Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования «Тульский государственный университет»

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

НАСТРОЙКА ЛОКАЛЬНОЙ ПОЛИТИКИ БЕЗОПАСНОСТИ

отчет о лабораторной работе №10

по дисциплине
ОПЕРАЦИОННЫЕ СИСТЕМЫ И ИХ БЕЗОПАСНОСТЬ

Выполнила:	студент гр. 230711	Павлова В.С.
Проверил:	доцент каф. ИБ	Антонов Д.М.

Тула, 2023 г

Лабораторная работа – Настройка локальной политики безопасности

Введение

В этой лабораторной работе вы настроите локальную политику безопасности Windows. Локальная политика безопасности Windows используется для настройки различных требований безопасности для автономных компьютеров, не входящих в домен Active Directory. Вы измените требования к паролю, включите аудит, настройте некоторые права пользователя и установите некоторые параметры безопасности. Затем вы будете использовать диспетчер событий для просмотра зарегистрированной информации.

Рекомендуемое оборудование

- Компьютер с установленной Windows.

Примечание. Доступ к инструменту локальной политики безопасности немного отличается в зависимости от версии Windows. Но после того, как он будет открыт, конфигурации для остальных шагов в этой лабораторной работе будут такими же.

Инструкции

Step 1: Ознакомьтесь с требованиями безопасности.

Клиенту необходимо иметь шесть автономных компьютеров Windows в филиале, настроенных в соответствии с политикой безопасности организации. Эти компьютеры не являются частью домена Active Directory. Политики должны быть настроены вручную на каждом компьютере.

Политика безопасности выглядит следующим образом:

- Пароли должны быть не менее 8 символов.
- Пароли необходимо менять каждые 90 дней.
- Пользователь может изменить свой пароль один раз в день.
- Пользователь должен использовать уникальный пароль не менее чем для 8 смен пароля.
- Пароль должен состоять из трех из следующих четырех элементов:
  - Хотя бы один буквенный символ нижнего регистра.
  - Хотя бы один альфа-символ верхнего регистра.
  - Хотя бы один цифровой символ.
  - По крайней мере, один символ символа.
- Пользователи блокируются от компьютера после 5 попыток ввести правильный пароль. Пользователь должен подождать 5 минут, пока счетчик просмотра не сбросится.
- Каждый параметр безопасности для политики аудита должен быть включен.
- Через 30 минут бездействия пользователь автоматически выйдет из системы. (только для Windows 8.1 и 8.0)
- Пользователи должны войти в систему, прежде чем снимать ноутбук с док-станции.
- При входе пользователям должны быть представлены следующие заголовок и текст:
  - Название: **Внимание:**
  - Текст: **Ваша активность отслеживается. Этот компьютер предназначен только для служебного использования.**

- Пользователи получат напоминание о смене пароля за 7 дней до истечения срока его действия.

Инструмент локальной политики безопасности Windows предоставляет гораздо больше параметров, которые выходят за рамки этого курса.

Step 2: Откройте средство локальной политики безопасности Windows.

a. Чтобы получить доступ к локальной политике безопасности в Windows 10, вы можете использовать следующие два пути:

Административные инструменты > Локальная политика безопасности

Или, **Поиск > secpol.msc** а затем щелкните **secpol.msc**.

b. Откроется окно Локальная **политика безопасности .** Эта лабораторная работа будет посвящена **политикам учетных записей** и **локальным политикам** , как показано на рисунке ниже. Остальные **настройки безопасности** выходят за рамки этого курса.

Step 3: Настройте параметры безопасности политики паролей.

Первые шесть требований политики безопасности компании настраиваются в разделе « **Политики учетных записей» инструмента «Локальная политика безопасности»** .

a. Щелкните стрелку рядом с **пунктом «Политики учетных записей»** , чтобы развернуть его, а затем щелкните **«Политика паролей»** . На правой панели отображаются шесть политик со связанными с ними параметрами безопасности по умолчанию.

b. Первая политика, **Enforce password history** , используется для установки количества уникальных паролей, которые пользователь должен ввести, прежде чем ему будет разрешено повторно использовать пароль. Согласно политике безопасности организации на шаге 1 параметр безопасности для этой политики должен быть равен **8** . Дважды щелкните **Принудительно использовать историю паролей** , чтобы открыть окно **Свойства Принудительно применять историю паролей** . Установите значение **8** .

c. Используя требования политики безопасности на шаге 1, заполните значения, которые вы должны установить в **локальной политике безопасности** для остальных параметров безопасности **политики паролей** .

Политика	Настройка безопасности
Использовать историю паролей	8
Максимальный срок действия пароля	*90 дней*
Минимальный срок действия пароля	*1 день*
Минимальная длина пароля	*Не менее 8 символов*
Пароль должен соответствовать требованиям сложности	*Требования:* *- Хотя бы один буквенный символ нижнего регистра.* *- Хотя бы один альфа-символ верхнего регистра.* *- Хотя бы один цифровой символ.* *- По крайней мере, один символ символа.*
Храните пароли с помощью обратимого шифрования	Отключен

Примечание . Параметр безопасности **«Хранить пароли с использованием обратимого шифрования»** всегда должен быть отключен. Хранение паролей с использованием обратимого шифрования по существу не отличается от хранения версий паролей в виде открытого текста. По этой причине никогда не следует включать эту политику, если только требования приложения не перевешивают необходимость защиты информации о пароле.

d. Дважды щелкните каждую из политик и установите значения в соответствии с вашими записями в таблице выше.

Step 4: Настройте параметры безопасности политики блокировки учетной записи.

a. Согласно политике безопасности на шаге 1, сколько раз пользователю разрешено пытаться войти в систему, прежде чем его учетная запись будет заблокирована?

Согласно ПБ, пользователи блокируются от компьютера после 5 попыток ввести правильный пароль.

b. Как долго пользователь должен ждать, прежде чем попытаться снова войти в систему?

Согласно ПБ, Пользователь должен подождать 5 минут, пока счетчик просмотра не сбросится.

c. Используйте параметры безопасности **политики блокировки учетных записей** в **локальной политике безопасности** , чтобы настроить требования политики.

Подсказка : сначала вам нужно настроить **порог блокировки учетной записи** .

Step 5: Настройте параметры безопасности политики аудита.

a. В «Локальной политике безопасности» разверните меню «Локальные политики» и нажмите «Политика аудита».

b. Дважды щелкните **Аудит событий входа в учетную запись** , чтобы открыть окно **Свойства** . Щелкните вкладку **Объяснение** , чтобы узнать об этом параметре безопасности.

c. Перейдите на вкладку **«Локальные параметры безопасности»** и установите флажки « **Успех** » и **«Сбой»** . Нажмите **ОК** , чтобы закрыть окно **свойств** и применить настройки безопасности.

d. Продолжайте изменять остальные параметры безопасности **политики аудита** . Нажмите вкладку **«Объяснение»** для каждого и прочитайте, что он делает. Установите флажки **«Успех»** и **«Неудача» в каждом окне «Свойства»** .

Step 6: Настройте дополнительные параметры безопасности локальных политик.

a. В локальной политике безопасности щелкните «Назначение прав пользователя» в разделе «Локальные политики», чтобы просмотреть параметры безопасности.

b. Хотя ни один из параметров безопасности не нужно изменять для соответствия требованиям политики безопасности, потратьте некоторое время на просмотр параметров по умолчанию.

Вопрос:

Есть ли какие-то, которые вы бы порекомендовали изменить? Почему?

На мой взгляд, целесообразно ограничить доступ простым пользователям к системным ресурсам и возможностям. Например, в доступе к управлению службами, установке программ и изменению системных настроек. Ограничение запуска исполняемых файлов также, на мой взгляд, поможет защитить систему от вредоносных программ и других угроз безопасности: нужно, чтобы пользователи могли запускать только те программы, которые были предварительно установлены администратором системы.

c. В локальной политике безопасности нажмите «Параметры безопасности» в разделе «Локальные политики», чтобы просмотреть параметры безопасности.

d. Что касается остальных требований политики безопасности на шаге 1, перечислите значения политики и параметров безопасности, которые необходимо изменить в **параметрах безопасности,** в таблице ниже. Первый сделан для тебя.

Политика	Настройка безопасности
Интерактивный вход: предел бездействия компьютера	1800 секунд
Интерактивный вход в систему: напоминать об истечении срока действия пароля	*7 дней*
Член пароля: максимальный срок действия пароля	*90 дней*
Устройства: разрешить отстыковку без входа в систему	*Отключен*
Аудит: доступ глобальных системных объектов и др. политики аудита	*Включен*

Step 7: Проверьте параметры безопасности политики паролей.

Проверьте параметры безопасности политики паролей, попытавшись изменить пароль. Попробуйте новый пароль, который не соответствует требованиям по длине или сложности.

Панель управления > Учетные записи пользователей > Внесите изменения в мою учетную запись в настройках ПК > Параметры входа и нажмите **Изменить** в разделе **Пароль** .

Вам должно быть представлено сообщение о том, что ваш новый пароль не соответствует требованиям политики паролей.

Step 8: Экспорт и импорт параметров политики безопасности.

У заказчика есть еще 5 автономных компьютеров, которые должны соответствовать тем же требованиям политики безопасности. Вместо ручной настройки параметров каждого компьютера экспортируйте параметры на этот компьютер.

a. В строке меню локальной политики безопасности нажмите «Действие» > «Экспортировать политику...».

b. Выберите имя для **. inf** и сохраните его в любом месте по вашему выбору.

c. Скопируйте политику безопасности **. инф** файл на флешку. Отнесите флешку на другой компьютер. Вставьте флэш-накопитель, откройте « **Локальная политика безопасности»** и нажмите **«Действие» > «Импортировать политику».** Найдите файл **. inf** на флэш-накопителе и откройте его, чтобы применить политику безопасности к новому компьютеру.