в соответствии с рис. 31. После применения фильтра в журнале останутся записи только об удачных и неудачных попытках входа под учётной записью «user».

Рис. 31 - Настройка фильтрации записей журнала безопасности

При поиске объекта с известным именем лучше использовать функцию поиска: «Вид» - «Найти» (рис. 32), введя имя (часть имени) файла.

В контекстном меню журнала «Безопасность» выберите «Свойства». В появившейся вкладке можно установить максимальный размер журнала и действия в случае его переполнения (рис. 33).

Установите размер журнала в минимально возможное значение - 64 КБ. Включите все возможные виды аудита.

Рис. 32 - Настройка поиска записей журнала безопасности

Рис. 33 - Настройка работы журнала безопасности

Для установки запрета работы пользователя в случае переполнении журнала необходимо включить параметр «Аудит: немедленное отключение системы, если невозможно внести в журнал записи об аудите безопасности» в разделе «Параметры безопасности» локальной групповой политики (рис. 34).

Рис. 34 - Настройка действий при переполнении журнала безопасности

Перезагрузите операционную систему. Войдите под учётной записью «Администратор». Генерируйте новые записи аудита до тех пор, пока не произойдёт заполнение журнала и перезагрузка системы. После этого войдите в систему под учётной записью «Администратор» (рис. 35), сохраните журнал (рис. 36) и очистите его.

Рис. 35 - Окно входа в систему при переполнении журнала безопасности

Рис. 36 - Сохранение журнала безопасности

Просмотр сохранённых журналов безопасности осуществляется при помощи функции «Открыть файл журнала» контекстного меню журнала безопасности.

Задание

Импортируйте журнал безопасности в соответствии со своим вариантом. Проанализируйте журнал безопасности согласно распределению вариантов и определите виновных. Параметры аудита, использовавшиеся при фиксации событий, перечислены в табл. 2. Также включен параметр «Аудит прав на архивацию и восстановление». Правом управлять аудитом и журналом безопасности могут только «Администратор» и пользователь «Анатолий». Сведения об учётных записях перечислены в табл. 3.

Таблица 2. Параметры политик аудита

Название параметра	***Успех***	***Отказ***
Аудит событий входа в систему	+	+
Аудит управления учётными записями	+	+
Аудит доступа к службе каталогов	-	-
Аудит входа в систему	+	+
Аудит доступа к объектам	+	+
Аудит изменения политики	+	+
Аудит использования привилегий	-	+
Аудит отслеживания процессов	-	-
Аудит системных событий	+	+

Таблица 3. Учётные записи

Имя учетной записи	***Должность, группа***
Дмитрий	стажёр, пользователь
Геннадий	финансовый менеджер, пользователь
Василий	оператор пульта видеонаблюдения, пользователь
Администратор	технический консультант, администратор системы
Валерий	директор, оператор архива
Людмила	бухгалтер, пользователь
Татьяна	секретарь, пользователь
Артур	помощник технического консультанта, пользователь
Анатолий	администратор безопасности, администратор системы
ДАВЫДОВ	руководитель отдела разработки, пользователь

Вариант 1

Администратор безопасности Анатолий предоставил полный доступ к материалам по безопасности отдела только стажеру Дмитрий. Эти материалы были размещены на сетевом ресурсе «Ресурсы предприятия\Обмен\Дмитрию», к которому был заранее выставлен аудит чтения, записи, удаления, а также смены владельца. При утилизации документации Анатолий обнаружил распечатанные копии этих материалов. Стажер утверждает свою непричастность к распечатанным копиям важных документов. Докажите или опровергните причастность Дмитрия к распечатанным документам.

Вариант 2

На предприятии есть сетевой ресурс «Ресурсы предприятия\Конкурентоспособность основного продукта», в котором находились два документа «Продукты конкурентов.doc» и «Стратегия развития основного продукта.doc». Доступ на запись и чтение имели только следующие пользователи: «Геннадий» и «ДАВЫДОВ».

Администратор безопасности Анатолий ранее настроил для этого ресурса аудит успехов и отказов удаления, чтения, записи, смены разрешений и смены владельца. Вскоре финансовый менеджер и руководитель отдела разработки сообщили об исчезновении этих документов. Выясните, кто причастен к удалению этих документов?

Вариант 3

Администратор системы неоднократно сообщал о действиях в системе, выполняемых кем-то под его учетной записью, включая смену паролей пользователей. Администратор безопасности посчитал необходимым настроить полный аудит ветви реестра, хранящий учетные записи и их пароли в неявном виде. Ветвь реестра, хранящая базу данных учетных записей, имеет следующий путь: «HKEY_LOCAL_MACHINE\SAM\SAM». Выясните, кто и какой программой получает доступ к базе данных учетных записей.

Вариант 4

Из организации, по собственному желанию, уволился системный администратор, не проработав и одной рабочей недели. По прошествии нескольких дней оператор пульта видеонаблюдения сообщил о странном поведении компьютера: «Компьютер самопроизвольно заблокировался, отобразив окно блокировки пользователем MS_Support_tech567». Выясните причину блокировки.

Вариант 5

В сетевых ресурсах предприятия дополнительной мерой защиты при обмене значимыми электронными документами между сотрудниками является установка пароля. Секретарь оповестила администратора безопасности о недейственности таких мер защиты, приведя в пример редактированный документ «Отчет деятельности сотрудников на апрель. doc» по сравнению с сохранившимся оригиналом. Администратор безопасности настроил аудит чтения на сетевой ресурс «C: \Ресурсы предприятия\Обмен» с применением наследования параметров аудита для создаваемых в нем файловых объектов. Проведите аудит файловых объектов этого ресурса на факт подбора пароля к ним.

Вариант 6

В предприятии имеется доступ к сети интернет, настроенный только для работы с почтовыми серверами. Приходящие счета за предоставления доступа к сети интернет не соизмеримы с объемом трафика, получаемого по почтовым протоколам. Директор потребовал администратора безопасности выяснить причину таких затрат. Проведите аудит запущенных пользователями программ, которые могли получать большой объем данных из сети интернет.

Вариант 7

Администратор безопасности ответственен за лицензионное ПО, используемое в компьютерах организации. Поэтому он должен отслеживать доступ к информации, приводящий к краже закрытой информации лицензионного ПО, такой как 25-тизначный ключ продукта Windows. Большинство такой информации хранится в ветвях реестра, к которым применим аудит чтения. Проведите аудит журнала безопасности на факт чтения значений ветвей реестра лицензионных программ, а также используемые программы.

Вариант 8

Директор организации использует встроенные средства резервирования для файла «База данных заказов.doc», архив которого он сохраняет в папку «C:\АРХИВ\backup», к которому только он имеет доступ. Служба внутренней безопасности организации сообщила об отфильтрованном электронном письме с поддельным адресом отправителя, не значившимся в списке разрешенных отправителей. Текст письма содержал предложение о продаже информации и список электронных документов, в число которых входил архивируемый директором файл. Администратору безопасности было поручено разобраться проблемами утечки информации, в число которых входит вопрос выявления способа получения ограниченных в доступе файлов. Выясните, кто и как получил ограниченный в доступе файл.

Вариант 9

Администратор безопасности посчитал необходимым провести аудит неблагонадежных сотрудников организации. Для этого он открыл доступ к документу «зарплата сотрудников на 30.04.09.doc», назначив аудит чтения и записи. Выявите неблагонадежных пользователей, которые редактировали этот файл.

Вариант 10

Администратор пожаловался на наличие в компьютерах организации нежелательного ПО (компьютерные игры), которое регулярно появляются вновь, включая то, которые требуют для установки права локального администратора. Проведите аудит, чтобы выяснить пользователей, обладающих паролем локального администратора.

Контрольные вопросы

1. Какие данные фиксируются при аудите входа/выхода в систему?
2. Чем отличается аудит входа в систему от аудита событий входа в систему?
3. Какие данные фиксируются при аудите управления учётными записями?
4. Какие данные фиксируются при аудите изменения политики?
5. Какие данные фиксируются при аудите использования прав?
6. Какие данные фиксируются при аудите системных событий?
7. Какие данные фиксируются при аудите отслеживания процессов?
8. Какие типы объектов могут подвергаться фиксации при аудите доступа к объектам? Какие при этом фиксируются данные?

9. Каким образом происходит настройка аудита доступа к объектам?
10. Какие существуют настройки политики безопасности, связанные с аудитом?

Задание

Отчет по лабораторной работе выполняется по стандарту, описанному в методических указаниях