**Практическая работа № 3**

**Тема работы:** Выявление и решение проблем входа в систему**.**

**Цель работы:** Научиться выявлять и устранять проблемы входа в систему.

**Краткие теоретические сведения:** Проблемы с входом в систему - это ситуации, когда машина фактически загружается до ожидаемого экрана приветствия или строки входа, но отказывается принять имя пользователя и пароль, или же принимает их, но затем ведет себя не правильно (не может запустить графический рабочий стол, выдает ошибки, выбрасывает в командную строку и т.д.).

Диагностика проблем входа в систему.Вход в компьютер является настолько привычной частью дня, что мы часто даже не задумываемся о нем. Но даже в этом случае, что-нибудь может и время от времени идет не так, когда пользователи входят в Windows.

Системные часы.Системные часы рабочей станции могут на самом деле служить причиной возникновения проблем входа. Если время на часах рабочей станции на пять минут отличается от времени на контроллере домена, то при входе в систему будет сбой.

Причина этого кроется в протоколе аутентификации Kerberos. В начале процесса аутентификации пользователь вводит пароль и имя пользователя. Затем рабочая станция отправляет запрос аутентификации сервера Kerberos Authentication Server Request на сервер распределения ключей (Key Distribution Server). Этот запрос аутентификации сервера Kerberos Authentication Server Request содержит несколько различных фрагментов информации, включая:

1. Идентификацию пользователя;
2. Имя службы, которую запрашивает пользователь;
3. Аутентификатор, который зашифрован универсальным ключом пользователя. Универсальный ключ пользователя (master key) производиться шифрованием пароля пользователя, используя однонаправленную функцию.

Когда сервер распределения ключей получает запрос, он просматривает пользовательскую учетную запись в Active Directory. Затем он высчитывает универсальный ключ пользователя и использует его для расшифровки аутентификатора также известного, как данные предварительной аутентификации - pre authentication data. Когда рабочая станция пользователя создала аутентификатор, она поместила временную отметку в зашифрованный файл. Как только сервер распределения ключей расшифровывает этот файл, он сравнивает временную отметку с текущим временем на своих часах. Если временная отметка и текущее время имеют разницу не более пяти минут, то запрос аутентификации сервера Kerberos считается действительным, и процесс аутентификации продолжается. Если временная отметка и текущее время имеет разницу в более чем пять минут, то Kerberos считает запрос повторным проигрыванием предварительно полученного пакета, в результате чего отвергает запрос входа. Когда это происходит, отображается следующее сообщение:

***Система не может впустить вас из-за следующей ошибки: наличие разницы во времени между клиентом и сервером. Пожалуйста, повторите попытку или обратитесь за помощью к своему системному администратору.***

Решение этой проблемы довольно простое; просто установите время рабочей станции, чтобы оно соответствовало времени на часах контроллера домена.

Сбои сервера глобальных каталогов.Еще одной главной причиной проблем входа в систему являются сбои сервера глобального каталога. Сервер глобальных каталогов – это контроллер домена, который был настроен на работу в качестве сервера глобальных каталогов. Сервер глобальных каталогов содержит поисковые образы (searchable representation) каждого объекта в каждом домене всего семейства. Когда семейство доменов (forest) изначально создается, первый контроллер домена, который вы запускаете в режим онлайн, автоматически настраивается на работу в качестве сервера глобальных каталогов. Проблема заключается в том, что этот сервер может стать единой точкой сбоя, так как Windows не назначает автоматически других контроллеров домена серверами глобальных каталогов. Если сервер глобальных каталогов дает сбой, то только администраторы домена смогут войти в Active Directory. Нужно настраивать все контроллеры домена на работу в качестве серверов глобальных каталогов только в том случае, если ваше семейство состоит из одного домена. Наличие нескольких серверов глобальных каталогов в семействе с несколькими доменами тоже может быть неплохой идеей, однако выяснение того, какие контроллеры домена должны работать в качестве серверов глобальных каталогов, является чем-то вроде формы искусства. Существует способ разрешения пользователям входить в систему, даже если сервер глобальных каталогов не работает, но с этим способом сопряжен определенный риск безопасности. Если Active Directory работает в собственном режиме (native mode), то сервер глобальных каталогов отвечает за проверку принадлежности пользователя к универсальной группе. Если разрешить пользователям вход во время сбоя, то проверка принадлежности пользователей к универсальной группе осуществляться не будет. Если назначить эксплицитные отказы членам определенных универсальных групп, то эти отказы не будут действовать, пока сервер глобальных каталогов не будет приведен обратно в режим он-лайн. Если позволить пользователям входить в систему, то нужно изменить системный реестр на всех контроллерах домена. Изменение системного реестра опасно, допущенные ошибки могут уничтожить Windows. Поэтому рекомендуется сделать полную резервную копию системы, прежде чем продолжать.

Откройте редактор реестра (Registry Editor) и перейдите по древу реестра к HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa. Теперь создайте DWORD значение с названием IgnoreGCFailures и задайте значение 1. Перезагрузите контроллеры домена после внесения этих изменений.

Сбои сервера DNS.Если ни один из пользователей не может войти в сеть, а контроллеры домена и серверы глобальных каталогов работают нормально, то, возможно, возникла проблема с DNS сервером. Active Directory полностью зависит от службы DNS. DNS сервер содержит записи хостов для каждого компьютера в сети. Компьютеры в сети используют эти записи хостов для разрешения компьютерных имен на IP адресах. Если возникает сбой на DNS сервере, то разрешение имен хостов также не будет работать, что в свою очередь повлияет на процесс входа. Существует два момента, которые необходимо знать относительно сбоев DNS, связанных с проблемами входа:

1. проблемы входа могут и не возникнуть немедленно. ОС Windows содержит DNS кэш, который включает результаты предыдущих DNS запросов. Этот кэш не позволяет рабочим станциям переполнять DNS серверы запросами разрешения имен для одних и тех же объектов снова и снова. Во многих случаях рабочие станции будут иметь в кэще IP адреса контроллеров домена и серверов глобальных каталогов. Но даже в этом случае элементы в DNS кэще со временем устаревают и нуждаются в обновлении. Скорее всего, проблемы входа обнаружатся, когда срок действия записей хоста в кэще начнет истекать.
2. при сбоях DNS существует множество других симптомов, помимо проблем входа. Если только машины в сети не настроены на использование вторичного DNS сервера в случае сбоя основного DNS сервера, вся среда Active Directory со временем придет к полной остановке. Хотя существуют исключения, отсутствие DNS сервера в сети Active Directory обычно ведет к тотальному сбою взаимодействия.

**Ход работы.**

**Пошаговый план устранения проблемы со входом в систему:**

1. загружаем LiveCD и запускаем редактор реестра Windows (команда regedit), рисунок 1;



Рисунок 1 - Запуск редактор реестра Windows

1. запускаем редактор реестра. Открываем раздел **HKEY\_LOCAL\_MACHINE** и монтируем туда реестр другой системы (хостовой), выбирая пункт меню «Файл — Загрузить куст», рисунок 2;



Рисунок 2 - Запуск редактора реестра

1. загружаем куст реестра. Открываем в файловой системе каталог **Windows\System32\config\** и загружаем файл **software —** важно выбрать файловую систему не LiveCD, а хостовой машины, т.е. файл на диске C:\, рисунок 3;



Рисунок 3 - Загрузка куста реестра

1. выбираем улей SOFTWARE.  Даём кусту произвольное имя (1111111111111) в диалоговом окне и открываем там путь (**Microsoft\WindowsNT\CurrentVersion\Winlogon**), а там ключ Userinit, который равен «C:\Windows\userinit.exe,». Видим, что пропущен каталог system32, дописываем его. Сохраняем. Выгружаем куст (аналогично, как и загрузили), рисунок 4;



Рисунок 4 – Выбор улея SOFTWARE

1. меняем значение ключа реестра. Было [3], стало [2] (см. скрин). Перезагружаем систему.

### Настройка часов:

1. на начальном экране введите Дата, коснитесь или щелкните Параметры, а затем коснитесь или щелкните Установка даты и времени;
2. на вкладке Время Интернета коснитесь или щелкните Изменение параметров;
3. установите флажок Синхронизировать с сервером времени Интернета, а затем коснитесь или щелкните Обновить сейчас;
4. если ваш компьютер не подключен к Интернету или находится в режиме «в самолете», синхронизация завершится ошибкой. Убедитесь, что компьютер подключен к Интернету и не находится в режиме «в самолете»;
5. по завершении синхронизации вы получите сообщение о том, что часы были успешно синхронизированы, с указанием имени сервера времени Интернета, а также даты и времени последней синхронизации;
6. после того как дата и время будут успешно синхронизированы, перезагрузите компьютер. Для этого проведите пальцем от правого края экрана и коснитесь Параметры. (Если используется мышь, поместите курсор в правый верхний угол экрана, переместите его вниз и щелкните Параметры.);
7. коснитесь или щелкните Выключение, а затем Перезагрузка.

**Последовательность действий по устранению проблемы входа пользователей в систему с примененными политиками AppLocker.** Правила AppLocker слишком ограничительны. Правила ограничивают запуск приложений и других исполняемых файлов, расположенных в каталоге Windows, что делает невозможным корректный запуск критически важных процессов.

## Решение. Если для задания политик AppLocker используются групповые политики, измените на сервере настройку групповой политики, которая влияет на целевой компьютер. Подождите несколько минут, а затем перезапустите клиентский компьютер, чтобы компонент оболочки загрузился корректно. Если для задания политик AppLocker используется оснастка «Локальная политика безопасности», воспользуйтесь следующей процедурой для устранения проблемы.

#### Создание правил AppLocker по умолчанию:

1. чтобы перезапустить компьютер в безопасном режиме, во время запуска компьютера нажмите и удерживайте клавишу F8 или нажимайте ее до тех пор, пока не отобразится меню **Дополнительные варианты загрузки**;
2. после запуска компьютера в безопасном режиме нажмите кнопку **Пуск**, в поле **Найти программы и файлы** введите **secpol.msc** и нажмите клавишу ВВОД;
3. в дереве консоли разверните пункт **Политики управления приложениями**, а затем разверните пункт **AppLocker**;
4. щелкните правой кнопкой мыши пункт **Исполняемые правила** и выберите команду **Создать правила по умолчанию**;
5. убедитесь, что для папок **Program Files** и **Windows** созданы правила по умолчанию, а затем перезапустите компьютер;
6. возможно, потребуется дважды перезагрузить компьютер, чтобы убедиться в правильном применении правил.

**Устранение типовых проблем, которые чаще всего встречаются при доступе в сетевым ресурсам сетей на базе Windows.**

## По умолчанию в стандартной Windows доступ к сетевым ресурсам без пароля запрещен. В бездоменной сети или необходимо создать пользователей с одинаковыми паролями на всех машинах, или же включить учетные записи гостей, «Все» (если используется авторизация через Гостя), или же назначить тех пользователей, которые будут авторизоваться на машине (в случае авторизации по имени пользователя и паролю).

И здесь могут возникнуть 2 типовые ошибки:

1. вход в систему не произведен. Имеются ограничения, связанные с учетной записью;
2. вход в систему не возможен: выбранный режим входа для данного пользователя на этом компьютере не предусмотрен.

Обе они вызваны настройками локальных политик безопасности на том компьютере, к которому производится подключение.

## Решение:

1. **Вход в систему не произведен. Имеются ограничения, связанные с учетной записью.** Необходимо  изменить: Панель управления > Администрирование > Локальные параметры безопасности > Локальные политики > Назначение прав пользователя > Отказ в доступе к компьютеру из сети. Из списка пользователей там необходимо удалить всех, кроме SUPPORT\_\*. Это позволит подключаться к машине под аккаунтом Гость (если на включена локально).
2. **Вход в систему не возможен: выбранный режим входа для данного пользователя на этом компьютере не предусмотрен.** Необходимо изменить: Панель управления > Администрирование > Локальные параметры безопасности > Локальные политики > Параметры безопасности > Учетные записи: ограничить использование пустых паролей только для консольного входа.Изменить на Выключен. Это позволит входить на компьютер по сети от имени пользователя с пустым паролем и без включенной учетной записи Гостя.

При выполнении лабораторной работы необходимо провести все действия по устранению проблем входа в систему, записать в отчет свои наблюдения и выводы, ответить на контрольные вопросы.

**Контрольные вопросы:**

1. Понятие проблемы входа в систему.
2. Типы проблем входа в систему.
3. Сетевые ошибки Windows.
4. Политики AppLocker.