ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ

ВЫСШЕГО ОБРАЗОВАНИЯ

**БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ НАЦИОНАЛЬНЫЙ**

**ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ**

(НИУ «БелГУ»)

ИНСТИТУТ ИНЖЕНЕРНЫХ И ЦИФРОВЫХ ТЕХНОЛОГИЙ

КАФЕДРА МАТЕМАТИЧЕСКОГО

И ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННЫХ СИСТЕМ

**Отчет по лабораторной работе 5**

**по дисциплине: «Компьютерные сети»**

студента очного отделения

4 курса 12001801 группы

Капустина Виктора Сергеевича

Проверил(а):

Маматов Евгений Михайлович

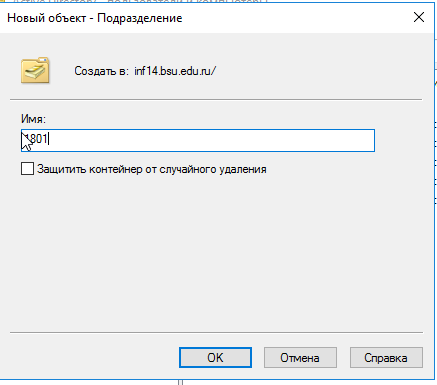
Белгород 2022

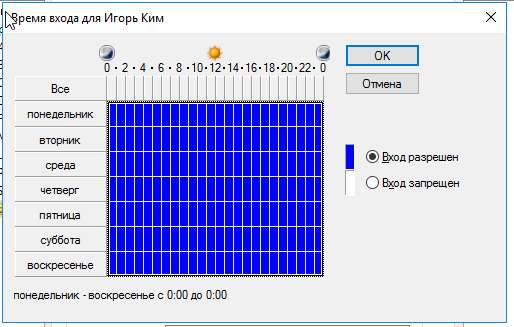
**Лабораторная работа 5**

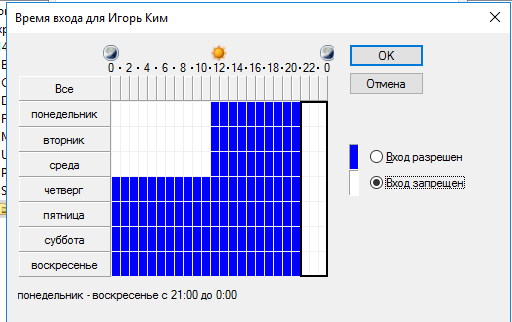
**Цель работы:** научиться администрировать учётные записи пользователей.

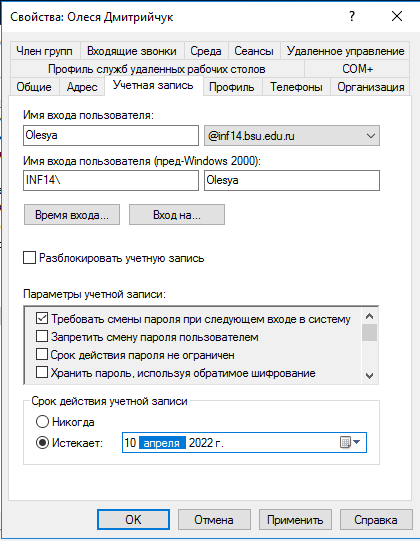
**Ход работы**

**Задание 1**

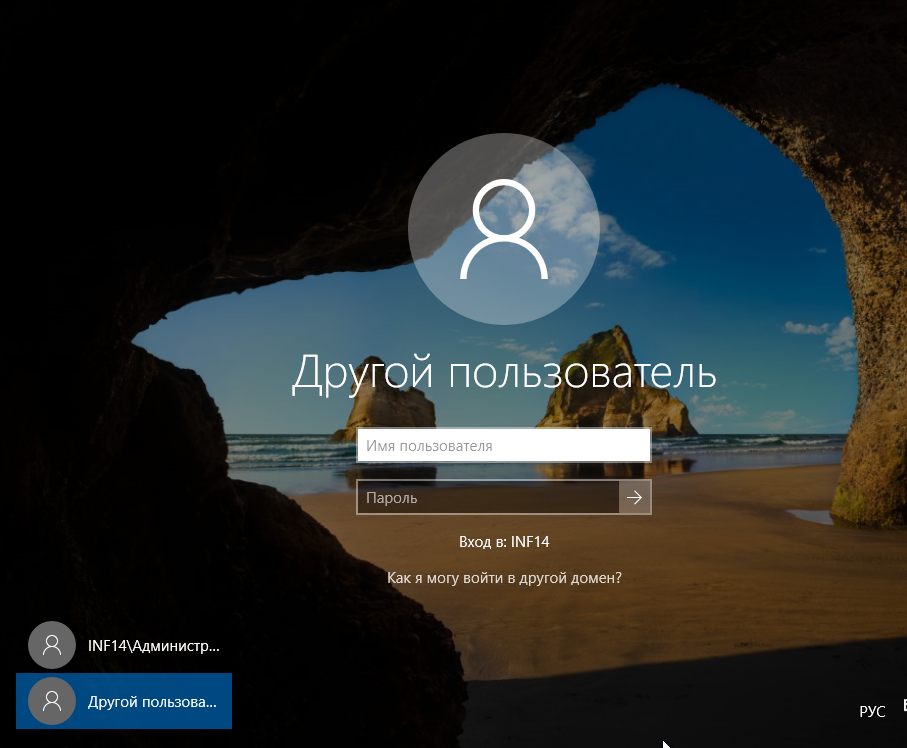
  
Рис. 1 Создание ОП с номером группы

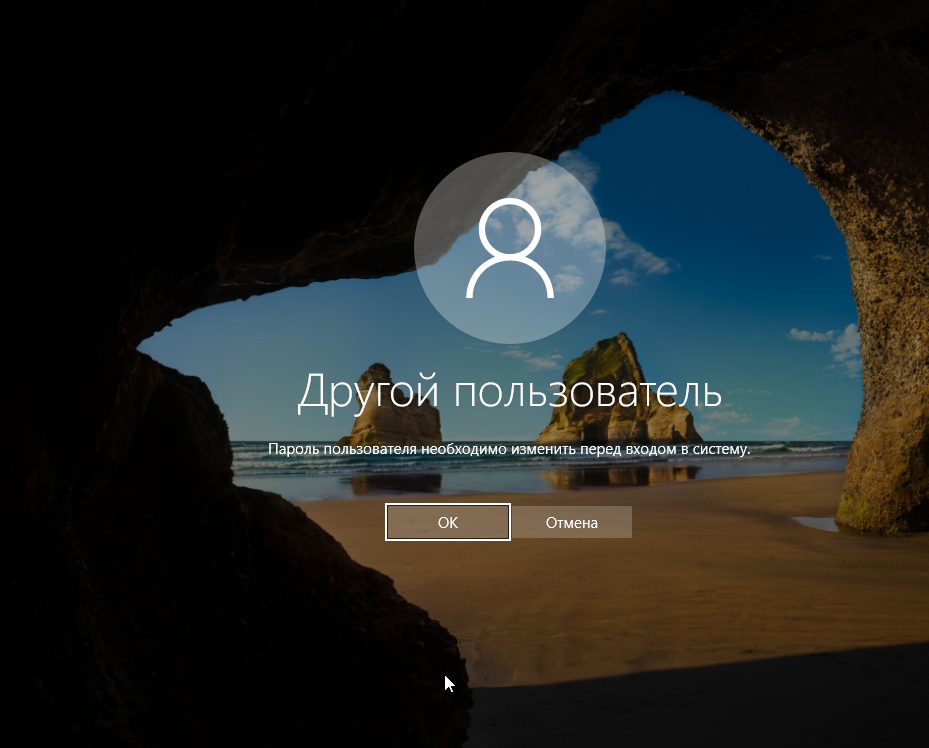
  
Рис. 2 Настройка времени входа пользователя

  
Рис. 3 Установка запрета на вход

  
Рис. 4 Установка срока действия учётной записи

**Задание 2**

  
Рис. 5 Вход в другого пользователя

  
Рис. 6 Требование смены пароля перед входом

**Вывод:** на данной лабораторной научился администрировать учётные записи пользователей.

**Ответы на контрольные вопросы:**

**1.** **Учётные записи пользователей Windows 2016.**

Windows 2016 поддерживает два типа учетной записи пользователя: доменную и локаль­ную. Первая позволяет пользователю войти в домен для доступа к сетевым ресурсам, вто­рая — войти в систему определенного компьютера для получения доступа к ресурсам это­го компьютера.

Кроме того, Windows 2016 предоставляет встроенные учетные записи, применяемые для выполнения административных задач или доступа к сетевым ресурсам.

**Доменные учетные записи**

Позволяют войти в домен и получить доступ к ресурсам сети. При входе пользователь вводит свой пароль и имя. Эта информация позволяет Windows 2016 аутентифицировать его и создать маркер доступа, содержащий сведения о пользователе и параметрах безопас­ности. Маркер доступа идентифицирует пользователя для компьютеров с Windows 2016, к ресурсам которых он пытается получить доступ. Windows 2016 предоставляет маркер до­ступа на время выполнения входа.

Учетная запись пользователя создается в организационном подразделении (ОП) в реплике хранилища Active Directory (именуемом каталогом) на контроллере домена. Контроллер домена реплицирует информацию о новой учетной записи пользователя на все кон­троллеры домена в домене.

После репликации информации о новой учетной записи пользователя все контроллеры данного домена могут аутентифицировать его при входе.

**Локальные учетные записи**

Разрешают пользователям входить в систему и получать доступ к ресурсам только на том компьютере, на котором создана локальная учетная запись. При создании локальной учет­ной записи Windows 2016 создает ее только в БД безопасности данного компьютера. Win­dows 2016 не реплицирует информацию о локальной учетной записи на контроллеры до­мена. После создания локальной учетной записи компьютер использует свою локальную БД безопасности для аутентификации локальной учетной записи, что позволяет пользо­вателю войти в систему данного компьютера.

**Встроенные учетные записи пользователей**

Windows 2016 автоматически создает несколько встроенных учетных записей, из которых чаще всего применяются Администратор (Administrator) и Гость (Guest). ОС не позволяет удалять встроенные учетные записи или отключать запись Administrator, хотя встроенные учетные записи можно переименовывать.

**Учетная запись Администратор (Administrator)**

Применяется для управления общей конфигурацией компьютера или домена, например, для создания и изменения учетных записей пользователей и групп, управления полити­кой безопасности, создания принтеров и предоставления учетным записям разрешений доступа к ресурсам. Если Вы администратор, создайте учетную запись пользователя для выполнения неадминистративных задач. Применяйте учетную запись Administrator толь­ко для выполнения административных задач.

**Учетная запись Гость (Guest)**

Позволяет случайным пользователям войти в систему и получить временный доступ к ре­сурсам.

*Примечание: учетная запись Гость (Guest) по умолчанию отключена. Включайте ее только в сетях с низким уровнем безопасности и всегда назначайте ей пароль.*

**2.** **Правила именования учётных записей**

| **Предмет рассмотрения** | **Объяснение** |
| --- | --- |
| Уникальные регистрационные имена пользователей | Регистрационные имена пользователей домена должны быть уникальны в пределах каталога и внутри ОП, где создаются доменные учетные записи. Локальные учетные записи должны быть уникальны в пределах компьютера. |
| Максимум 20 символов | Регистрационное имя может содержать не более 20 симво­лов прописных или строчных букв. Поле ввода принимает более 20 символов, но Windows 2003 распознает только первые 20. |
| Недопустимые символы | “ / \ [ ] : ; | , + \* ? < > |
| Регистрационные имена не чувствительны к регистру | Для создания уникальных учетных записей можно использовать комбинацию специальных и алфавитно-цифровых символов. Регистрационные имена не чувствительны к регистру, хотя и сохраняют его. |
| Сотрудники с одинаковыми именами | Для различения одинаковых имен можно использовать имя и первую букву фамилии и затем добавить разное количество букв фамилии. |
| Тип сотрудника | Иногда по учетным записям пользователей полезно идентифицировать временных сотрудников. |
| Имена учетных записей служб | Для работы многих фоновых служб требуются учетные записи. Добавьте к именам таких учетных записей аббревиатуру, например svc. |

**Требования к паролю**

В целях защиты доступа к домену или компьютеру каждый пользователь должен иметь пароль.

Для паролей существуют следующие правила.

1 Для предотвращения несанкционированного доступа к учетнойзаписи Администратор (Administrator) присваивайте пароль для этой учетной записи.

2 Определите, будут ли администратор илипользователи контролировать пароли.Вы можете присвоить уникальные пароли для учетных записей пользователей и запретить пользователям изменятьих или разрешить им ввести свои пароли при первом входе в систему. В большинстве случаев контролировать пароли следует пользователям.

3 Используйте пароли, которые сложно разгадать. Избегайте паролей, содержащих яв­ные ассоциации, например, имена членов семьи.

4 Пароль может содержать до 128 символов, минимальная рекомендуемая длина - 8 символов.

5 Используйте прописные и строчные буквы, цифры и допустимые специальные симво­лы. Недопустимые символы перечислены в приведенной выше таблице.

**3.** **Параметры учётных записей**

Определите время, когда пользователь может входить в сеть, и компьютеры, с которых это можно делать. Установите сроки действия учетных записей временных пользователей.

**Время входа**

Для контроля за входом пользователя на домен задайте часы входа в систему – срок в течение, которого пользователи могут работать в сети. По умолчанию Windows 2016 раз­решает доступ в любой день 24 часа в сутки. Можно разрешить вход только в рабочее время. Установка времени входа сокращает срок, в течение которого учетная запись от­крыта для несанкционированного доступа.

**Компьютеры, с которых пользователи могут входить в систему**

По умолчанию пользователи могут входить в домен с любого компьютера домена. Потре­буйте, чтобы пользователи входили в домен только с их собственных компьютеров. Это предотвратит их доступ к конфиденциальной информации на других компьютерах.

*Примечание: Если отключить NetBIOS поверх TCP/IP, Windows 2016 не сможет опреде­лить компьютер, с которого осуществлен вход в систему, и Вы не сможете ограничить вход пользователей определенными компьютерами. Дело в том, что NetBT ограничивает доступ по имени компьютера, а не по МАС-адресу.*

**Срок действия учетной записи**

Определите, задавать ли срок действия учетной записи пользователя. Если да, то для от­ключения учетной записи при прекращении доступа к сети установите дату окончания действия учетной записи пользователя. Для временных сотрудников установите срок дей­ствия учетных записей в соответствии с датой окончания их контрактов.

**Создание учетных записей пользователей**

Можно создать два типа учетных записей пользователей: доменные и локальные.

**Создание доменных учетных записей**

Для этого служит оснастка Active Directory — пользователи и компьютеры (Active Directory Users And Computers). Учетная запись пользователя домена создается на первом доступ­ном для ММС контроллере домена и затем тиражируется на все контроллеры домена.

**Параметры доменной учетной записи:**

| Параметры | Описание |
| --- | --- |
| First Name (Имя) | Имя пользователя |
| Last Name (Фамилия) | Фамилия пользователя |
| Full Name (Полное имя) | Имя и фамилия пользователя. При вводе информации в поля First Name или Last Name Windows 2016 автоматически заполняет это поле. Windows 2016 отображает имя пользователя в ОП, к которому относится его учетная запись. |
| User Logon Name (имя входа пользователя) | Уникальное имя пользователя для входа в систему, созданное (имя входа пользователя) на основе правил именования. Оно требуется в обязательном порядке и должно быть уникальным в каталоге. |
| User Logon Name (pre-Windows 2016) (Имя входа пользователя Windows NT 4.0/3.51) | Уникальное имя пользователя, применяемое для входа в систему клиентов низшего уровня (пред-Windows 2016), например, Windows NT 4.0/3.51. Оно требуется в обязательном и должно быть уникальным в домене. |

**Настройка требований к паролю**

При добавлении новой учетной записи для пользователя можно ввести пароль. В диалого­вом окне Новый объект (New Object) — Пользователь (User) щелкните кнопку Далее (Next), чтобы открыть второе диало­говое окно Новый объект (New Object) — Пользователь (User). Здесь задаются параметры пароля для доменной учетной записи. Вводить пароль для пользователя не обязательно, но тогда пользователь будет вхо­дить в домен без пароля.

Параметры пароля таковы:

| Параметры | Описание |
| --- | --- |
| Password (Пароль) | Пароль служит для аутентификации пользователя. Для обеспечения большей безопасности пароль следует присваивать всегда. Заметьте: при наборе пароль представлен на экране в виде звездочек. |
| Confirm Password (Подтверждение) | Чтобы убедиться в правильности ввода пароля, подтвердите его набрав еще раз. |
| User Must Change Password At Next Logon (Потребовать смену пароля при следующем входе в систему) | Выберите этот параметр, если хотите, чтобы пользователь изменил свой пароль при первом входе в систему. Это гарантирует, что пароль будет знать только он. |
| User Cannot Change Password (Запретить смену пароля пользователем) | Выберите этот параметр, если несколько человек пользуются одной доменной учетной записью (например, Guest) или для контроля за паролями учетных записей. Этот параметр обычно задают для контроля паролей учетных записей фоновых служб. |
| Account Is Disabled (Отключить учетную запись) | Служит для запрещения этой учетной записи, например для нового сотрудника, еще не приступившего к работе. |
| Password Never Expires (Срок действия пароля не ограничен) | Выберите этот параметр, если пароль не должен меняться, например, для доменной учетной записи, которая понадобится какой-либо программе или службе Windows 2003. Данныйпараметр переопределяет параметр User Must Change Password At Next Logon (Потребовать смену пароля при следующем входе в систему). Если выбраны оба, Windows 2003 автоматически снимает флажок User Must Change Password At Next Logon. |

*Примечание: Всегда требуйте, чтобы новые пользователи изменяли свои пароли при первом входе в систему. Это заставит их применять пароли, известные только им. Для усиления безопасности в сетях при помощи комбинации цифр и букв создайте для всех новых учетных записей пользователей пароли со случайным набором символов. Создание пароля со случайным набором символов будет способствовать обеспечению безопасности учетной запи­си пользователя.*