

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Политехнический институт
Факультет приборостроения,
информационных технологий и
электроники

Кафедра
«Информационная безопасность
систем и технологий»

Специальность 10.05.02 –

Специализация -

Информационная безопасность
телекоммуникационных систем
Разработка защищенных
телекоммуникационных систем

ДИПЛОМНЫЙ ПРОЕКТ

на тему

ЛАБОРАТОРНЫЙ ПРАКТИКУМ ПО ИЗУЧЕНИЮ МЕХАНИЗМОВ
ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ДОСТУПА К ЛОКАЛЬНЫМ И СЕТЕВЫМ
РЕСУРСАМ В ОПЕРАЦИОННЫХ СИСТЕМАХ СЕМЕЙСТВА WINDOWS

Студент Горбунов Максим Александрович
Руководитель к.т.н., доцент кафедры ИБСТ Шумкин С.Н.
Нормоконтролёр Фатеев А.Г.
Рецензент заместитель генерального директора
по специальным вопросам АО «ПНИЭИ» Сомкин С.А.

Работа допущена к защите (протокол заседания кафедры от 23.01.18 № 1)
Заведующий кафедрой С.Л. Зефирова

Работа защищена с отметкой хорошо (протокол заседания ГЭК
от 15.01.18 № 17)
Секретарь ГЭК А.Г. Фатеев

Пенза 2018

Работа проверена 10 баллов
24.01.2018 Б. Султанов

Оглавление

Введение.....	4
1 Обзор и анализ способов идентификации, протоколов аутентификации и настроек безопасности в различных ОС семейства Windows	6
1.1 Способы идентификации и аутентификации в ОС семейства Windows.....	6
1.2 Локальная и доменная аутентификация.....	6
1.3 Настройки безопасности в ОС семейства Windows.....	9
2 Обзор вариантов использования разрешений NTFS в различных ОС семейства Windows	12
3 Обзор и анализ способов организации общего и сетевого доступа к локальным и сетевым ресурсам на локальных и на удаленных компьютерах под управлением ОС семейства Windows	16
3.1 Что такое общий доступ?.....	16
3.2 Настройка общего доступа на компьютере, не входящем в домен.....	16
3.3 Настройка общего доступа на компьютере, входящем в домен	17
3.4 Конфликты прав доступа к сетевым ресурсам.....	17
4 Разработка лабораторного практикума по изучению механизмов обеспечения безопасности доступа к локальным и сетевым ресурсам в операционных системах семейства Windows.....	19
5 Вредные психофизиологические факторы, влияющие на нервную систему специалиста по защите информации. Методы и средства физической культуры, снижающие их воздействие.....	21
Заключение	24
Список используемых источников.....	25
Приложение А Лабораторная работа №1 «Изучение механизмов идентификации и аутентификации в ОС семейства Windows»	26

Приложение Б Лабораторная работа №2 «Изучение механизмов разграничения доступа к локальным ресурсам в ОС семейства Windows»	50
Приложение В Лабораторная работа №3 «Изучение механизмов разграничения доступа к сетевым ресурсам в ОС семейства Windows»	59
Приложение Г Протокол проверки на оригинальность в системе «Антиплагиат.ВУЗ»	71

Введение

Операционные системы семейства Windows – наиболее распространенные операционные системы, которые используются в частных, государственных и муниципальных организациях, у подавляющего большинства из которых недостаточно средств для приобретения специальных программных и аппаратных средств защиты информации. Именно поэтому важно уделить особое внимание встроенным механизмам защиты операционных систем.

Многие студенты, обучающиеся на специальностях, связанных с защитой информации, после получения высшего образования пойдут работать в организации, в которых в основном используются операционные системы семейства Windows. Именно поэтому следует уделить внимание на ознакомление студентов со встроенными механизмами защиты информации операционных систем семейства Windows. Для более детального изучения и получения студентами практических навыков в этой сфере следует составить лабораторный практикум.

Целью выпускной квалификационной работы является разработка лабораторного практикума по изучению механизмов обеспечения безопасности доступа к локальным и сетевым ресурсам в операционных системах Windows.

Задачами выпускной квалификационной работы являются:

- обзор и анализ способов идентификации, протоколов аутентификации и настроек безопасности в различных ОС семейства Windows;
- обзор вариантов использования разрешений NTFS в различных ОС семейства Windows;
- обзор и анализ способов организации общего и сетевого доступа к локальным и сетевым ресурсам на локальных и на удалённых компьютерах под управлением ОС семейства Windows;
- разработка лабораторного стенда для проведения лабораторного практикума;

- разработка лабораторного практикума, включающего в себя три работы по следующим темам:

- изучение механизмов идентификации и аутентификации в ОС семейства Windows;

- изучение механизмов разграничения доступа к локальным ресурсам в ОС семейства Windows;

- изучение механизмов разграничения доступа к сетевым ресурсам в ОС семейства Windows;

- разработка рекомендаций для проведения работ лабораторного практикума;

- разработка вариантов заданий для проведения лабораторного практикума;

- исследование вредных психофизиологических факторов, влияющих на нервную систему специалиста по защите информации, а также методов и средств физической культуры, снижающих их воздействие.

Актуальность данной работы состоит в том, что получение студентами практических навыков в изучении встроенных механизмов защиты операционных систем семейства Windows пригодится им в дальнейшем в профессиональной деятельности, поскольку встроенные механизмы защиты информации операционных систем семейства Windows используются всегда, в том числе совместно с другими специальными аппаратными или программными средствами защиты информации.

1 Обзор и анализ способов идентификации, протоколов аутентификации и настроек безопасности в различных ОС семейства Windows

1.1 Способы идентификации и аутентификации в ОС семейства Windows

Система идентификации и аутентификации является одним из основных элементов защиты от несанкционированного доступа любой информационной системы.

Выделяют три основные группы способов аутентификации пользователей:

- аутентификация по паролю;
- аутентификация с помощью идентификатора;
- аутентификация с помощью биометрических данных.

Также аутентификация может быть усиленной, т.е. совмещать в себе одновременно несколько способов аутентификации.

Поскольку идентификация с помощью идентификатора или биометрических данных требует специальных программно-аппаратных средств, рассмотрим только идентификацию пользователей с использованием пароля.

1.2 Локальная и доменная аутентификация

1.2.1 Локальная идентификация и аутентификация.

Под локальной аутентификацией понимается проверка подлинности пользователя на рабочей станции, не входящей в домен.

Аутентификация пользователя непосредственно на рабочей станции происходит следующим образом:

- после того как пользователь ввел свои аутентификационные данные, эти данные передаются подсистеме локальной безопасности (LSA), которая сразу преобразует пароль в хэш. В открытом виде пароль нигде в

системе не хранится и не фигурирует, пользователь - единственный кто его знает;

- затем служба LSA обращается к диспетчеру учетных записей безопасности (SAM) и сообщает ему имя пользователя. Диспетчер обращается в базу SAM и извлекает оттуда хэш пароля указанного пользователя, сгенерированный при создании учетной записи;

- затем LSA сравнивает хэш введенного пароля и хэш из базы SAM, в случае их совпадения аутентификация считается успешной, а хэш введенного пароля помещается в хранилище службы LSA и находится там до окончания сеанса пользователя.

Также локальная аутентификация может осуществляться на удаленном компьютере, не входящем в домен, если несколько компьютеров объединены в рабочую группу. Такая аутентификация происходит с помощью протоколов LM[1], NTLM[2] и NTLMv2[3].

Впервые протокол LM появился в Windows 3.11, а затем использовался в семействе Windows 9.x.

Недостатками протокола LM являются:

- слабое шифрование паролей;
- приведение хэша к фиксированной длине в 14 знаков;
- разбиение полученного хэша на две 7-байтовые части.

Благодаря этим недостаткам восстановление злоумышленником исходного пароля не составляет труда. Поэтому на данный момент протокол считается совершенно небезопасным[4].

Протокол аутентификации NTLM появился в Windows NT. А до появления Kerberos в Windows 2000 был единственным протоколом аутентификации в домене NT.

На данный момент протокол NTLM, также как и протокол LM, считается небезопасным[4]. У злоумышленника существует возможность восстановить хэш пароля. Помимо этого подлинность клиента сервером никак не

проверяется, следовательно, злоумышленник может использовать перехваченные данные для доступа к ресурсам сети. Отсутствие проверки подлинности обусловлено тем, что протокол изначально разрабатывался для небольших сетей, где все узлы считаются легитимными.

С выходом Windows 2000 Microsoft представила вторую версию протокола NTLMv2, который был серьезно доработан в плане улучшений криптографической стойкости и противодействия распространенным типам атак.

Наличие метки времени позволяет избежать ситуации, когда злоумышленник первоначально накапливает перехваченные данные, а потом с их помощью осуществляет атаку, однако NTLMv2, как и его предшественник, не осуществляет взаимную проверку подлинности, что является уязвимостью протокола. Благодаря данной уязвимости протокол NTLMv2 подвержен атакам типа «прослушивание сетевого трафика»[5].

1.2.2 Доменная идентификация и аутентификация.

Главным отличием доменной аутентификации от локальной является то, что хэши паролей пользователей хранятся не в локальных базах SAM, а на контроллерах доменов, НСД к которым злоумышленнику получить сложнее. Помимо этого при доменной аутентификации используется протокол Kerberos[6]. Следовательно, использование доменной аутентификации позволяет избежать уязвимости, которые присущи локальной аутентификации.

В отличие от NTLM протокол Kerberos изначально разрабатывался с условием, что первичная передача информации будет производиться в открытых сетях, где она может быть перехвачена и модифицирована. Также протокол предусматривает обязательную взаимную аутентификацию клиента и сервера, а взаимное доверие обеспечивает единый удостоверяющий центр, который обеспечивает централизованную выдачу ключей.

Основой инфраструктуры Kerberos является центр распространения ключей (KDC), который является доверенным центром аутентификации для всех участников сети. Он содержит долговременные ключи для всех

участников сети, долговременные ключи формируются на основе пароля и являются так называемым "секретом для двоих". С помощью такого секрета каждый из его хранителей может легко удостовериться, что имеет дело со своим напарником. При этом долговременные ключи ни при каких обстоятельствах не передаются по сети и располагаются в защищенных хранилищах центра распространения ключей, либо сохраняются только на время сеанса.

В структуре Active Directory центр распространения ключей располагается на контроллере домена, но Kerberos отвечает только за аутентификацию клиентов, а контроллер домена - за авторизацию.

Таким образом, в протоколе Kerberos был учтен главный недостаток протокола NTLM, а именно отсутствие взаимной аутентификации. Помимо этого при использовании протокола Kerberos хэш пароля клиента экспонируется намного реже, чем в случае применения NTLM. Хэш пароля экспонируется только в том случае, когда клиент запрашивает TGT - один раз каждые восемь часов. С другой стороны, в случае применения NTLM хэш пароля экспонируется всякий раз, когда клиент использует NTLM для аутентификации на сервере. Благодаря этим факторам, данный протокол является основным протоколом доменной аутентификации в ОС Windows. Однако существует недостаток, отсутствие синхронизации времени между рабочими станциями может привести к ошибкам в процессе аутентификации.

1.3 Настройки безопасности в ОС семейства Windows

1.3.1 Локальные параметры безопасности.

В операционных системах семейства Windows существует встроенный инструментарий, позволяющий управлять безопасностью компьютеров. Данный инструментарий называется групповая политика безопасности. Групповая политика безопасности включает в себя такие разделы, как «Политики учетных записей» и «Локальные политики».

В разделе «Политики учетных записей» есть два подраздела: «Политики пароля» и «Политики блокировки учетной записи».

В подразделе «Политики пароля» задаются следующие параметры безопасности:

- максимальный срок действия пароля;
- минимальная длина пароля;
- минимальный срок действия пароля;
- пароль должен отвечать требованиям сложности;
- хранение паролей, используя обратимое шифрование.

В подразделе «Политики блокировки учетной записи» задаются следующие параметры безопасности:

- время до сброса счетчика блокировки;
- пороговое значение блокировки;
- продолжительность блокировки учетной записи.

Настройка параметров «Политики учетных записей» затрудняет подбор пароля злоумышленником путем перебора всевозможных комбинаций, а также делает невозможным использование злоумышленником старых, уже известных ему паролей.

Подраздел «Локальные политики» содержит следующие типы параметров политики:

- «политика аудита» содержит параметры безопасности, которые управляют регистрацией событий безопасности в журнале безопасности на компьютере, а также указывает, какие типы событий безопасности следует регистрировать;
- «назначение прав пользователя» определяет пользователей или группы, которые имеют права или привилегии входа на устройстве;
- «параметры безопасности» определяет параметры безопасности для компьютера, например имена учетных записей администратора и гостя, доступ

к дисководам и приводам компакт-дисков, установка драйверов, попытки входа и т. д.

Настройка параметров «Локальных политик» позволяет предотвратить случайные ошибки пользователей, а также позволяет проводить мониторинг инцидентов информационной безопасности и на основе полученных сведений проводить усовершенствование системы защиты.

1.3.2 Доменные параметры безопасности.

Отличие доменных параметров безопасности от локальных заключается в том, что доменные параметры применяются сразу ко всем рабочим станциям, входящим в домен. Помимо этого доменные параметры безопасности находятся на более высоком уровне иерархии, чем локальные. Это означает, что первым обрабатывается объект локальной групповой политики, а объекты групповой политики, привязанные к домену, обрабатываются в последнюю очередь, то есть переопределяют более ранние объекты групповой политики.

Также в доменных параметрах безопасности в разделе «Политики учетных записей» существует подраздел «Политика Kerberos», определяющая, связанные с Kerberos параметры, такие как срок действия и применение билета.

2 Обзор вариантов использования разрешений NTFS в различных ОС семейства Windows

Файловая система NTFS позволяет настраивать параметры безопасности для каждого файла или папки. Для каждого файла или папки файловая система NTFS хранит так называемые списки доступа ACL, в которых перечислены все пользователи и группы, которые имеют определенные права доступа к данному файлу или папке.

Использование разграничения доступа пользователей к системе позволяет явно указать, какие пользователи и группы имеют доступ к файлам и папкам, и какие операции с их содержимым они могут выполнять. В результате этого пользователи не смогут модифицировать или удалить данные, которые им не нужны для выполнения их профессиональной деятельности. Можно ограничить пользователям просмотр содержимого некоторых файлов и папок, если они содержат некую конфиденциальную информацию. Также разграничение доступа используется для того, чтобы запрещать всем пользователям, кроме тех, что входят в группу администраторов, изменения настроек безопасности.

Таким образом, правильная настройка разрешений NTFS является важной составляющей частью настройки безопасности системы, поскольку ошибки в настройке могут привести к таким последствиям, как непреднамеренное удаление или модификация файлов и данных в системе, что, в свою очередь, может приостановить деятельность организации.

В файловой системе NTFS каждый файл или папка могут иметь следующие права безопасности:

- чтение — разрешает или запрещает обзор папок и просмотр списка файлов и подпапок, просмотр и доступ к содержимому файла;
- запись — разрешает или запрещает добавление файлов и подпапок, запись данных в файл;

- чтение и выполнение — разрешает или запрещает обзор папок и просмотр списка файлов и подпапок, разрешает просмотр и доступ к содержимому файла, а также запуск исполняемого файла;
- список содержимого папки — разрешает или запрещает обзор папок и просмотр только списка файлов и подпапок, данное разрешение устанавливается только для папок;
- изменение — разрешает или запрещает просмотр содержимого и создание файлов и подпапок, удаление папки, чтение и запись данных в файл, удаление файла;
- полный доступ — разрешает или запрещает просмотр содержимого, а также создание, изменение и удаление файлов и подпапок, чтение и запись данных, а также изменение и удаление файла.

При настройке разрешений NTFS обычно только группе администраторов назначается «полный доступ» ко всем файлам и папкам. Для остальных пользователей рекомендуется создавать отдельную личную папку, к которой ему назначается «полный доступ», кроме «удаления» или «изменения параметров» этой папки, а для всех остальных папок пользователю назначается либо разрешение на «чтение» или «просмотр содержимого», либо запрещаются любые действия.

Перечисленные выше права являются базовыми. Базовые права состоят из особых прав. Особые права представляют собой более подробные права, из которых формируются базовые права. Использование особых прав дает очень большую гибкость при настройке прав доступа.

Список особых прав доступа к файлам и папкам:

- обзор папок/выполнение файлов — разрешает или запрещает перемещение по структуре папок в поисках других файлов или папок, выполнение файлов;

- содержание папки/чтение данных — разрешает или запрещает просмотр имен файлов или подпапок, содержащихся в папке, чтение данных из файла;
- чтение атрибутов — разрешает или запрещает просмотр атрибутов файла или папки;
- чтение дополнительных атрибутов — разрешает или запрещает просмотр дополнительных атрибутов файла или папки;
- создание файлов/запись данных — разрешает или запрещает создание файлов в папке, внесение изменений в файл и запись в него данных поверх имеющегося содержимого;
- создание папок/дозапись данных — разрешает или запрещает создание папок в папке, внесение данных в конец файла, но не изменение, удаление или замену имеющихся данных;
- запись атрибутов — разрешает или запрещает смену атрибутов файла или папки;
- запись дополнительных атрибутов — разрешает или запрещает смену дополнительных атрибутов файла или папки;
- удаление подпапок и файлов — разрешает или запрещает удаление подпапок и файлов;
- удаление — разрешает или запрещает удаление файла или папки;
- чтение разрешений — разрешает или запрещает чтение разрешений на доступ к файлу или папке;
- смена разрешений — разрешает или запрещает смену разрешений на доступ к файлу или папке;
- смена владельца — разрешает или запрещает вступать во владение файлом или папкой;
- синхронизация — разрешает или запрещает ожидание различными потоками файлов или папок и синхронизацию их с другими потоками. Это

разрешение применимо только к программам, выполняемым в многопоточном режиме с несколькими процессами.

При настройке особых разрешений работают те же рекомендации, как и при настройке разрешений NTFS. Отличие в том, что особые разрешения позволяют более гибко настроить права пользователей, например, разрешение «удаление файлов и подпапок» будет работать даже при отсутствии разрешения «удаление»

Все разрешения или запрещения файлов и папок делятся на два вида: явные и наследуемые. Механизм наследования подразумевает автоматическую передачу чего-либо от родительского объекта дочернему. В файловой системе это означает, что любой файл или папка могут наследовать свои права от родительской папки. Это очень удобный механизм, избавляющий от необходимости назначать явные права для всех вновь создаваемых файлов и папок.

Результатом применения явных и наследуемых прав и будут фактические права на конкретную папку или файл. Но у совместного использования явных и наследуемых прав есть один недостаток. При установке явных запретов дочернему объекту, который унаследовал разрешения от родительского объекта, данные запреты могут не работать, потому что в наследуемых правах доступа установлено разрешение на данное действие. В таких случаях следует либо пользоваться только наследуемыми правами доступа, избегая явных запретов на совершение каких-либо действий, либо предотвратить наследование разрешений, назначенных для родительской папки, подпапками и файлами, содержащимися в ней. При использовании второго варианта папка, для которой было предотвращено наследование становится новой родительской папкой.

3 Обзор и анализ способов организации общего и сетевого доступа к локальным и сетевым ресурсам на локальных и на удаленных компьютерах под управлением ОС семейства Windows

3.1 Что такое общий доступ?

Под общим ресурсом понимается устройство или часть информации, к которой может быть осуществлен удаленный доступ с другого компьютера. Как правило, общий доступ организовывается с целью облегчения работы пользователей. В общей папке располагаются данные необходимые для работы нескольким пользователям, следовательно, исключается необходимость пересылать какие-либо файлы каждому пользователю при внесении в них изменений.

Также общий доступ может быть организован и к периферийным устройствам, таким как, принтеры, сканеры, проекторы и т.п. В результате этого исключается необходимость наличия периферийных устройств у каждого компьютера сети.

3.2 Настройка общего доступа на компьютере, не входящем в домен

Организация общего доступа к сетевым ресурсам на компьютере, не входящем в домен, представляет собой создание общей папки, к которой могут обращаться пользователи с других компьютеров. Для этого в свойствах папки, к которой необходимо предоставить общий доступ, во вкладке «доступ» нужно нажать кнопку «Общий доступ». Далее в открывшемся окне добавить учетные записи пользователей, которым будет предоставляться общий доступ к данной папке, и назначить им уровень разрешений или сетевые разрешения.

Существуют следующие уровни разрешений к общей папке на локальном компьютере:

- чтение — разрешает или запрещает обзор папок и просмотр списка файлов и подпапок, просмотр и доступ к содержимому файла;
- изменение — разрешает или запрещает просмотр содержимого и создание файлов и подпапок, удаление папки, чтение и запись данных в файл, удаление файла;
- полный доступ — разрешает или запрещает просмотр содержимого, а также создание, изменение и удаление файлов и подпапок, чтение и запись данных, а также изменение и удаление файла.

При настройке разрешений для общей папки на локальном компьютере рекомендуется устанавливать уровень разрешений «полный доступ» только учетным записям, входящим в группу администраторов. Учетным записям пользователей рекомендуется устанавливать уровень разрешений «изменение».

3.3 Настройка общего доступа на компьютере, входящем в домен

Организация общего доступа по сети на любом компьютере домена осуществляется с помощью контроллера домена.

Для создания общего ресурса на любом компьютере, входящем в домен, нужно на контроллере домена открыть консоль управления сервером и перейти в раздел «Общие папки». Далее необходимо подключиться к удаленному компьютеру, на котором будет располагаться общий ресурс. Затем с помощью «Мастера создания общих ресурсов» создать на нем общую папку и настроить для пользователей сетевые разрешения к этой папке.

3.4 Конфликты прав доступа к сетевым ресурсам

При организации общего ресурса, помимо разрешений NTFS, также могут применяться сетевые разрешения, которые слегка отличаются от общих разрешений NTFS. При одновременном использовании и разрешений NTFS, и сетевых разрешений могут появляться, так называемые конфликты прав доступа. Конфликты прав доступа образуются в случае, если разрешения NTFS

и сетевые разрешения противоречат друг другу. В таких случаях в ОС семейства Windows применяется концепция эффективных прав доступа: когда существует несколько списков прав доступа, которые имеют субъекты к объектам, действуют те права доступа, которые есть во всех списках. Также права доступа на запрет сильнее, чем права на разрешения.

Для того чтобы конфликтов прав доступа не возникало, а из-за того что разрешения NTFS более гибкие, чем сетевые разрешения, рекомендуется в сетевых разрешениях устанавливать полный доступ всем пользователям ко всем объектам, а регулирование доступа к ресурсам осуществлять с помощью разрешений NTFS.

4 Разработка лабораторного практикума по изучению механизмов обеспечению безопасности доступа к локальным и сетевым ресурсам в операционных системах семейства Windows

Лабораторный практикум содержит три работы по следующим темам:

- изучение механизмов идентификации и аутентификации в ОС семейства Windows;
- изучение механизмов разграничения доступа к локальным ресурсам в ОС семейства Windows;
- изучение механизмов разграничения доступа к сетевым ресурсам в ОС семейства Windows.

Методические указания к данным работам представлены в приложениях с А по В.

В первой работе обучающиеся должны будут создать в локальной сети несколько учетных записей, затем создать несколько групп пользователей и добавить созданные учетные записи в группы, назначить каждой группе пользователей определенные права и установить политики учетных записей. Также обучающиеся должны будут повторить все предыдущие действия в доменной сети.

Во второй работе обучающиеся должны будут создать несколько учетных записей и групп пользователей, создать несколько папок и файлов и настроить для них разрешения NTFS и особые разрешения. Затем осуществить проверку назначенных разрешений и запретов.

В третьей работе обучающиеся должны будут создать несколько учетных записей, создать для них общую папку на локальном компьютере и настроить права пользователей для созданной общей папки. Проверить назначенные права. Также обучающиеся должны будут повторить все предыдущие действия в доменной сети.

Лабораторный стенд состоит из двух виртуальных машин с установленными операционными системами Windows 7 и Windows Server

2012R2. Данные виртуальные машины объединены в локальную сеть. На ОС Windows Server 2012R2 был установлен и настроен Active Directory и DNS-сервер. Таким образом, виртуальная машина с ОС Windows Server 2012R2 выполняет роль контроллера домена, а виртуальная машина с ОС Windows 7 является рабочей станцией, входящей в домен.

Рекомендуется выполнение данных работ в средстве виртуализации Virtual Box версии 5.1.8 или выше. Выполнение работ в средстве виртуализации было выбрано по следующим причинам:

- для выполнения работ требуется одна рабочая станция, так как на ней можно одновременно запустить виртуальные машины с операционными системами Windows 7 и Windows Server 2012R2;
- для выполнения работ не требуется наличие реальных локальной и доменной сетей, так как данные сети можно воспроизвести с помощью виртуальных машин;
- в средствах виртуализации существует возможность сделать «снимок системы». В таком случае исключается необходимость осуществлять настройку виртуальных машин после каждой проведенной лабораторной работы. Достаточно восстановить исходное состояние системы с помощью «снимка системы».

В качестве средства виртуализации был выбран Virtual Box в связи с тем, что он распространяется бесплатно и обладает всеми необходимыми функциями для выполнения лабораторного практикума.

5 Вредные психофизиологические факторы, влияющие на нервную систему специалиста по защите информации. Методы и средства физической культуры, снижающие их воздействие

Так как специалист по защите информации большую часть времени проводит за компьютером, к вредным психофизиологическим факторам, влияющим на нервную систему специалиста по защите информации, можно отнести [8]:

- интеллектуальные и, эмоциональные и длительные статические нагрузки;
- постоянная концентрация внимания;
- монотонность труда;
- большой объем информации, обрабатываемый в единицу времени;
- повышенный уровень электромагнитного излучения.

Работа за компьютером предполагает переработку большого массива информации и постоянную концентрацию внимания, поэтому при длительной работе за компьютером нередко развивается умственная усталость и нарушение внимания, а также это способствует более быстрому наступлению утомления.

Человек, работающий за компьютером, вынужден все время принимать решения, от которых зависит эффективность его работы. Порой бывает довольно сложно предположить последствия того или иного шага. Поэтому, длительная работа за компьютером, часто является причиной хронического стресса. Также необходимость перерабатывать большое количество неоднородной информации может привести к развитию стресса.

Работа за компьютером нередко поглощает все внимание работающего человека и потому, такие люди часто пренебрегают нормальным питанием и работают впроголодь весь день. Неправильное питание приводит не только к нарушениям работы органов пищеварительного тракта, но и к возникновению минеральной и витаминной недостаточности. Известно, что недостаток

витаминов и минералов негативно сказывается на процессе обмена веществ в организме, что приводит к снижению интеллектуальных способностей человека. Снижение эффективности работы в свою очередь вызывает необходимость находиться еще больше времени за компьютером. Таким образом, образуется своеобразный «порочный круг», в котором длительная работа за компьютером является пусковым моментом определяющим все последующие нарушения.

Повышенный уровень электромагнитного излучения от компьютера может привести к повышенной возбудимости нервной системы, проявляющейся раздражительностью, нарушением сна, эмоциональной неустойчивостью. В последующем может развиваться нервно-психическая слабость. Поэтому при воздействии электромагнитного излучения на организм специалиста по защите информации характерны: головная боль, утомляемость, ухудшение самочувствия. Указанные симптомы могут быть выражены в разной степени.

Для снижения вреда от психофизиологических факторов, влияющих на нервную систему специалиста по защите информации, следует делать регулярные перерывы в работе. Каждые 30 минут работы за компьютером следует делать перерыв на 10 минут.

Во время перерыва необходимо делать упражнения на расслабление, например, при обнаружении таких симптомов, как сонливость или утомляемость, следует делать следующие упражнения:

- круговые движения головой;
- перевод взгляда с ближнего на дальнее расстояние – одним глазом;
- перевод взгляда с ближнего на дальнее расстояние – двумя глазами;
- пальминг.

При обнаружении такого симптома, как головная боль после кропотливой работы, следует делать следующие упражнения:

- круговые движения головы; перевод взгляда с ближайших точек на дальние — одним глазом;
- перевод взгляда из угла в угол;
- пальминг;
- общее потягивание тела;
- пожимание плечами, круговые движения плечами.

При обнаружении такого симптома, как раздражительность во время или после работы, следует делать следующие упражнения:

- напряжение глаз;
- перевод взгляда с ближнего на дальнее расстояние — одним глазом;
- перевод взгляда с ближнего на дальнее расстояние — двумя глазами;
- поочередное фокусирование взгляда на левом и правом углах комнаты;
- пальминг.

Заключение

В ходе выполнения выпускной квалификационной работы были проанализированы основные методы и протоколы идентификации и аутентификации в операционных системах семейства Windows, рассмотрены разрешения NTFS и сетевые разрешения, рассмотрены процессы организации общего доступа на компьютере, входящем в домен, и на компьютере, не входящем в домен. Описано содержание лабораторного стенда для проведения лабораторного практикума, разработаны рекомендации и варианты заданий для проведения лабораторного практикума. Также были разработаны методические указания для проведения лабораторного практикума, включающего в себя три работы по следующим темам:

- изучение механизмов идентификации и аутентификации в ОС семейства Windows;
- изучение механизмов разграничения доступа к локальным ресурсам в ОС семейства Windows;
- изучение механизмов разграничения доступа к сетевым ресурсам в ОС семейства Windows.

В заключение были исследованы вредные психофизиологические факторы, влияющих на нервную систему специалиста по защите информации, а также методы и средства физической культуры, снижающие их воздействие.

Таким образом, задание на выпускную квалификационную работу выполнено в полном объеме.

Список используемых источников

- 1 Протоколы Lan Manager и NT // Студопедия. URL: <https://studopedia.info/2-5402.html> (дата обращения: 12.11.2017).
- 2 Microsoft Ntlm // Microsoft: официальный сайт. URL: [https://msdn.microsoft.com/ru-ru/library/windows/desktop/aa378749\(v=vs.85\).aspx](https://msdn.microsoft.com/ru-ru/library/windows/desktop/aa378749(v=vs.85).aspx) (дата обращения: 14.11.2017).
- 3 Аутентификация в системах Windows. Часть 1 // Записки IT специалиста. Технический блог специалистов ООО «Интерфейс» URL: https://interface31.ru/tech_it/2015/03/autentifikaciya-v-sistemah-windows-chast-1-ntlm.html (дата обращения: 15.11.2017).
- 4 NTLM не умер, он просто так пахнет, А. Карпов // SecurityLab.ru URL: <https://www.securitylab.ru/analytics/362448.php> (дата обращения: 20.11.2017).
- 5 Атаки SMB Relay и контроль NTLMv2 с помощью Python, М. Баггетт // SecurityLab.ru URL: <https://www.securitylab.ru/analytics/442313.php> (дата обращения: 20.11.2017).
- 6 Аутентификация в системах Windows. Часть 2 // Записки IT специалиста. Технический блог специалистов ООО «Интерфейс» URL: https://interface31.ru/tech_it/2016/07/autentifikaciya-v-sistemah-windows-2-kerberos.html (дата обращения: 29.11.2017).
- 7 Приказ ФСТЭК России от 18 февраля 2013 г. №21 // ФСТЭК России: официальный сайт. URL: <https://fstec.ru/normotvorcheskaya/akty/53-prikazy/691-prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21> (дата обращения: 08.12.2017).
- 8 Основные вредные факторы, влияющие на состояние здоровья людей работающих за компьютером // Медпортал.com. URL: http://xn--80ahc0abogjs.com/valeologiya_739/osnovnyie-vrednyie-factoryi-vliiyayuschie.html (дата обращения: 08.01.2018).

Приложение А

(обязательное)

Лабораторная работа №1 «Изучение механизмов идентификации и аутентификации в ОС семейства Windows»

Лабораторная работа №1 «Изучение механизмов идентификации и аутентификации в ОС семейства Windows»

А.1 Цель и задание на лабораторную работу

Цель работы – получить навыки настройки механизмов идентификации и аутентификации в ОС семейства Windows, включающие:

- создание учетных записей локальных и доменных пользователей;
- настройку блокировок, связанных с функционированием подсистемы контроля входа.

Задание на лабораторную работу включает в себя:

- создание учетных записей локальных и доменных пользователей;
- создание групп пользователей в локальной и доменной системах;
- настройку локальных параметров безопасности;
- настройку политики паролей;
- настройку политики блокировки учетных записей;
- имитацию событий НСД, возникающих при входе пользователей;
- вывод о проделанной работе.

А.2 Порядок выполнения лабораторной работы

А.2.1 Подготовка к выполнению лабораторной работы

А.2.1.1 Для выполнения лабораторной работы в VirtualBox необходимо запустить виртуальные машины с именами Windows 7 и Windows Server 2012R2.

Для этого откройте папку *LabWork1* на рабочем столе, и запустите виртуальную машину, дважды щелкнув по ярлыкам *Windows 7* и *Windows Server 2012R2*. Откроются окна виртуальных машин. Подождите, пока загрузится операционная система и появится приглашение для входа в систему.

Все последующие действия, связанные с управлением локальными учетными записями, выполняются на виртуальной машине с операционной системой Windows 7.

А.2.1.2 Осуществить вход в систему используя локальную учетную запись администратора.

Для этого после появления диалогового окна, показанного на рисунке А.1, необходимо выбрать пользователя *admin*. Так как пароль для данной учетной записи не установлен, сразу будет выполнен вход в систему.



Рисунок А.1 – Диалог входа в систему

А.2.2 Управление локальными учетными записями

А.2.2.1 Создание учетной записи локального пользователя.

Создайте учетные записи пользователей в соответствии с вариантом задания, представленным в таблице А.1. Данная таблица приведена в конце методических указаний.

Для создания учетной записи откройте меню *Пуск*, правой кнопкой мыши щелкните на записи *Мой компьютер* и в контекстном меню выберите *Управление*. Откроется консоль «Управление компьютером», как показано на рисунке А.2.

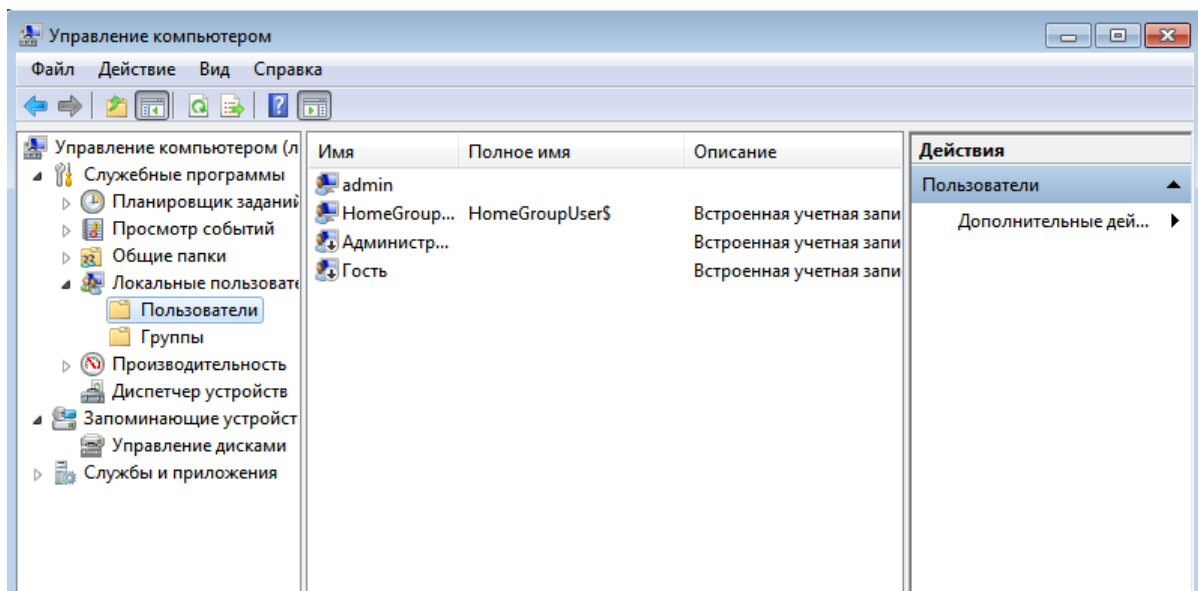


Рисунок А.2 – Консоль «Управление компьютером»

В левой части окна перейдите в папку *Локальные пользователи и группы/Пользователи*. В правой части окна щелчком правой кнопки мыши откройте контекстное меню и выберите пункт меню *Новый пользователь....* Откроется диалоговое окно создания нового пользователя, показанный на рисунке А.3.

Введите имя пользователя, согласно варианту задания, полное имя, описание пользователя (для первого пользователя – бухгалтер, для второго – секретарь, для третьего - программист), укажите пароль и подтвердите пароль, введя его повторно, оставьте значения остальных органов управления в значении по умолчанию. Пароль должен удовлетворять требованиям, приведенным в таблице А.1.

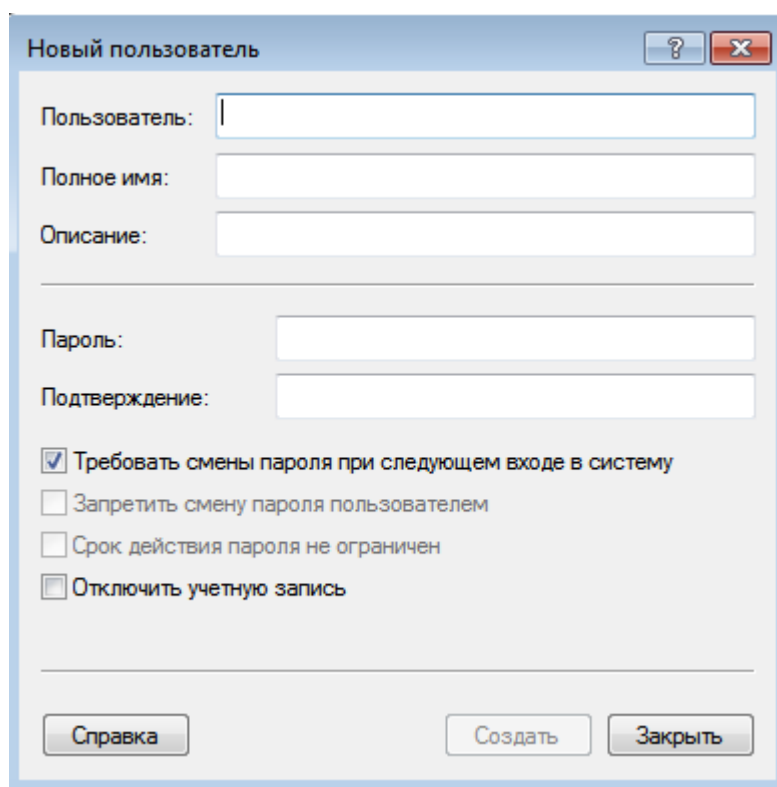


Рисунок А.3 – Диалоговое окно создания нового пользователя

После заполнения необходимых полей, нажмите кнопку *Создать*, после чего можете вводить данные следующего создаваемого пользователя. После создания всех пользователей нажмите кнопку *Закреть*.

Для того чтобы проверить новую учетную запись выйдите из системы и войдите в нее, используя новую учетную запись. Для этого в меню *Пуск* выберите *Выход из системы*.

В появившемся диалоговом окне, представленном на рисунке А.4, нажмите кнопку *Сменить пользователя*. Затем нажмите кнопку *Другой пользователь*.

После этого появится диалоговое окно, представленное на рисунке А.5.

Введите имя локального пользователя в виде *ADMIN-PC\Имя пользователя* и пароль пользователя. При вводе пароля обратите внимание на выбранную раскладку клавиатуры. После ввода пароля нажмите клавишу *Enter*, появится диалоговое окно смены пароля, представленное на рисунке А.6.



Рисунок А.4 – Диалоговое окно входа в систему

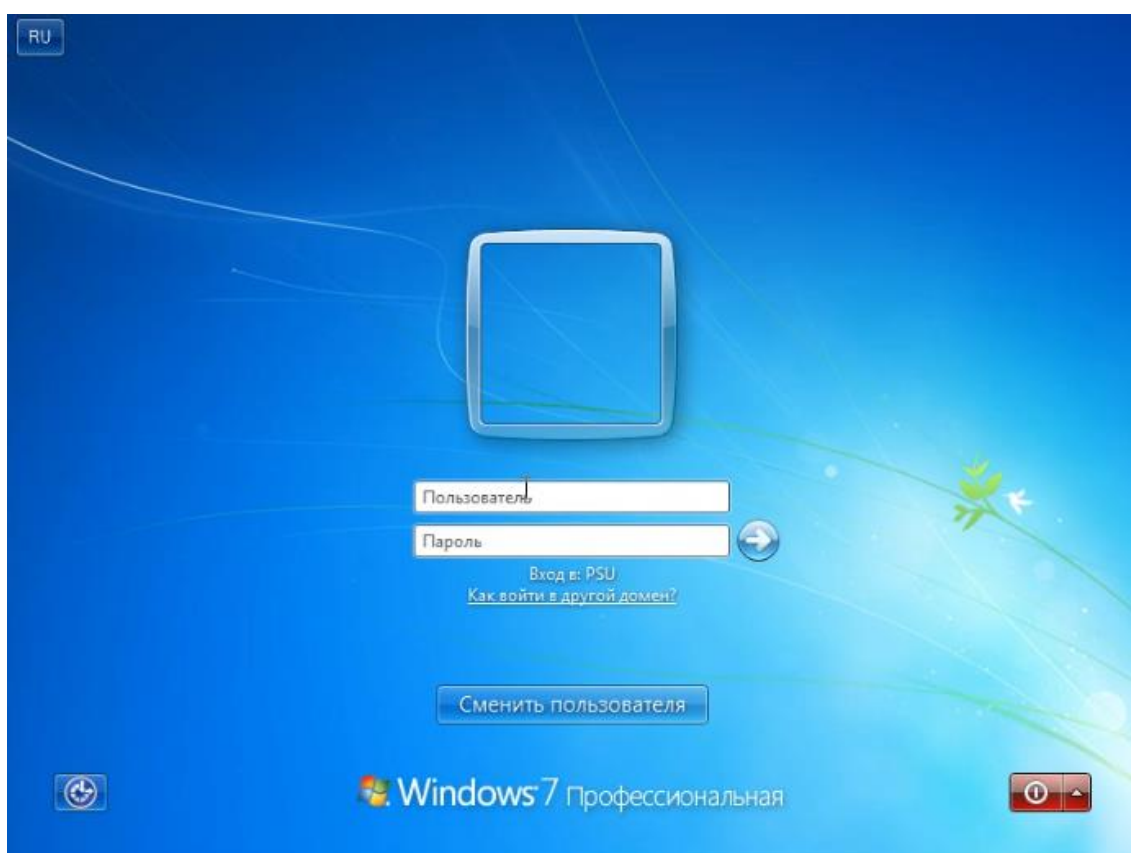


Рисунок А.5 – Диалоговое окно смены пользователя

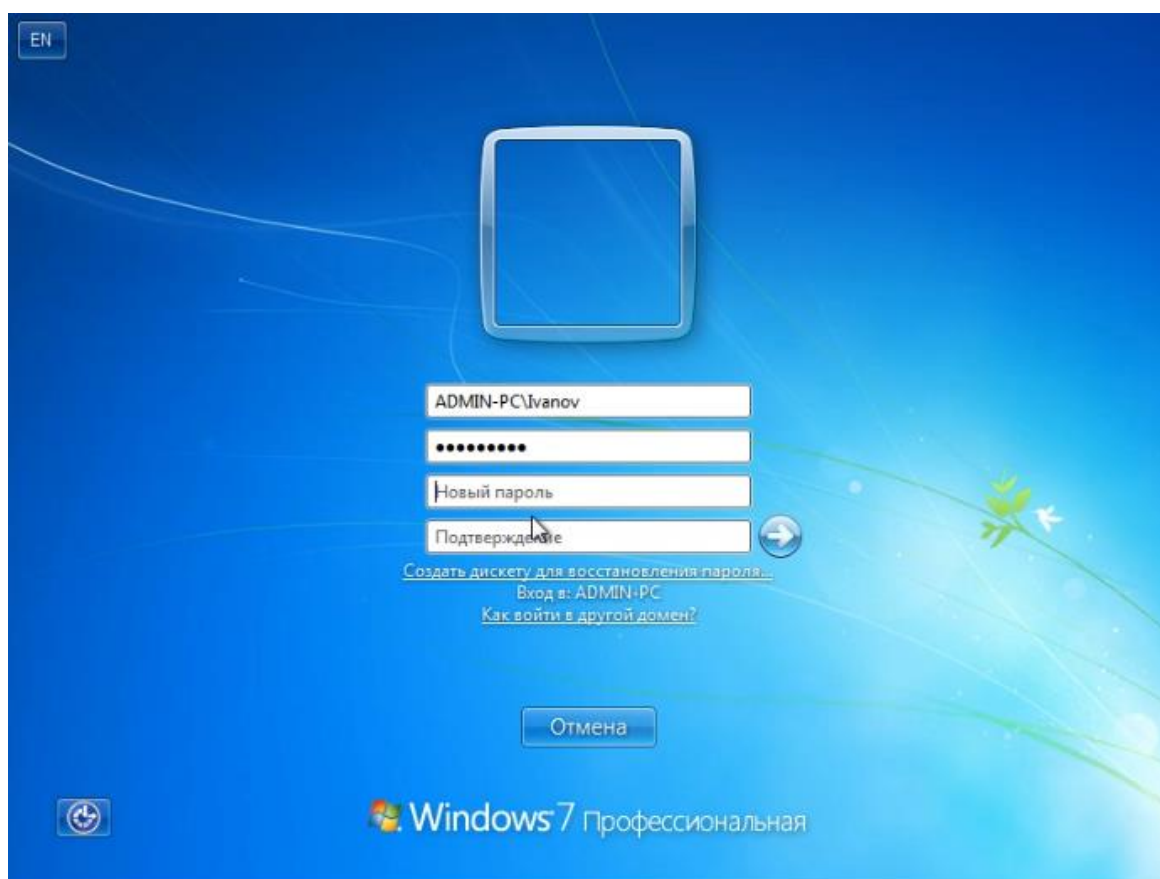


Рисунок А.6 – Диалоговое окно смены пароля при первом входе в систему

Укажите новый пароль и подтвердите пароль, введя его повторно. Пароль должен удовлетворять требованиям, приведенным в таблице А.1.

После успешной смены пароля отобразится рабочий стол пользователя.

А.2.2.2 Создание группы пользователей на локальном компьютере.

Для создания новой группы откройте консоль «Управление компьютером» и перейдите в папку *Локальные пользователи и группы/Группы*, как показано на рисунке А.7.

В правой части окна щелчком правой кнопки мыши откройте контекстное меню и выберите пункт *Создать группу...*. Откроется диалоговое окно создания новой группы, представленное на рисунке А.8.

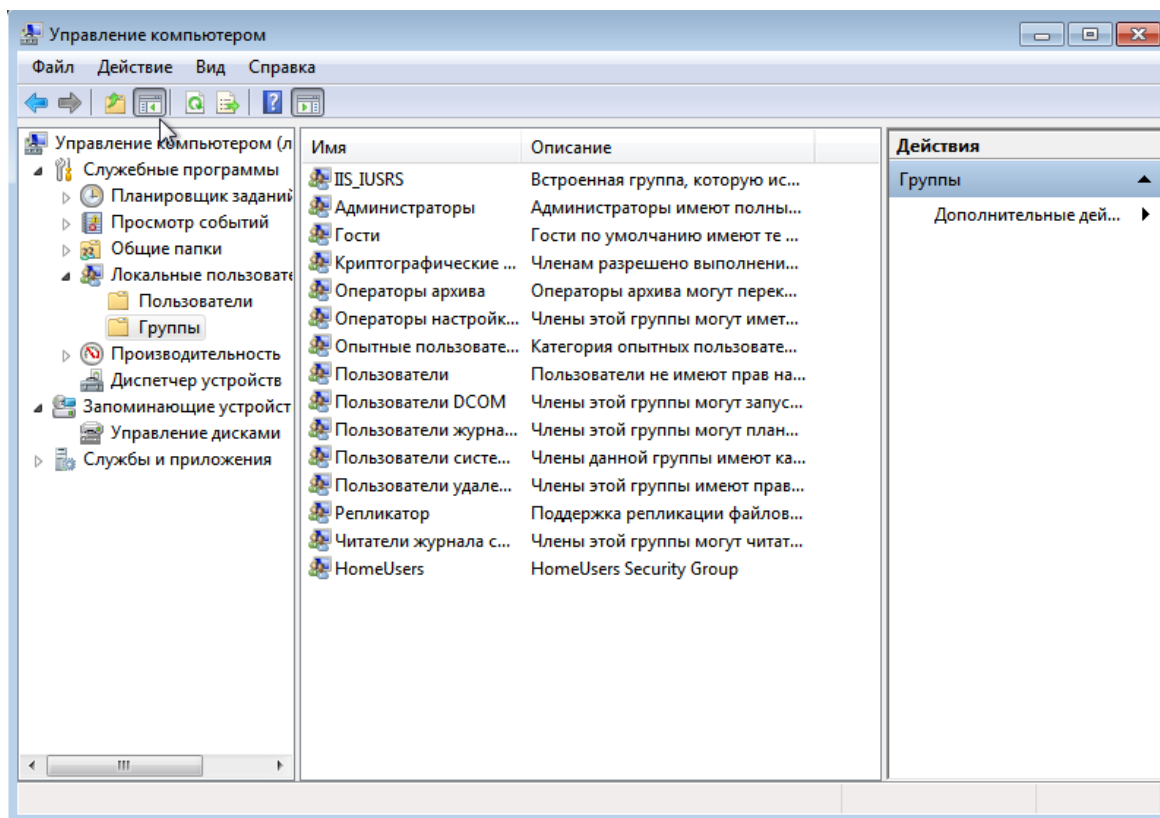


Рисунок А.7 – Консоль «Управление компьютером», категория Группы

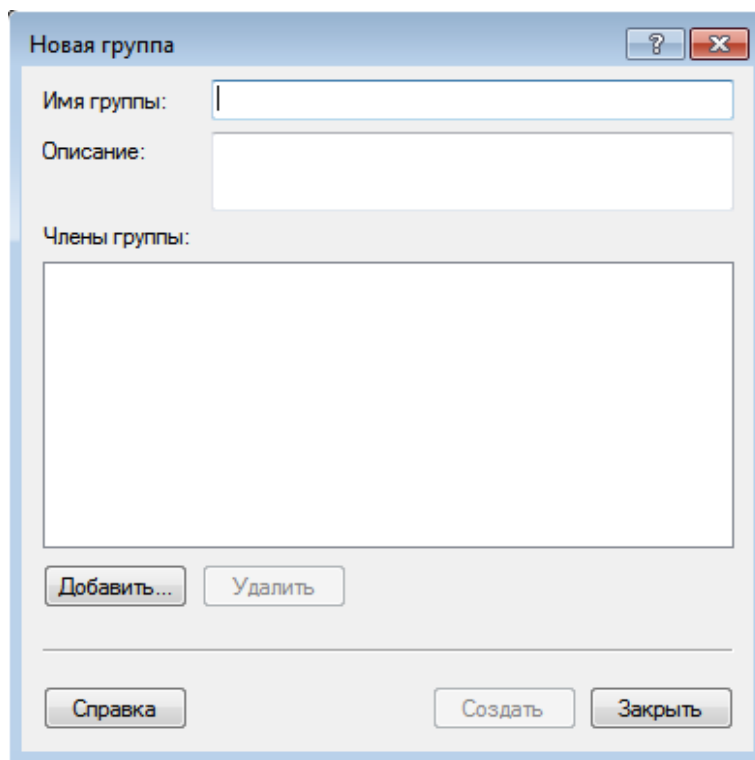


Рисунок А.8 – Диалоговое окно создания новой группы

Введите имя группы *Бухгалтерия* и ее описание. Нажмите кнопку *Добавить...* Откроется диалоговое окно выбора пользователей, представленное на рисунке А.9.

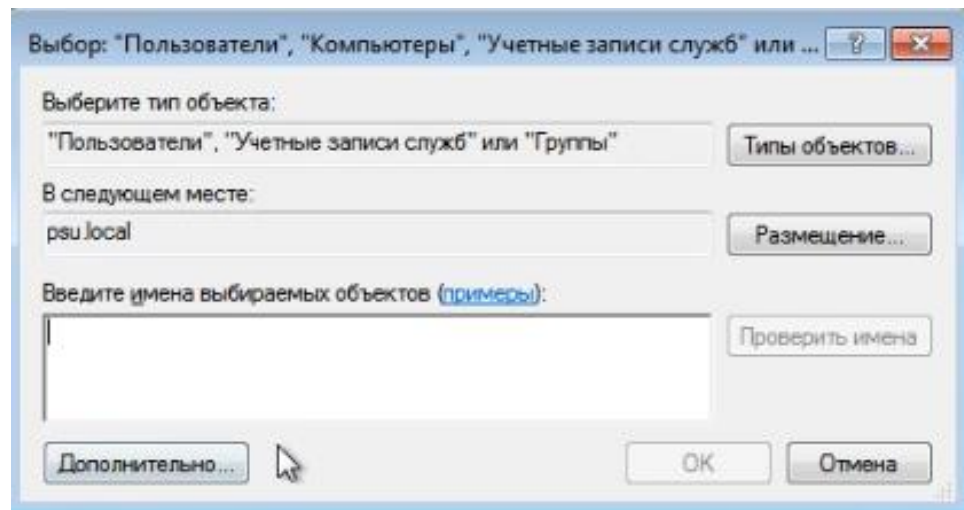


Рисунок А.9 – Диалоговое окно выбора пользователей группы

Нажмите кнопку *Размещение*, появится диалоговое окно контроля учетных записей, представленное на рисунке А.10.

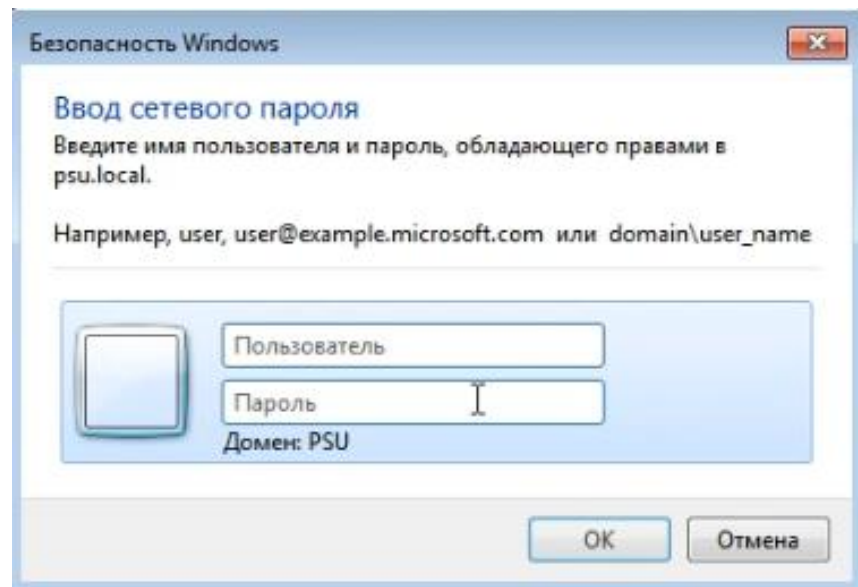


Рисунок А.10 – Диалоговое окно контроля учетных записей пользователей

Нажмите кнопку *Отмена*, после чего откроется диалоговое окно, представленное на рисунке А.11. Еще раз нажмите кнопку *Размещение....* В появившемся списке выберите ADMIN-PC.

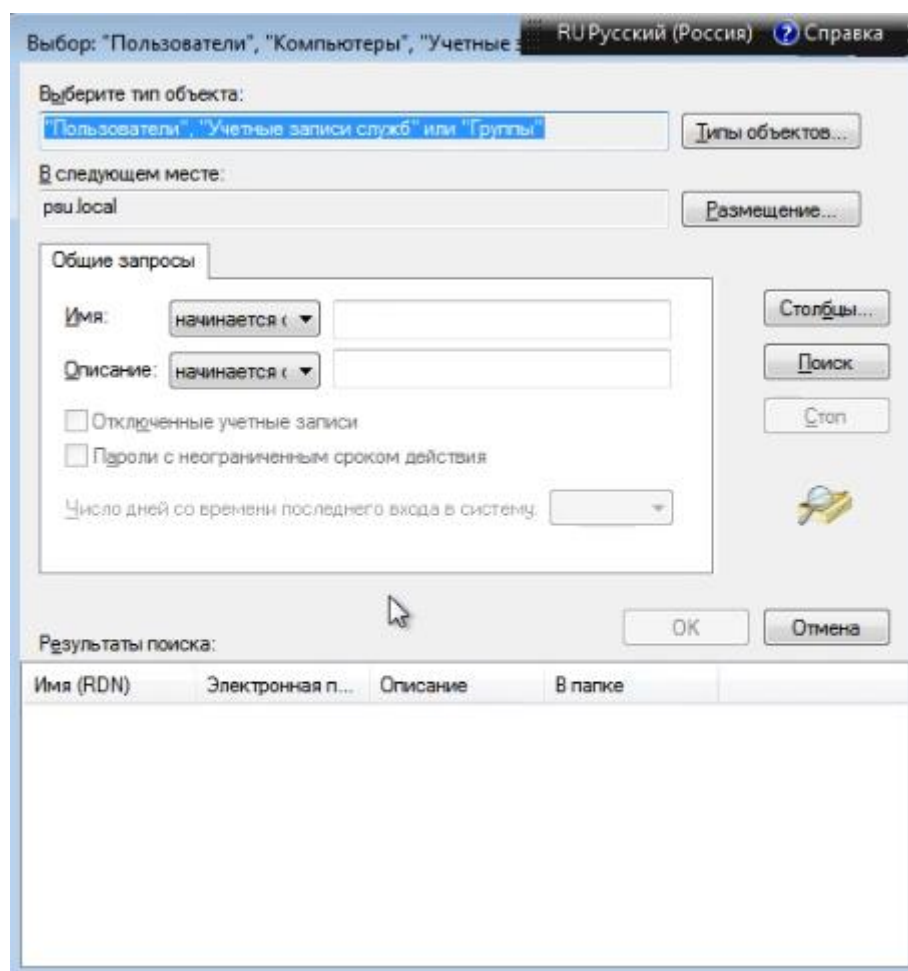


Рисунок А.11 – Диалоговое окно

Введите имена первого и второго пользователей, созданных на предыдущем этапе выполнения лабораторной работы, через точку с запятой.. Нажмите кнопку *Проверить имена*. Система выполнит поиск имен пользователей в базе данных учетных записей. Корректные имена пользователей будут выделены подчеркиванием. Если имя пользователя написано с ошибкой, система отобразит сообщение об ошибке.

Нажмите кнопку *OK*. Диалоговое окно выбора пользователей закроется.

В диалоговом окне создания новой группы нажмите кнопку *Создать*, будет создана новая группа.

Создайте группу *IT-Отдел* и добавьте в нее третьего пользователя, созданного на предыдущем этапе выполнения лабораторной работы.

Для выбора имен пользователей также можно воспользоваться поиском. Для этого нажмите кнопку *Дополнительно...*, после чего откроется диалоговое окно, представленное на рисунке А.12.

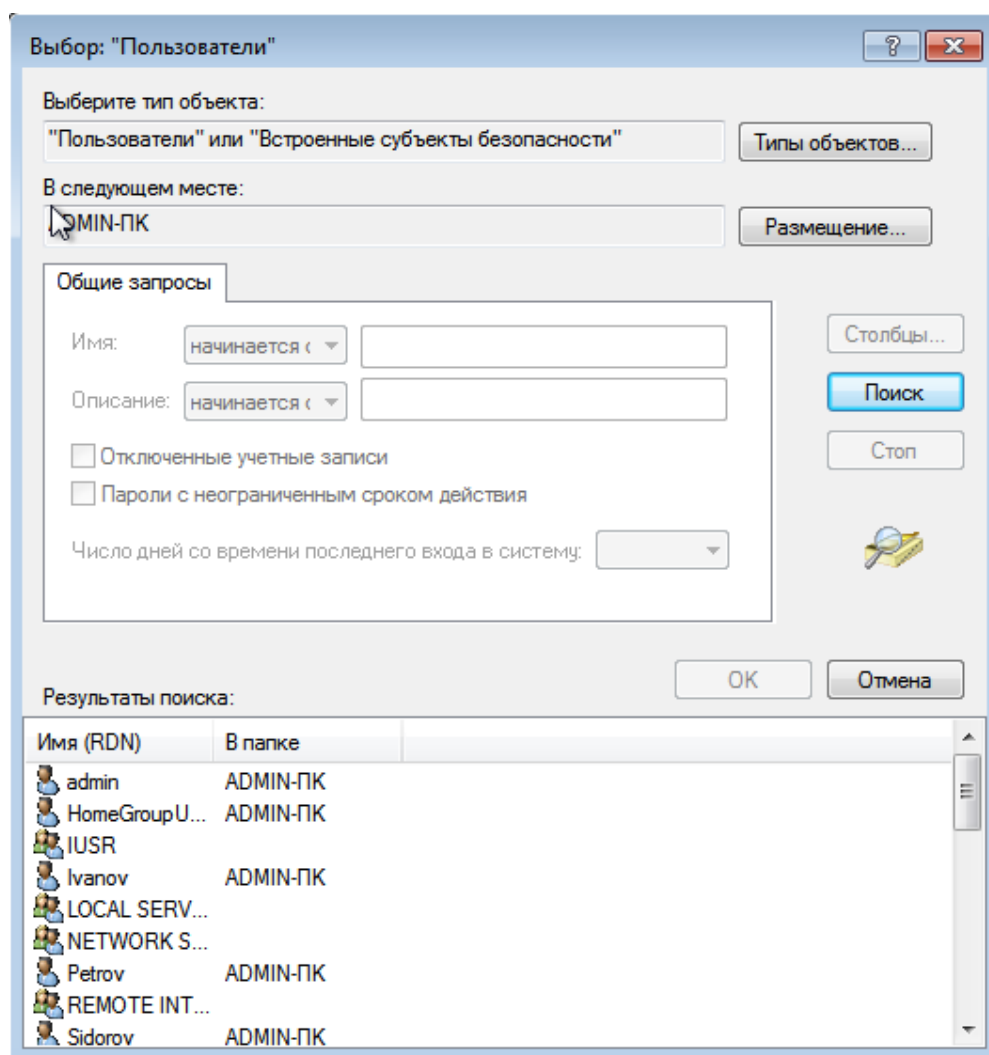


Рисунок А.12 – Диалоговое окно «Выбор: Пользователи»

Нажмите кнопку *Поиск*, после чего выберите в результатах поиска имя третьего пользователя, созданного на предыдущем этапе выполнения лабораторной работы, и нажмите кнопку *OK*.

Нажмите кнопку *OK*. Диалоговое окно выбора пользователей закроется.

В диалоговом окне создания новой группы нажмите кнопку *Создать*, будет создана новая группа.

А.2.2.3 Управление локальными параметрами безопасности.

В меню *Пуск* выберите *Панель управления*, в правом верхнем углу окна во вкладке *Просмотр* выберите *Крупные значки*, далее выберите

Администрирование, а затем *Локальная политика безопасности*. Откроется консоль «Локальные параметры безопасности», как показано на рисунке А.13.

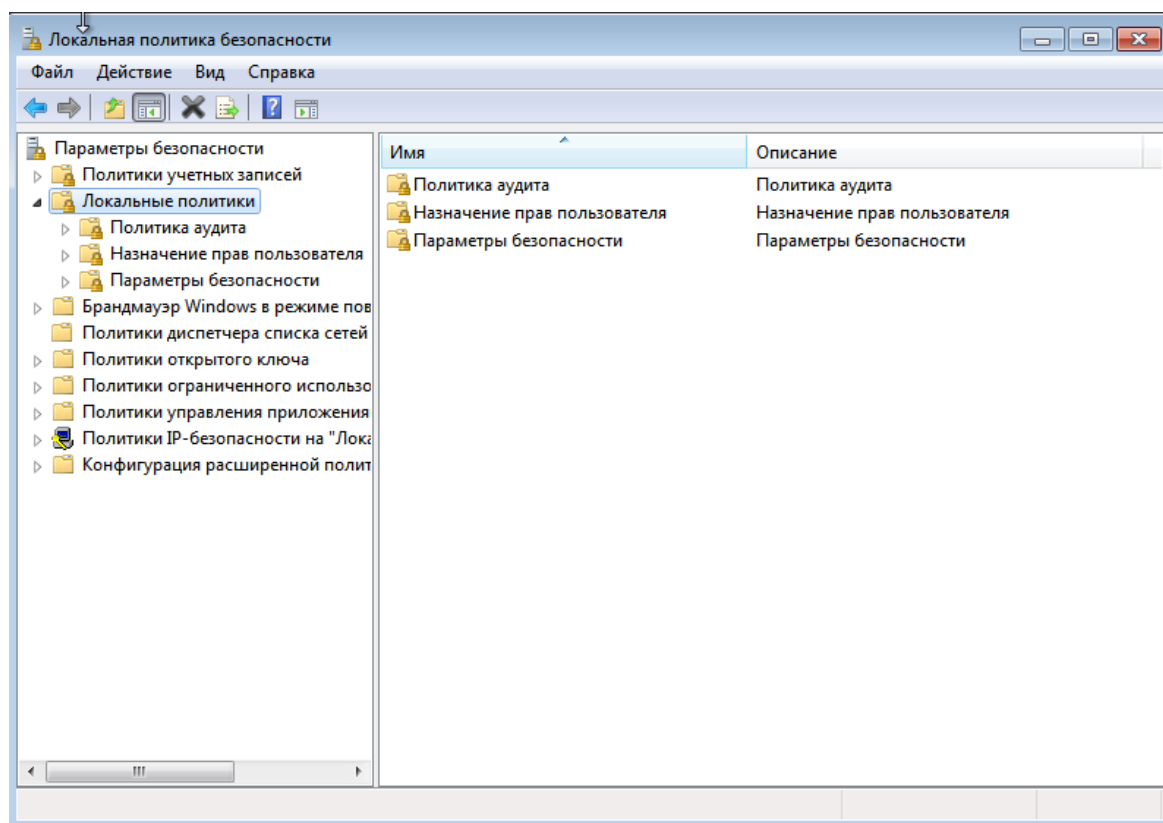


Рисунок А.13 – Консоль «Локальные параметры безопасности»

Выберите папку *Локальные политики/Назначение прав пользователя*. В правой части окна двойным щелчком откройте запись *Изменение системного времени*, откроется диалоговое окно изменения значения данного параметра, представленное на рисунке А.14.

По умолчанию только члены групп Администраторы и LOCAL SERVICE могут изменять системное время. Нажмите кнопку *Добавить пользователя или группу*.... Откроется диалоговое окно выбора пользователей или групп, представленное на рисунке А.15. Нажмите кнопку *Размещение*..., появится диалоговое окно контроля учетных записей. Нажмите кнопку *Отмена*, после чего откроется диалоговое окно. Еще раз нажмите кнопку *Размещение*.... В появившемся списке выберите ADMIN-PC.

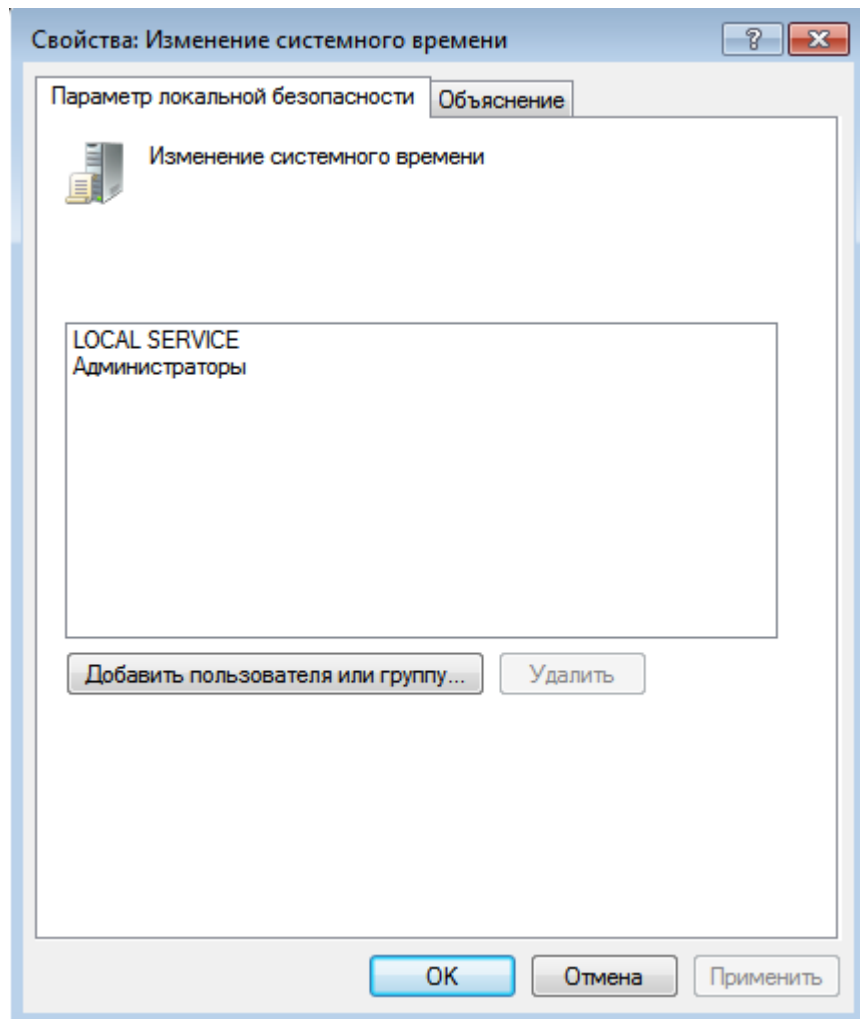


Рисунок А.14 – Диалоговое окно изменения системного времени

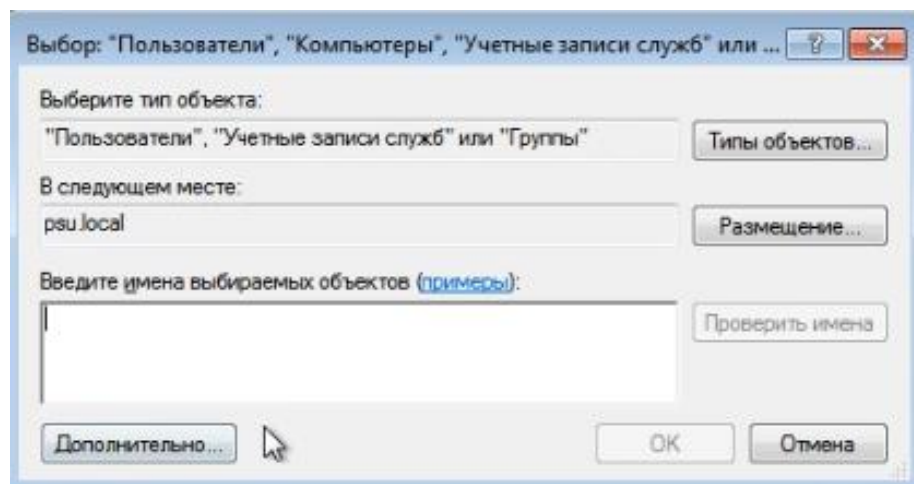


Рисунок А.15 – Диалоговое окно выбора пользователей или групп

В данном диалоговом окне нажмите кнопку *Типы объектов...*. В диалоговом окне выбора типов объектов выберите *Группы*, как показано на рисунке А.16, и нажмите *ОК*.

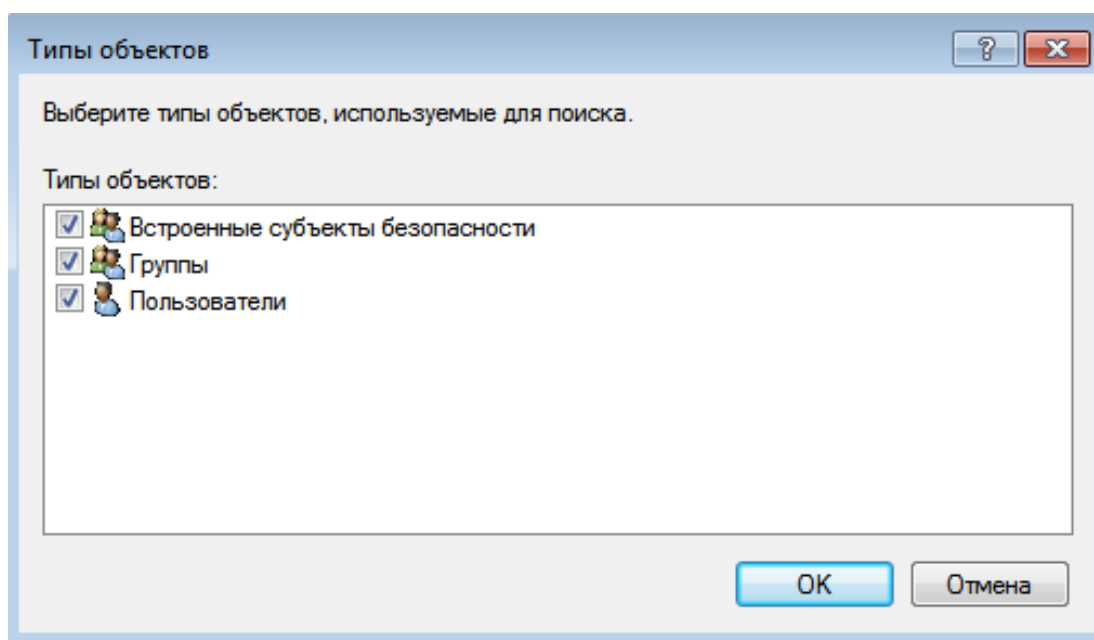


Рисунок А.16 – Диалоговое окно выбора типов объектов

В диалоговом окне выбора пользователей или групп добавьте группу пользователей ИТ-Отдел. Для этого введите имя группы или воспользуйтесь поиском и нажмите *ОК*. Группа будет добавлена в список объектов.

В диалоговом окне изменения системного времени нажмите кнопку *Применить*. Теперь членам этой группы будет разрешено изменять системное время. Нажмите *ОК*.

А.2.2.4 Проверка установленных параметров.

Для того чтобы проверить установленные параметры выйдите из системы и попробуйте войти в систему под учетной записью второго пользователя, введя неверный пароль. Должно появиться диалоговое окно, показанное на рисунке А.17.

Затем войдите в систему под учетной записью второго пользователя, введя верный пароль. Попробуйте изменить системное время. Для этого на рабочем столе щелкните правой кнопкой мыши по системному времени, расположенному в правом нижнем углу, и выберите вкладку *Настройка даты и времени*. В появившемся диалоговом окне, представленном на рисунке А.18, щелкните кнопку *Изменить дату и время*. Должно появиться диалоговое окно контроля учетных записей пользователей. Данное диалоговое окно означает, что у второго пользователя нет прав на выполнение действия *Изменение*

системного времени и ему требуется разрешение администратора на выполнение данного действия.

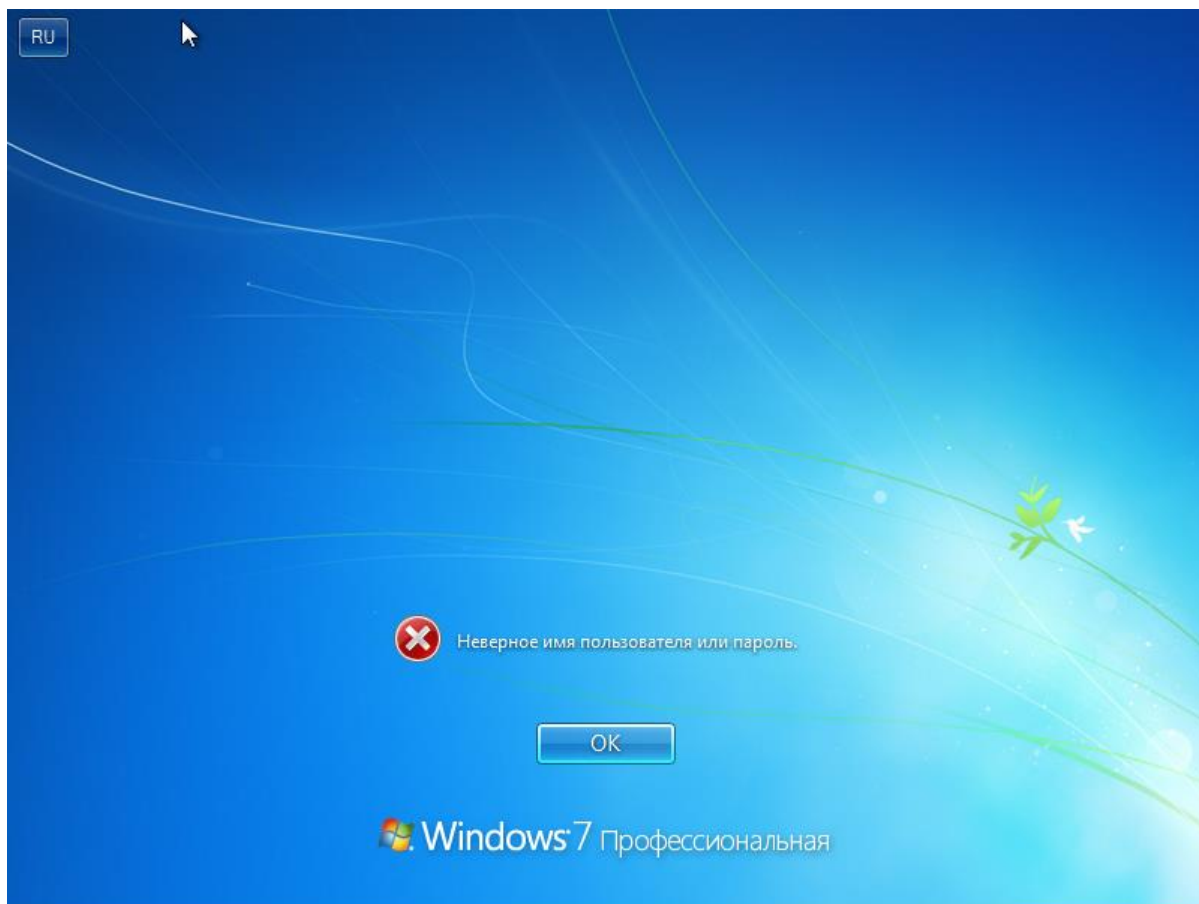


Рисунок А.17 – Диалоговое окно неверного ввода пароля

Выйдите из системы, а затем войдите под учетной записью третьего пользователя. Попробуйте изменить системное время. Должно появиться диалоговое окно, показанное на рисунке А.19. Данное диалоговое окно означает, что у третьего пользователя есть права на выполнение действия *Изменение системного времени*.

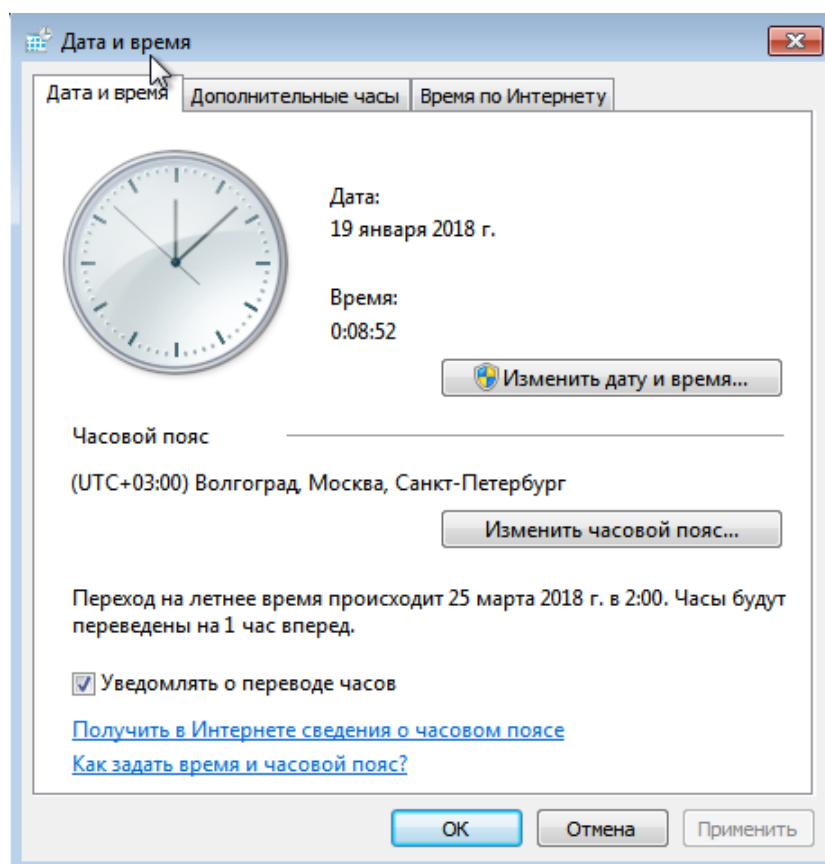


Рисунок А.18 – Диалоговое окно «Дата и время»

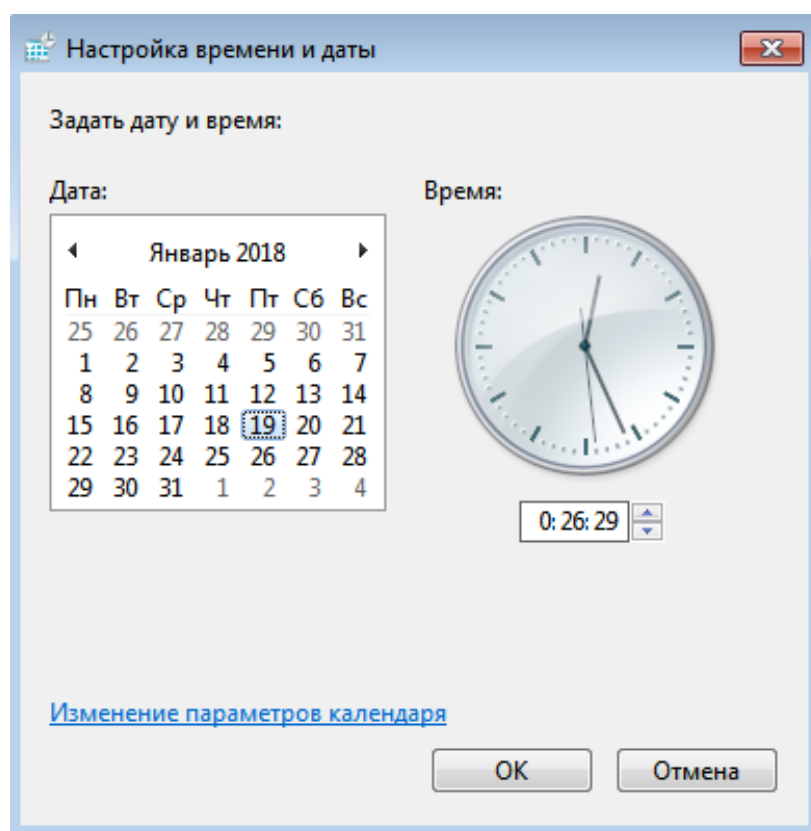


Рисунок А.19 – Диалоговое окно настройки системного времени

А.2.3 Управление доменными учетными записями

А.2.3.1 Создание учетных записей пользователей на контроллере домена.

Для создания учетных записей пользователей на контроллере домена потребуется виртуальная машина с операционной системой Windows Server 2012R2.

Войдите в систему на контроллере домена под учетной записью администратора. Для этого выберите учетную запись PSU\Администратор и введите пароль *Qwerty123*.

Откройте консоль «Диспетчер серверов». В правом верхнем углу откройте вкладку *Средства* и выберите пункт *Пользователи и компьютеры Active Directory*, появится диалоговое окно, представленное на рисунке А.20.

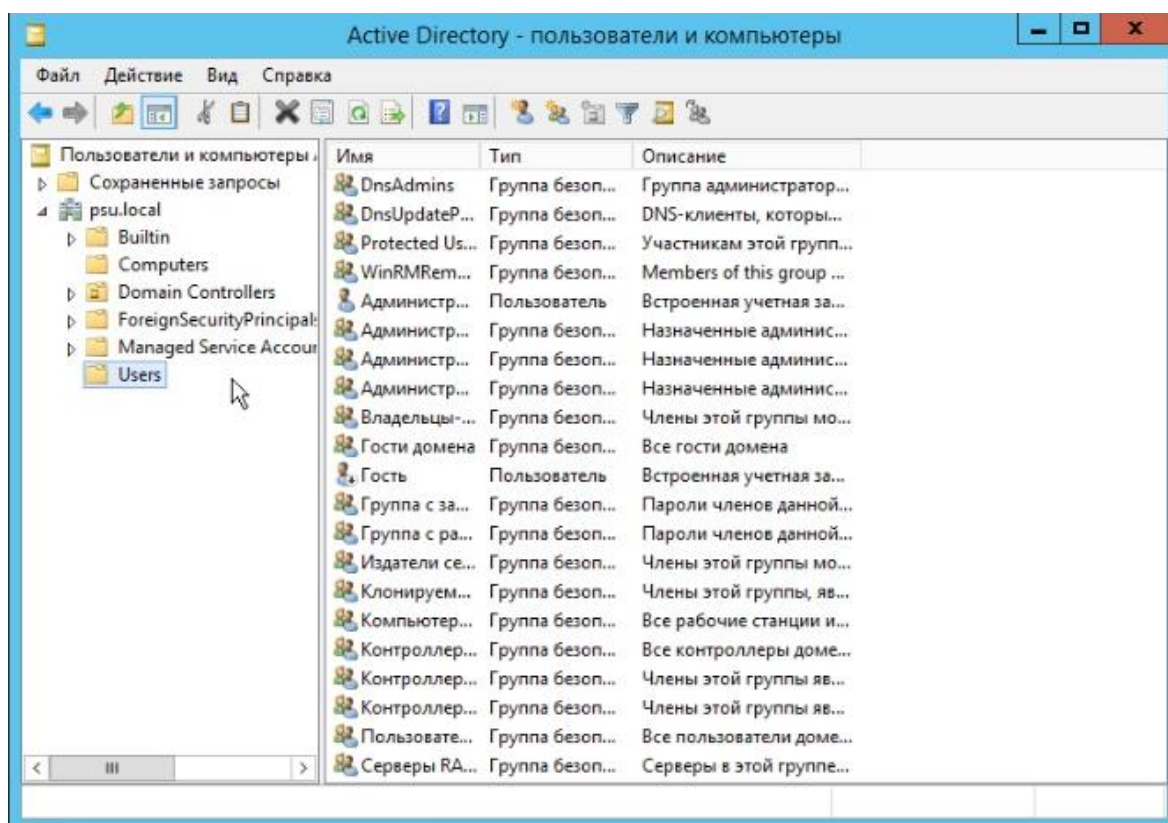


Рисунок А.20 – Диалоговое окно Active Directory – пользователи и компьютеры

В правой части окна щелкните правой кнопкой мыши и выберите *Создать/Пользователь*, появится диалоговое окно создания пользователя, представленное на рисунке А.21.

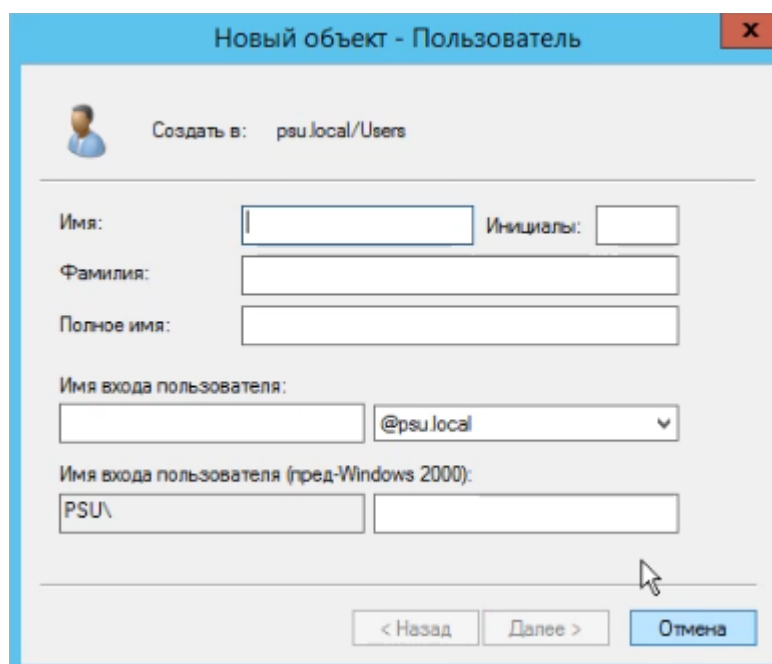


Рисунок А.21 – Диалоговое окно создания пользователя в домене

Заполните поля *Имя*, *Фамилия* и *Имя входа пользователя* и нажмите кнопку *Далее*. Появится окно создания пароля, укажите пароль и подтвердите его. Уберите галочку с пункта *Требовать смены пароля при следующем входе в систему* и поставьте галочки в пунктах *Запретить смену пароля пользователем* и *Срок действия пароля не ограничен*. Таким образом, создайте три учетные записи доменных пользователей, согласно варианту задания.

А.2.3.2 Создание группы пользователей на контроллере домена.

Создайте две группы пользователей Бухгалтерия и IT-Отдел. Для этого в диалоговом окне *Active Directory – пользователи и компьютеры* в правой части окна щелкните правой кнопкой мыши и выберите *Создать/Группа*, появится диалоговое окно создания группы, представленное на рисунке А.22.

В поле *Имя группы* введите имя создаваемой группы и щелкните кнопку *ОК*.

Добавьте первого и второго пользователей в группу Бухгалтерия, а третьего пользователя и администратора – в группу IT-Отдел. Для этого щелкните правой кнопкой мыши по названию группы и выберите пункт *Свойства*. Появится диалоговое окно, представленное на рисунке А.23.

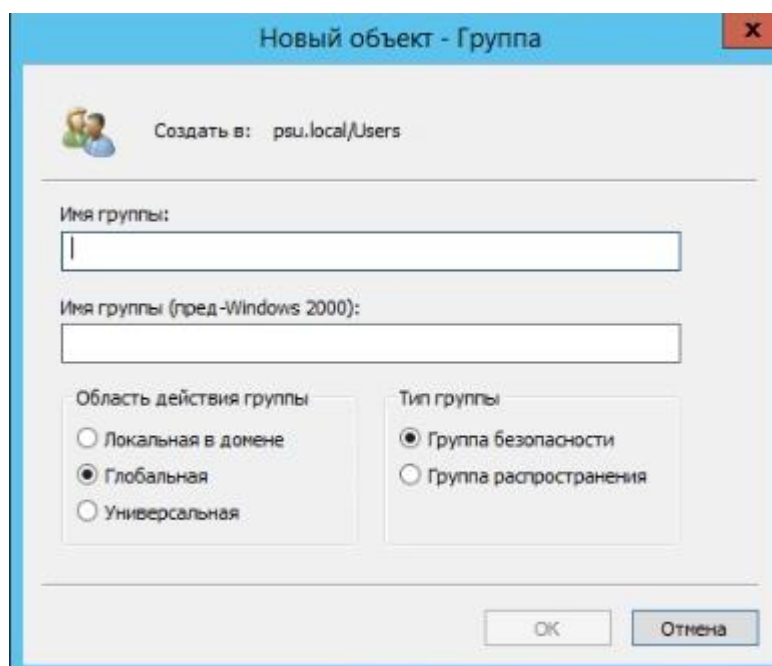


Рисунок А.22 – Диалоговое окно создания группы

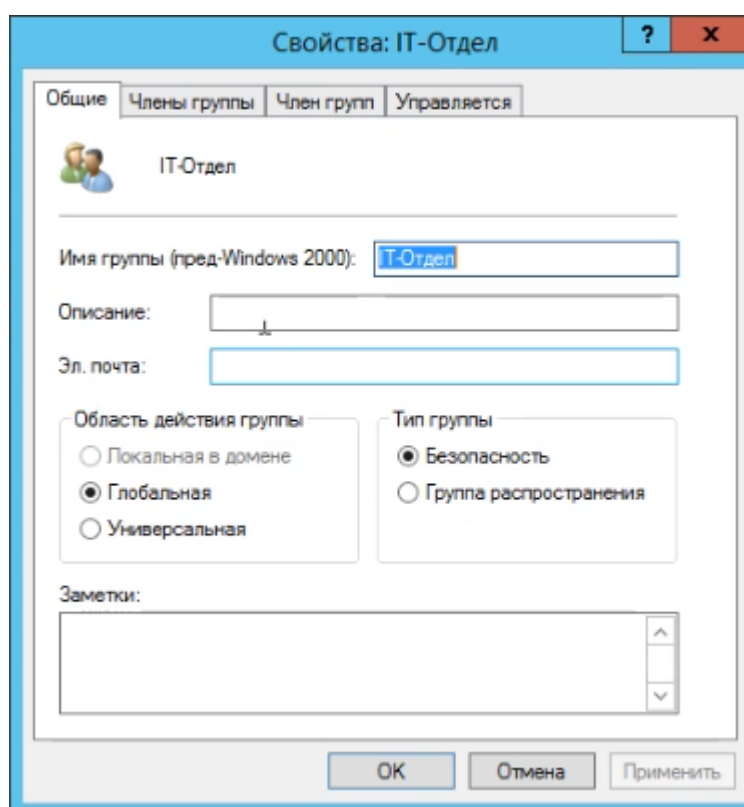


Рисунок А.23 – Диалоговое окно свойств группы

Перейдите во вкладку *Члены группы* и нажмите кнопку *Добавить*.
Откроется диалоговое окно, показанное на рисунке А.24.

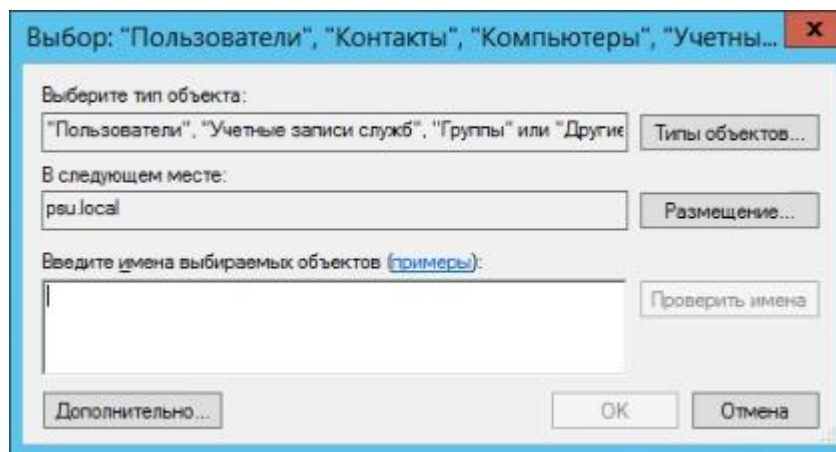


Рисунок А.24 – Диалоговое окно выбора пользователей

Нажмите кнопку *Дополнительно...*, а затем кнопку *Поиск*. В приведенном списке выберите нужных пользователей и нажмите *ОК*. Нажмите *ОК* еще раз. Затем нажмите кнопку *Применить* и выйдите из диалогового окна свойств группы.

А.2.3.3 Управление политиками учетных записей.

Установите для пользователей домена пороговое значение блокировки учетной записи. Для этого на контроллере домена откройте консоль «Диспетчер Серверов». В правом верхнем углу откройте вкладку *Средства* и выберите пункт *Управление групповой политикой*, появится диалоговое окно, представленное на рисунке А.25.

Перейдите по пути Лес:psu.local/Домены/psu.local. Найдите вкладку *Default domain*, щелкните по ней правой кнопкой мыши и выберите пункт *Изменить....* Откроется диалоговое окно, показанное на рисунке А.26.

Перейдите по пути Конфигурация компьютера/Политики/Конфигурация Windows/Параметры безопасности/Политики учетных записей/Политика блокировки учетной записи. В правой части окна выберите пункт *Пороговое значение блокировки*. Откроется диалоговое окно, представленное на рисунке А.27.

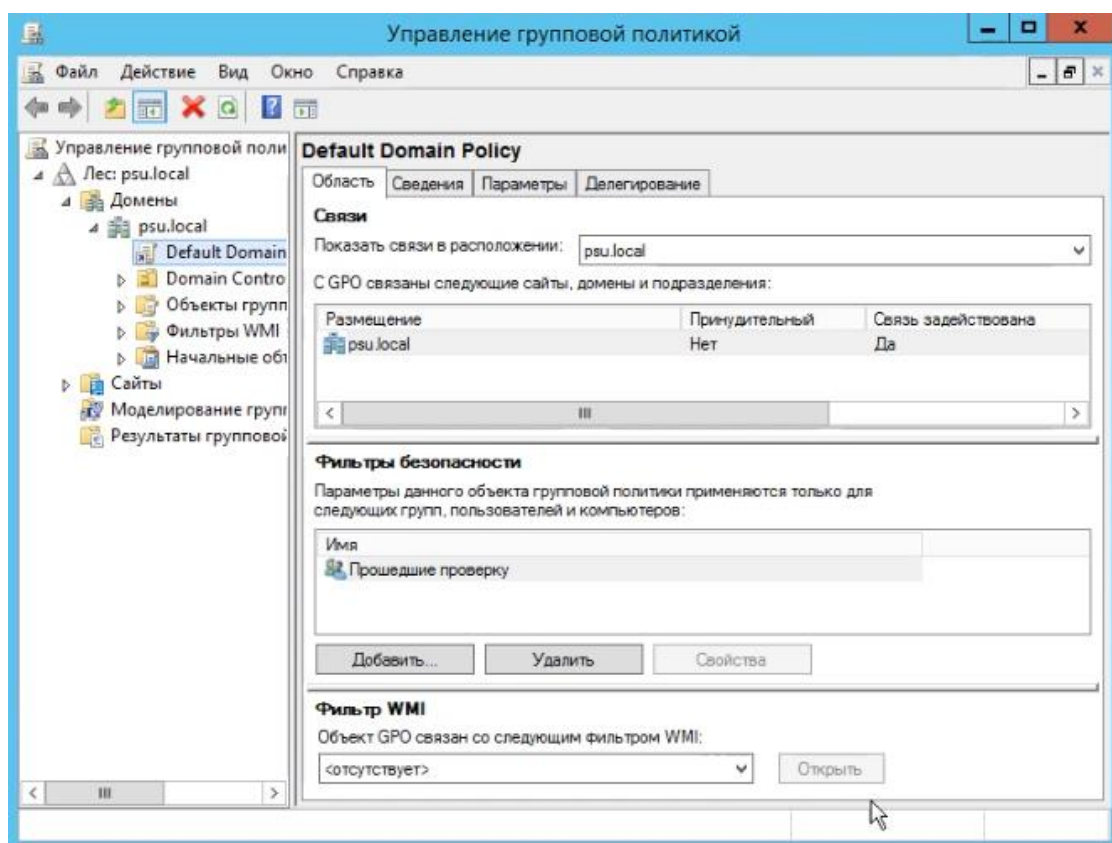


Рисунок А.25 – Диалоговое окно управления групповой политикой

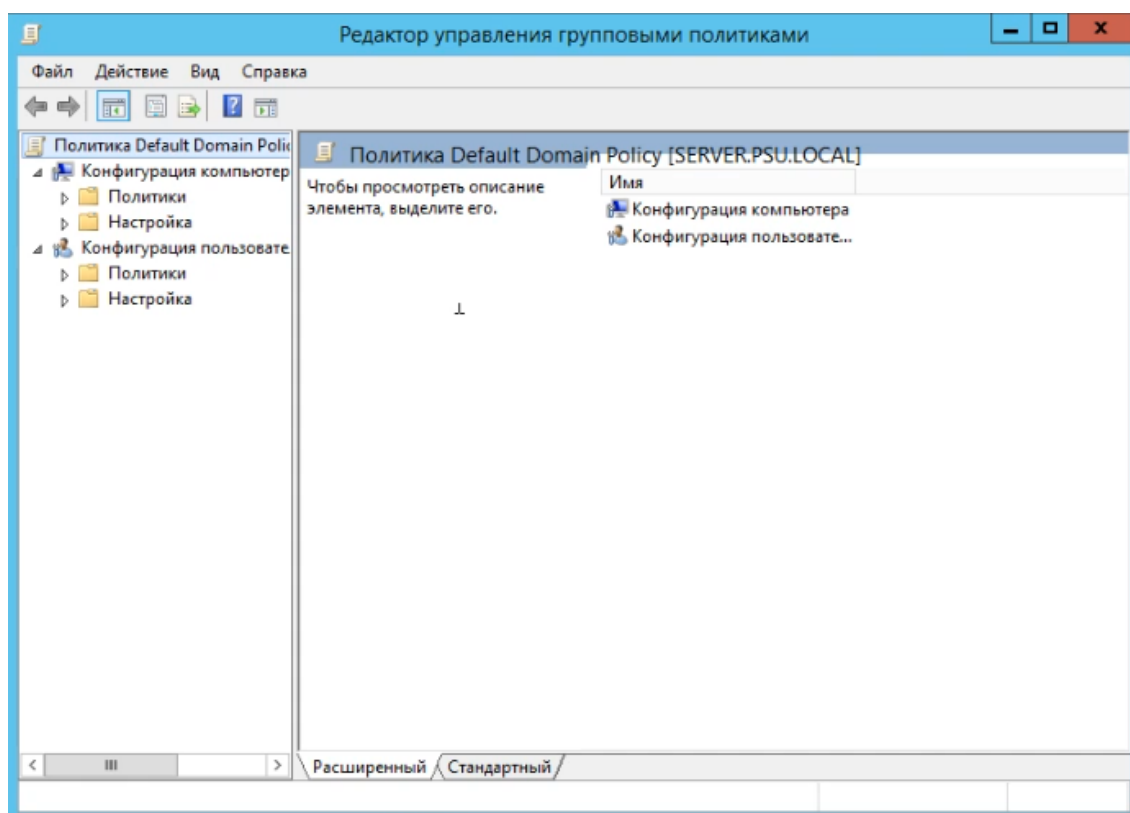


Рисунок А.26 – Диалоговое окно редактора управления групповыми политиками

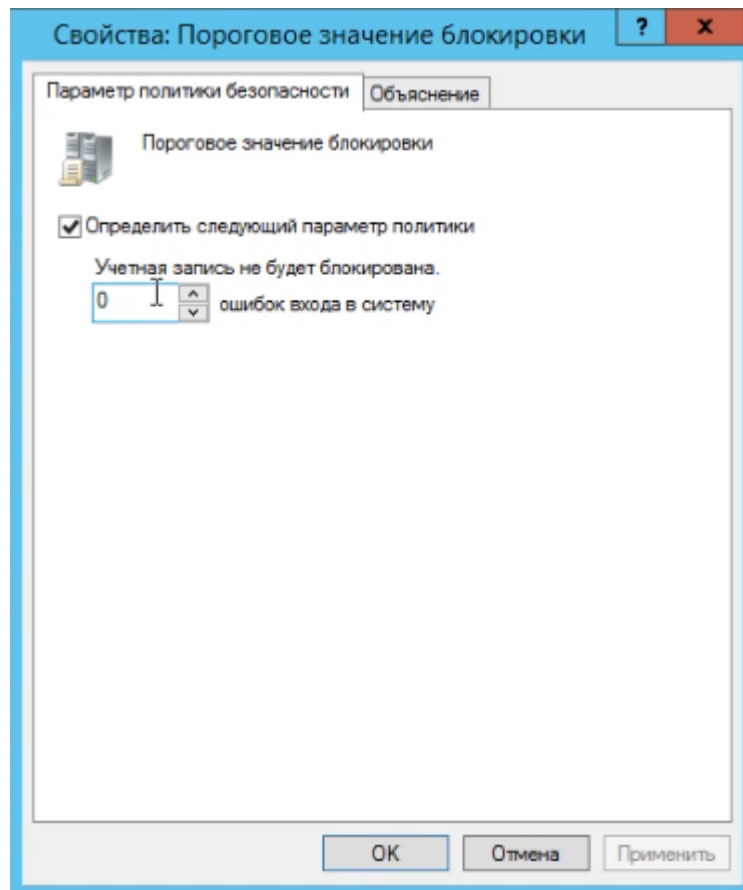


Рисунок А.27 – Диалоговое окно свойств параметра блокировки

В поле количества ошибок входа в систему введите цифру 3. Нажмите кнопки *Применить* и *ОК*.

Проверьте установленные настройки. Для этого на виртуальной машине с ОС Windows 7 попробуйте войти в систему через учетную запись первого доменного пользователя, введя неверно пароль от учетной записи четыре раза. Должно появиться диалоговое окно, показанное на рисунке А.28.

Теперь попробуйте войти в систему, введя верный пароль от учетной записи. Вход должен быть запрещен, поскольку учетная запись заблокирована.

Для разблокировки учетной записи на контроллере домена откройте консоль «Диспетчер Серверов». В правом верхнем углу откройте вкладку *Средства* и выберите пункт *Active Directory – пользователи и компьютеры*. Во вкладке *Пользователи* найдите учетную запись заблокированного пользователя и щелкните по ней правой кнопкой мыши. Откроется диалоговое окно, представленное на рисунке А.29.

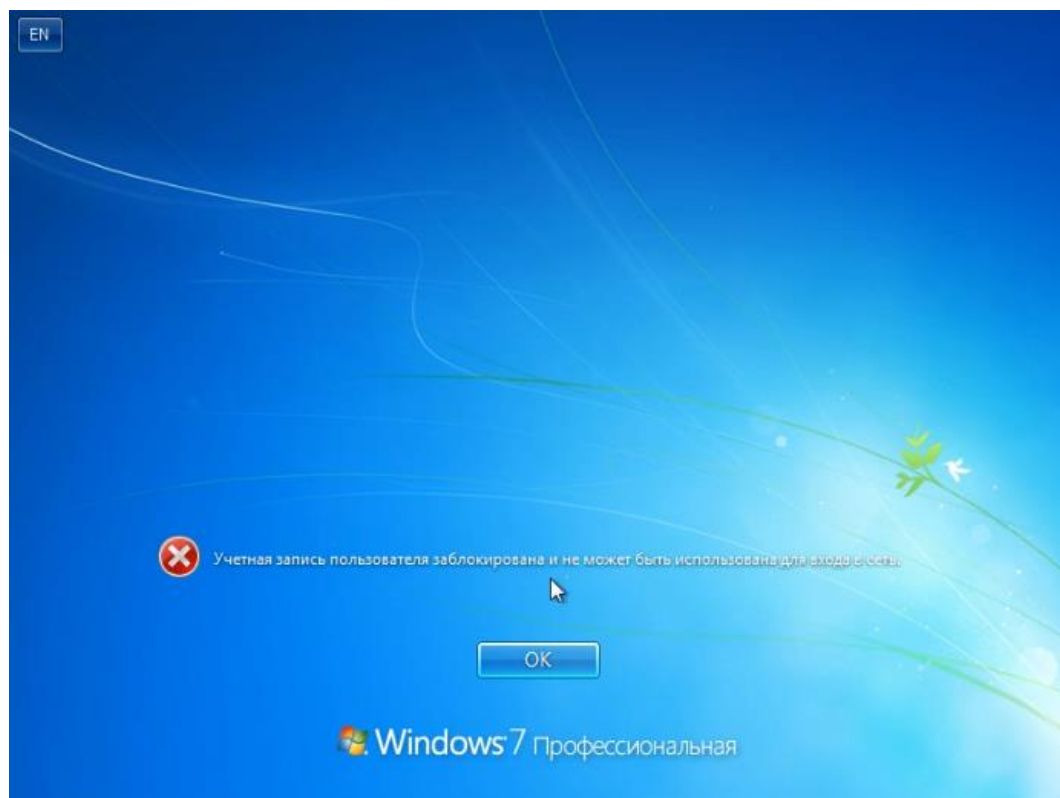


Рисунок А.28 – Диалоговое окно блокировки учетной записи

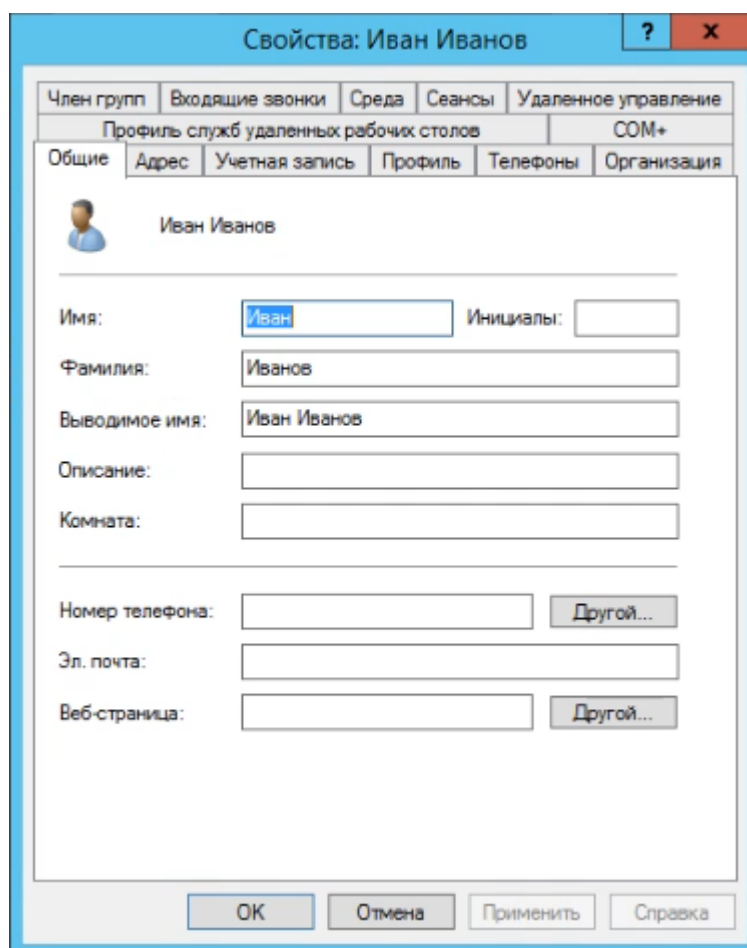


Рисунок А.29 – Диалоговое окно свойств учетной записи пользователя

Перейдите во вкладку *Учетная запись*, поставьте галочку у параметра *Разблокируйте учетную запись*. *Учетная запись на этом контроллере домена Active Directory на данный момент заблокирована* и нажмите кнопку *Применить* и *ОК*.

На виртуальной машине с ОС Windows 7 попробуйте снова войти в систему через учетную запись первого пользователя, введя верный пароль. Вход должен быть успешным.

Таблица А.1 – Варианты заданий

Вариант	Имя первого пользователя	Имя второго пользователя	Имя третьего пользователя	Длина пароля	Категории символов, используемых в паролях
1	Ivanov	Petrov	Sidorov	9	1;2;3
2	User01	User02	User03	8	1;3;4
3	Vasilijev	Sergeev	Andreev	10	1;2;4
4	User04	User05	User06	7	2;3;4
5	Maximov	Antonov	Alexeev	8	1;3;4
6	User07	User08	User09	12	1;2;4
7	Olegov	Rustamov	Vladimirov	9	1;2;3
8	User10	User11	User12	7	2;3;4
9	Pavlov	Dmitriev	Mihailov	`10	1;3;4
10	User13	User14	User15	8	1;2;3

Категории символов, используемых в паролях:

- 1 – прописные латинские буквы;
- 2 – строчные латинские буквы;
- 3 – цифры;
- 4 – спецсимволы.

Приложение Б

(обязательное)

Лабораторная работа №2 «Изучение механизмов разграничения доступа к локальным ресурсам в ОС семейства Windows»

Лабораторная работа №2 «Изучение механизмов разграничения доступа к локальным ресурсам в ОС семейства Windows»

Б.1 Цель и задание на лабораторную работу

Цель работы – получить навыки настройки механизмов разграничения доступа к локальным ресурсам в ОС семейства Windows.

Задание на лабораторную работу включает в себя:

- определение, устанавливаемых по умолчанию разрешений для папки;
- установку разрешений NTFS;
- проверку разрешений NTFS;
- вывод о проделанной работе.

Б.2 Порядок выполнения лабораторной работы

Б.2.1 Подготовка к выполнению лабораторной работы

Б.2.1.1 Для выполнения лабораторной работы в VirtualBox необходимо запустить виртуальную машину с именем Windows 7.

Для этого откройте папку *LabWork1* на рабочем столе, и запустите виртуальную машину, дважды щелкнув по ярлыку *Windows 7*. Откроется окно виртуальной машины. Подождите, пока загрузится операционная система и появится приглашение для входа в систему.

Б.2.1.2 Осуществить вход в систему, используя локальную учетную запись администратора.

Б.2.1.3 Создать учетные записи четырех локальных пользователей.

Б.2.1.4 Создать папки C:\Public и C:\Public\Library. Для этого в консоли «Мой компьютер» откройте диск C, щелкните правой кнопкой мыши по пустому месту в открывшемся окне и выберите вкладку *Создать/Папку*.

Б.2.2 Определение, устанавливаемых по умолчанию разрешений для папки

Б.2.2.1 Откройте диалоговое окно свойств папки Public. Для этого щелкните правой кнопкой мыши значок папки Public и выберите пункт *Свойства*.

Б.2.2.2 Перейдите на вкладку *Безопасность*, как показано на рисунке Б.1, для просмотра разрешений, установленных для папки Public. Если для какого-либо пользователя или группы установлены особые разрешения, выделите пользователя или группу и щелкните кнопку *Дополнительно* для просмотра списка особых разрешений.

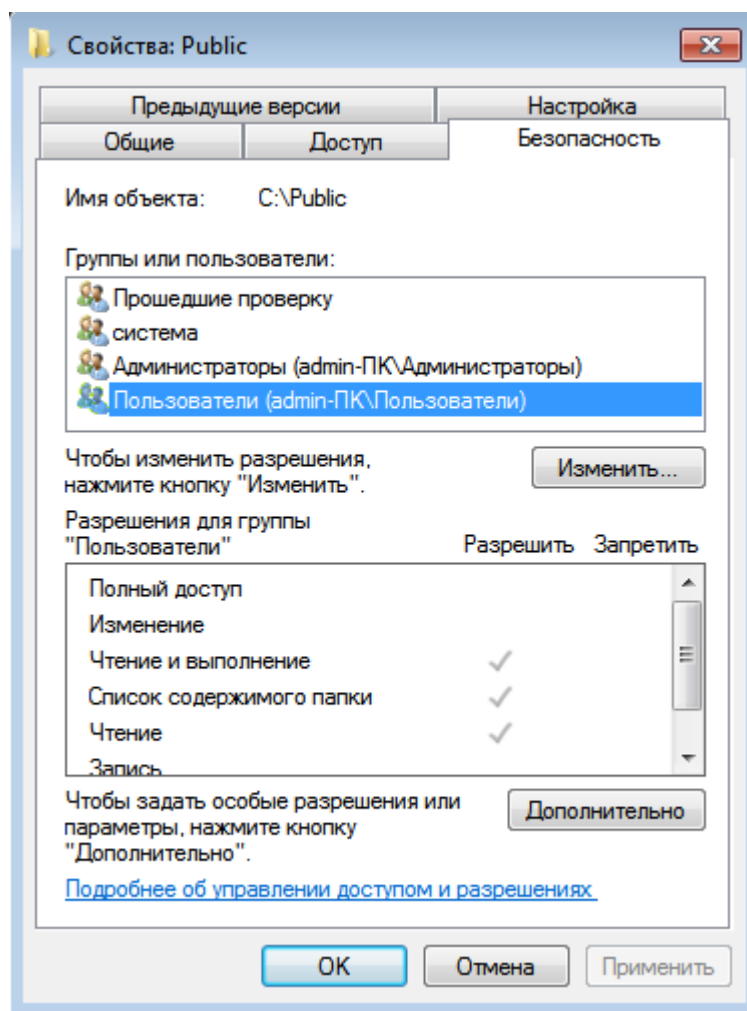


Рисунок Б.1 – Диалоговое окно вкладки «Безопасность»

Б.2.2.3 Для проверки разрешений NTFS, установленных по умолчанию, выйдите из системы, а затем войдите под учетной записью первого пользователя. Попробуйте создать текстовый файл в папке C:\Public. Для этого

через консоль «Мой компьютер» зайдите на диск С, затем в папку Public. Далее щелкните правой кнопкой мыши и выберите вкладку *Создать/Текстовый документ*. Должен создаться новый тестовый документ, назовите его «User01». Откройте созданный документ и введите произвольный текст, сохраните изменения. Попробуйте удалить созданный текстовый документ. Все произведенные действия должны быть успешны.

Создайте текстовый документ «User01» еще раз и введите в него произвольный текст. Выйдите из системы и войдите под учетной записью второго пользователя. Попробуйте изменить содержимое документа «User01», изменения должны сохраниться успешно. Затем попробуйте удалить документ «User01», документ должен быть успешно удален.

Б.2.3 Установка разрешений NTFS

Б.2.3.1 Для установки разрешений NTFS пользователям войдите в систему под учетной записью администратора. Затем перейдите в диалоговое окно свойств папки Public на вкладку *Безопасность*. Нажмите кнопку *Изменить*, должно появиться диалоговое окно, представленное на рисунке Б.2.

Нажмите кнопку *Добавить* и добавьте учетные записи созданных пользователей.

Установите разрешения NTFS для пользователей согласно варианту задания, представленному в таблице Б.1. Данная таблица приведена в конце методических указаний.

В таблице приведены списки действий, которые должны быть разрешены пользователям, все остальные действия требуется запретить.

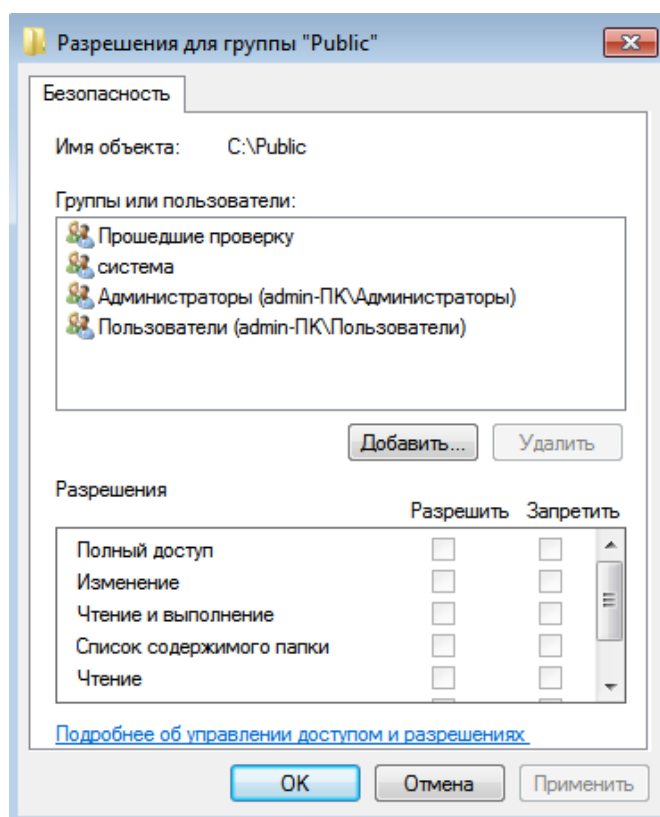


Рисунок Б.2 – Диалоговое окно настройки разрешений для папки

Б.2.3.2 Для установки разрешений NTFS в диалоговом окне настройки разрешений для папки Public во вкладке *Группы и пользователи* выберите пользователя, для которого устанавливаются разрешения. Далее во вкладке *Разрешения* в колонке *Разрешить* поставьте галочки напротив действий, которые должны быть разрешены пользователю согласно варианту задания. При установке таких разрешений, как *Изменение* или *Чтение и выполнение*, автоматически ставятся разрешения на выполнение действий, без которых невозможно осуществить назначаемое действие. Например, при установке разрешения NTFS на *Изменение*, автоматически ставятся разрешения *Чтение и выполнение*, *Список содержимого папки*, *Чтение* и *Запись*, поскольку невозможно осуществить изменение содержимого папки без предварительного чтения содержимого папки или последующей записи изменений. Для действий, у которых после выполнения предыдущих операций колонка *Разрешить* осталась пустой, поставьте галочки в колонке *Запретить*.

Выполните данную процедуру для всех четырех пользователей и нажмите кнопку *Применить*, в затем кнопку *ОК*.

Проверьте установленные разрешения NTFS. Для этого поочередно зайдите под учетными записями всех четырех пользователей и попробуйте создать текстовый файл, посмотреть или изменить его содержимое, удалить текстовый файл. Для удобства рекомендуется называть создаваемый текстовый файл именем учетной записи пользователя, который осуществляет создание файла.

Б.2.3.3 Войдите в систему под учетной записью администратора. Отберите у созданных учетных записей и группы *Пользователи* все права. Для этого в диалоговом окне настройки разрешений для папки Public во вкладке *Группы и пользователи* выберите первого пользователя. Далее во вкладке *Разрешения* в колонках *Разрешить* и *Запретить* уберите все галочки. Выполните данную процедуру для оставшихся трех пользователей и группы *Пользователи* и нажмите кнопку *Применить*, в затем кнопку *ОК*.

Создайте две группы пользователей Group1 и Group2. Включите первого и второго пользователей в группу Group1, а третьего и четвертого – в группу Group2.

Для установки разрешений NTFS группам пользователей в диалоговом окне настройки разрешений для папки Public нажмите кнопку *Добавить* и добавьте созданные группы Group1 и Group2. Затем для группы Group1 установите разрешение на *Чтение и выполнение*, а для группы Group2 – разрешение на *Изменение*. Нажмите кнопку *Применить*, в затем кнопку *ОК*.

Проверьте установленные разрешения NTFS. Для этого поочередно зайдите под учетными записями всех четырех пользователей и попробуйте создать текстовый файл, посмотреть или изменить его содержимое, удалить текстовый файл.

Б.2.4 Установка особых разрешений

Б.2.4.1 Войдите в систему под учетной записью администратора. Для установки особых разрешений перейдите в свойства папки Library и откройте

вкладку *Безопасность*. Нажмите кнопку *Добавить* и добавьте учетную запись первого пользователя. Далее нажмите кнопку *Дополнительно*, откроется диалоговое окно дополнительных параметров безопасности, представленное на рисунке Б.3.

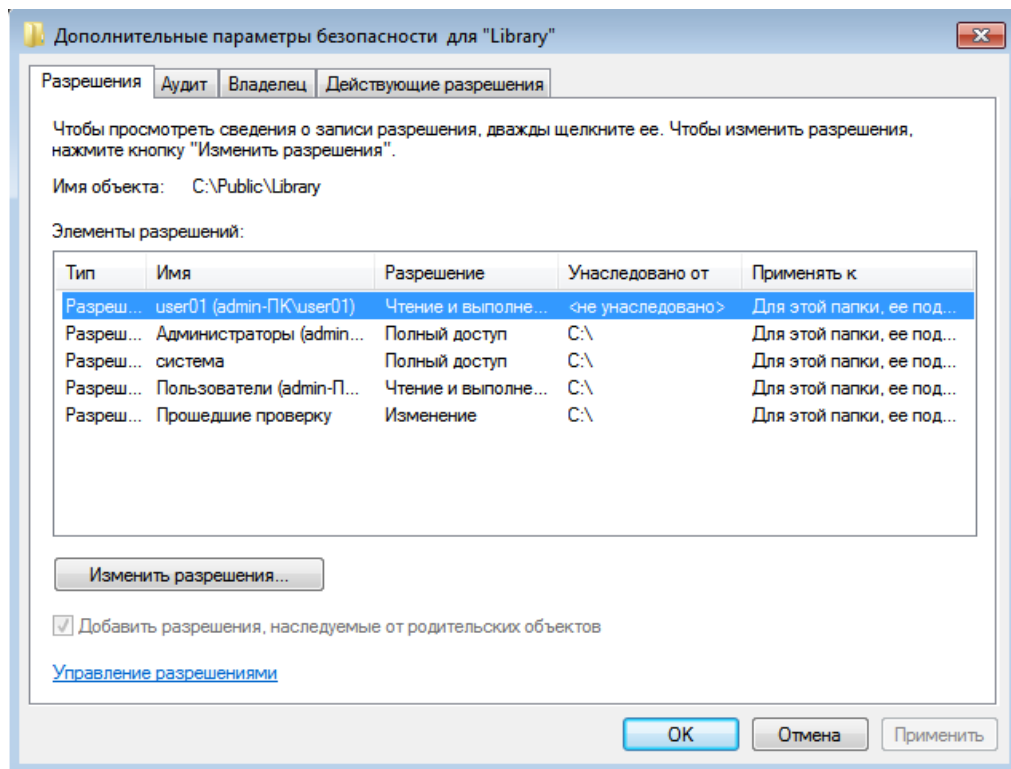


Рисунок Б.3 – Диалоговое окно дополнительных параметров безопасности

В полученном списке выберите первого пользователя и нажмите кнопку *Изменить разрешения....* Появится диалоговое окно дополнительных параметров безопасности, представленное на рисунке Б.4.

Еще раз в полученном списке выберите первого пользователя и нажмите кнопку *Изменить....* Появится диалоговое окно настройки особых разрешений, представленное на рисунке Б.5.

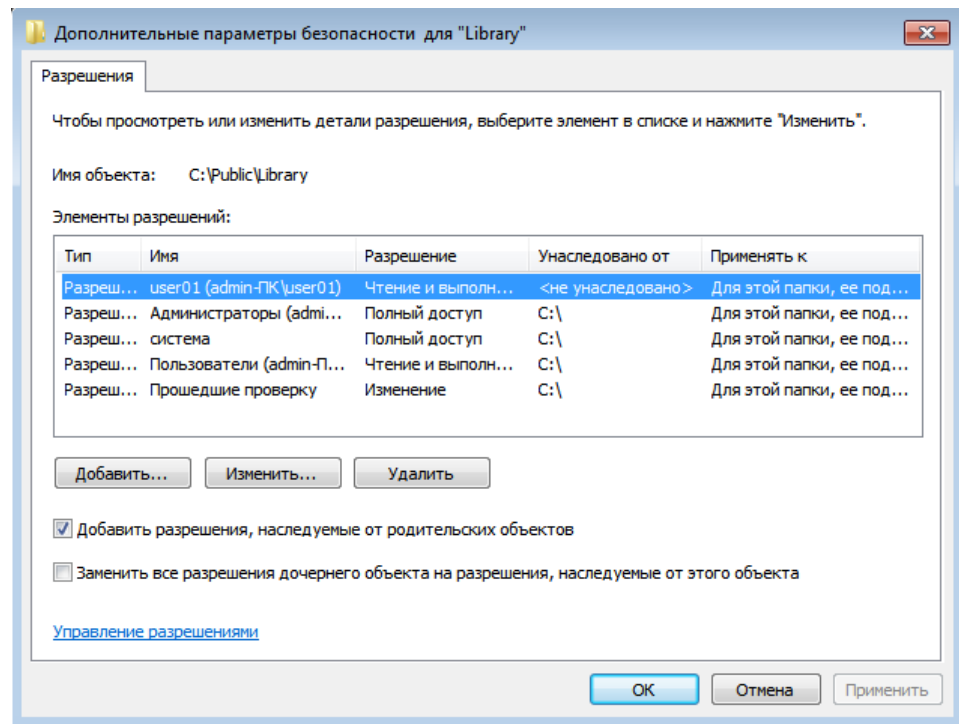


Рисунок Б.4 – Диалоговое окно дополнительных параметров безопасности

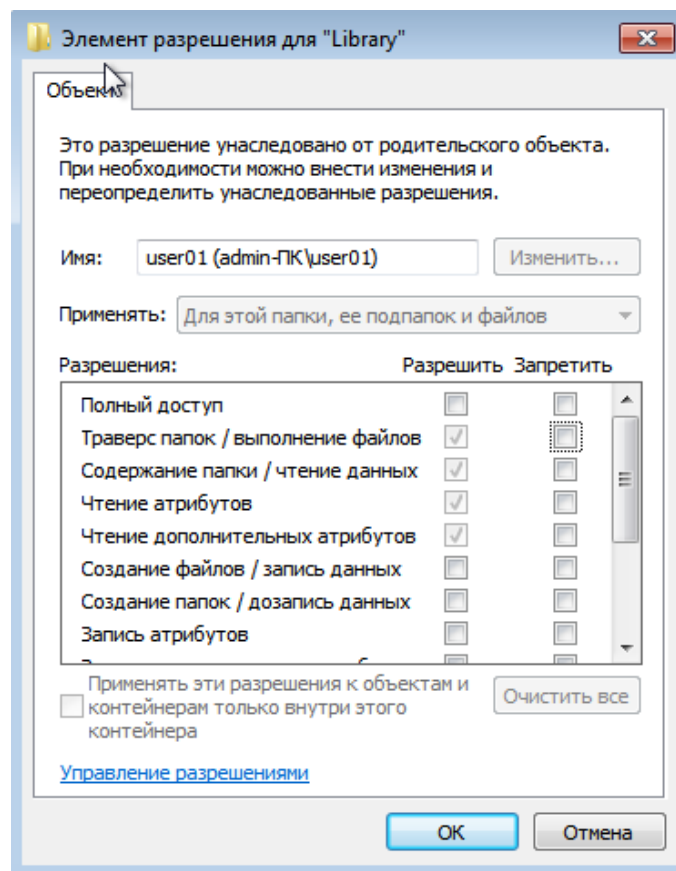


Рисунок Б.5 – Диалоговое окно настройки особых разрешений

Для первого пользователя установите разрешение *Смена разрешений*. Проверьте установленные особые разрешения. Для этого войдите под учетной записью первого пользователя и попробуйте изменить особые разрешения другого пользователя. Данное действие должно закончиться успешно.

Таблица Б.1 – Варианты заданий

Вариант	Разрешения NTFS для первого пользователя	Разрешения NTFS для второго пользователя	Разрешения NTFS для третьего пользователя	Разрешения NTFS для четвертого пользователя
1	Полный доступ	Чтение и выполнение	Запись	–
2	Чтение и выполнение	Полный доступ	–	Запись
3	–	Запись	Полный доступ	Чтение и выполнение
4	Запись	Чтение и выполнение	–	Полный доступ
5	Полный доступ	Запись	–	Чтение и выполнение
6	–	Полный доступ	Чтение и выполнение	Запись
7	Чтение и выполнение	–	Полный доступ	Запись
8	Запись	–	Чтение и выполнение	Полный доступ
9	Полный доступ	Чтение и выполнение	Запись	–
10	Запись	Полный доступ	–	Чтение и выполнение

Приложение В

(обязательное)

Лабораторная работа №3 «Изучение механизмов разграничения доступа к сетевым ресурсам в ОС семейства Windows»

Лабораторная работа №3 «Изучение механизмов разграничения доступа к сетевым ресурсам в ОС семейства Windows»

В.1 Цель и задание на лабораторную работу

Цель работы – получить навыки настройки механизмов разграничения доступа к сетевым ресурсам в ОС семейства Windows, включающие:

Задание на лабораторную работу включает в себя:

- организацию доступа к общей папке на локальном компьютере;
- организацию общего сетевого ресурса на контроллере домена;
- проверку доступа к общему ресурсу;
- проверку назначенных прав;
- вывод о проделанной работе.

В.2 Порядок выполнения лабораторной работы

В.2.1 Подготовка к выполнению лабораторной работы

В.2.1.1 Для выполнения лабораторной работы в VirtualBox необходимо запустить виртуальные машины с именами Windows 7 и Windows Server 2012R2.

Для этого откройте папку *LabWork1* на рабочем столе, и запустите виртуальные машины, дважды щелкнув по ярлыку *Windows 7* и *Windows Server 2012R2*. Откроются окна виртуальных машин. Подождите, пока загрузится операционная система и появится приглашение для входа в систему.

В.2.1.2 Осуществить вход в ОС Windows Server 2012R2, используя доменную учетную запись администратора.

В.2.1.3 Создать учетную запись доменного пользователя.

В.2.2 Организация доступа к общей папке на локальном компьютере

В.2.2.1 Войдите на контроллер домена под учетной записью администратора. Добавьте пользователя в группу администраторов домена. Для этого откройте консоль «Диспетчер серверов», в правом верхнем углу нажмите вкладку *Средства* и выберите пункт *Пользователи и компьютеры Active Directory*. Перейдите во вкладку *Пользователи* и щелкните правой кнопкой мыши по группе *Администраторы домена* и выберите пункт *Свойства*. Откроется диалоговое окно, представленное на рисунке В.1.

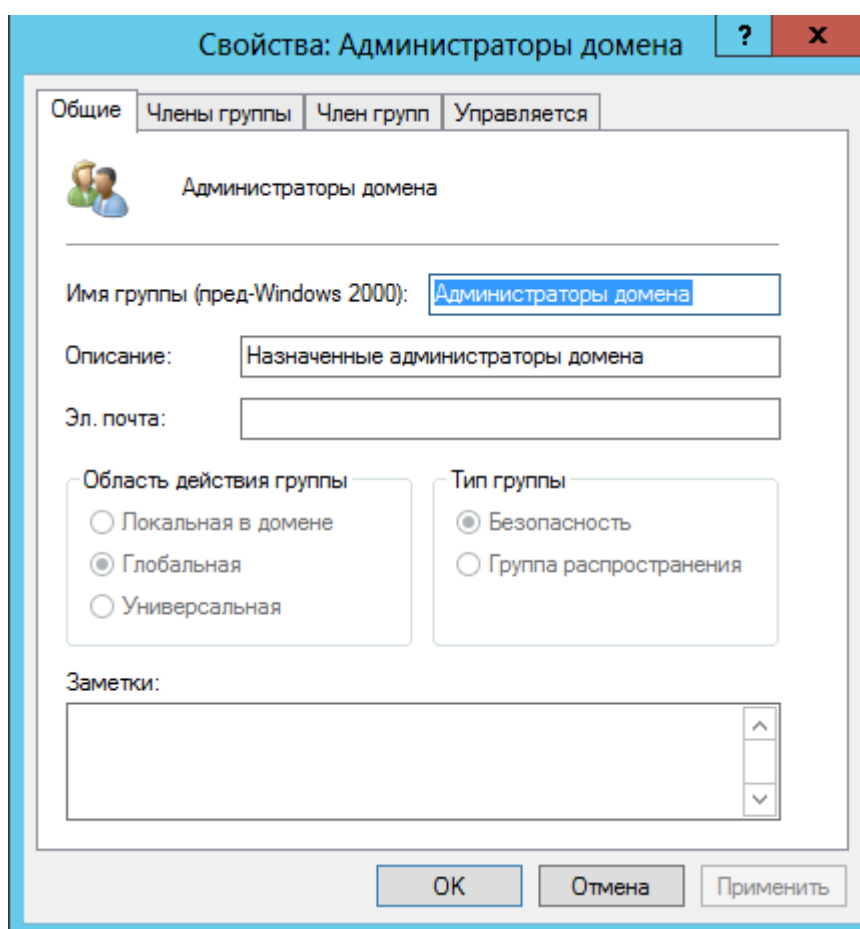


Рисунок В.1 – Диалоговое окно свойств группы пользователей

Перейдите во вкладку *Члены группы* и нажмите кнопку *Добавить....*. Добавьте в данную группу пользователя и нажмите кнопку *Применить*.

В.2.2.2 Для организации доступа к общей папке на локальном компьютере войдите в ОС Windows 7, используя учетную запись пользователя,

и на диске С создайте папку, согласно варианту задания, приведенному в таблице В.1. Данная таблица приведена в конце методических указаний.

Откройте свойства, созданной папки. Для этого щелкните правой кнопкой мыши по созданной папке и выберите вкладку *Свойства*. Откроется диалоговое окно, представленное на рисунке В.2.

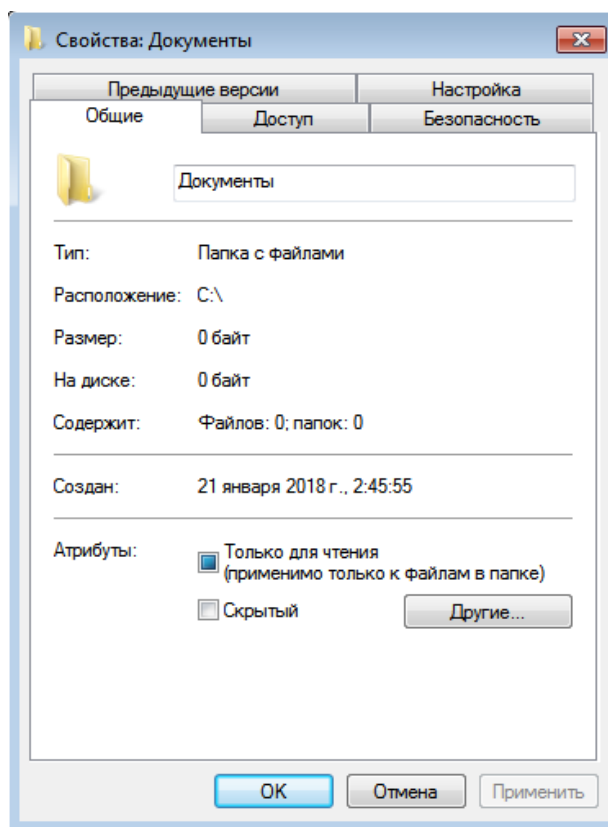


Рисунок В.2 – Диалоговое окно свойств папки

Перейдите во вкладку *Доступ* и нажмите кнопку *Общий доступ*. Откроется диалоговое окно, показанное на рисунке В.3.

В выпадающем меню выберите пункт *Все* и нажмите кнопку *Общий доступ*. В появившемся диалоговом окне нажмите кнопку *Готово*.

Перейдите во вкладку *Безопасность* и просмотрите список управления доступом этого каталога. Нажмите кнопку *Дополнительно*, появится диалоговое окно редактирования особых разрешений, представленное на рисунке В.4.

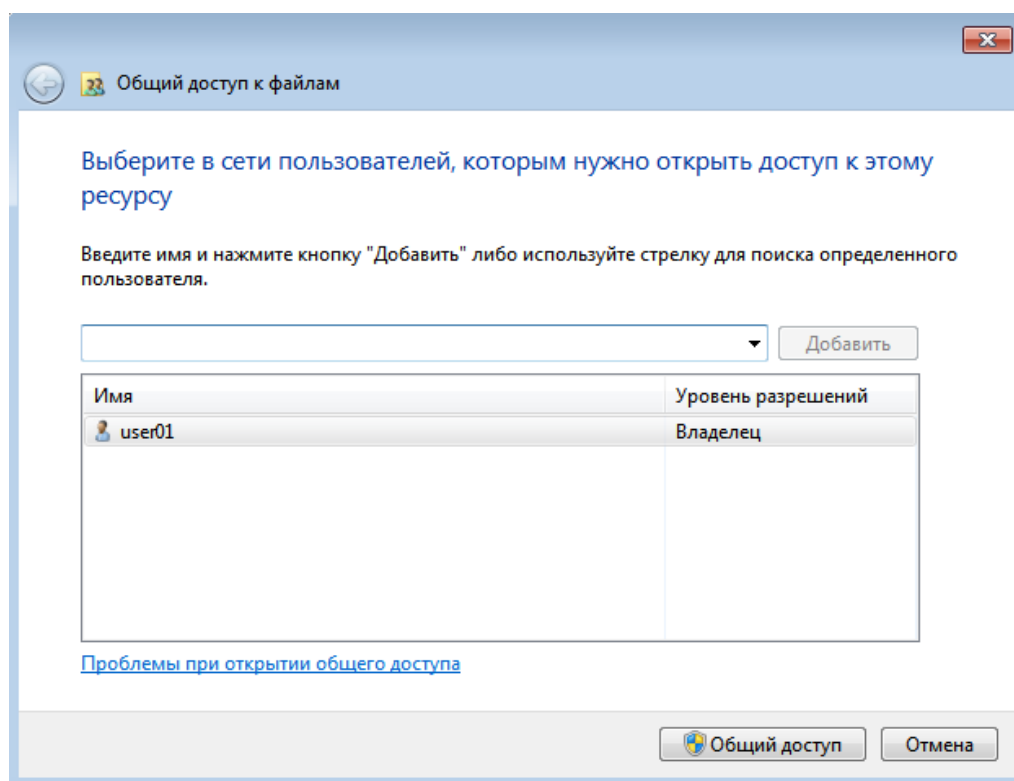


Рисунок В.3 – Диалоговое окно настройки общего доступа

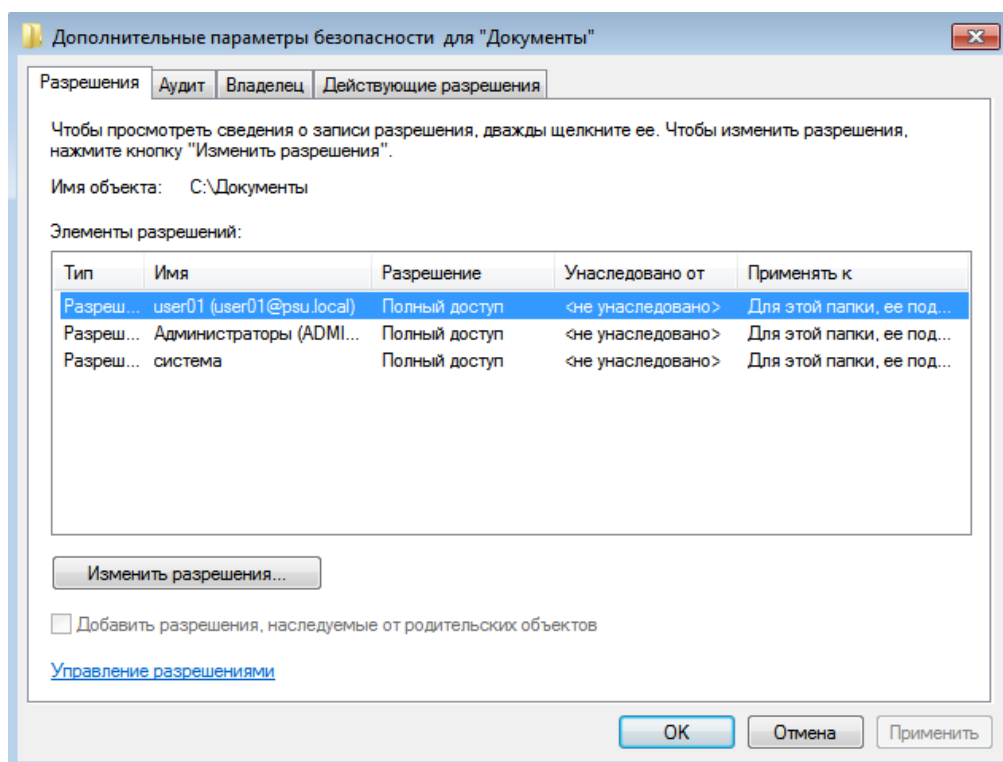


Рисунок В.4 – Диалоговое окно редактирования особых разрешений

Убедитесь, что наследование разрешений от родительских объектов отключено. Для этого уберите галочку с пункта *Добавить разрешения, наследуемые от родительских объектов*.

Вернитесь в предыдущее диалоговое окно и нажмите кнопку *Изменить...*, а затем в появившемся диалоговом окне нажмите кнопку *Добавить...* Добавьте учетную запись пользователя и группу администраторов домена. Для этого нажмите кнопку *Дополнительно...*, а затем кнопку *Поиск*. В появившемся списке выберите учетную запись пользователя и группу *Администраторы домена* и нажмите кнопку *ОК*. Нажмите кнопку *ОК* еще раз.

Установите для пользователя разрешение согласно варианту задания, приведенному в таблице В.1. Данная таблица приведена в конце методических указаний. Группе администраторов домена установите разрешение на *Чтение и Список содержимого папки*. Нажмите кнопку *Применить* и выйдите из диалогового окна свойств папки.

В.2.2.3 Для проверки доступа к общему сетевому ресурсу зайдите на контроллер домена под учетной записью администратора.

Удалите пользователя из группы администраторов домена. Для этого в диалоговом окне свойств группы администраторов домена перейдите во вкладку *Члены группы*, выберите пользователя и нажмите кнопку *Удалить*. Нажмите кнопку *Применить* и выйдите из данного диалогового окна.

Откройте консоль «Компьютер» через меню *Пуск*. В левой части окна откройте вкладку *Сеть*, а затем откройте вкладку *ADMIN-PC*, появится диалоговое окно, представленное на рисунке В.5.

Перейдите к виртуальной машине с ОС Windows 7 и войдите в систему, используя учетную запись пользователя. Попробуйте открыть папку, для которой настроен общий доступ, создать внутри папки текстовый файл, изменить его содержимое и удалить его. Убедитесь, что Вам доступно изменение ресурсов.

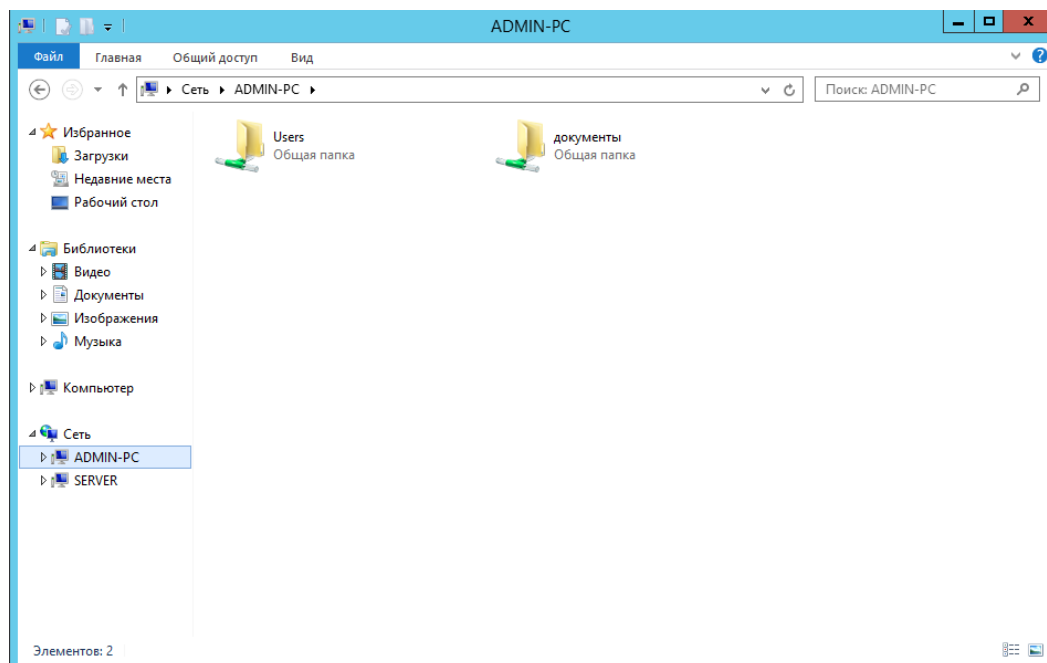


Рисунок В.5 – Диалоговое окно управления компьютером

В.2.3 Организация общего сетевого ресурса на контроллере домена

В.2.3.1 Перейдите к виртуальной машине с ОС Windows 7 и войдите в систему, используя учетную запись доменного администратора.

Откройте диалоговое окно свойств папки, к которой был предоставлен общий доступ и перейдите на вкладку *Доступ*. Нажмите кнопку *Расширенная настройка*, появится диалоговое окно, показанное на рисунке В.6.

Уберите галочку с пункта *Открыть общий доступ к этой папке*.

Перейдите на контроллер домена и войдите под учетной записью администратора. Откройте консоль «Компьютер» через меню *Пуск*, перейдите на вкладку *Сеть/ADMIN-PC* и убедитесь, что общий доступ к папке был отключен.

Откройте консоль «Диспетчер серверов». В правом верхнем углу откройте вкладку *Средства* и выберите пункт *Управление компьютером*, появится диалоговое окно, представленное на рисунке В.7.

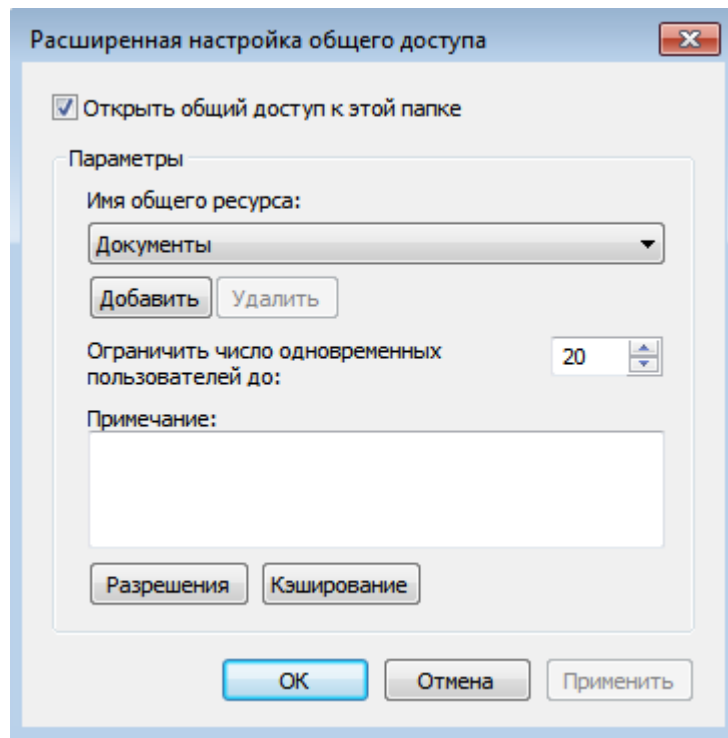


Рисунок В.6 – Диалоговое окно расширенной настройки общего доступа

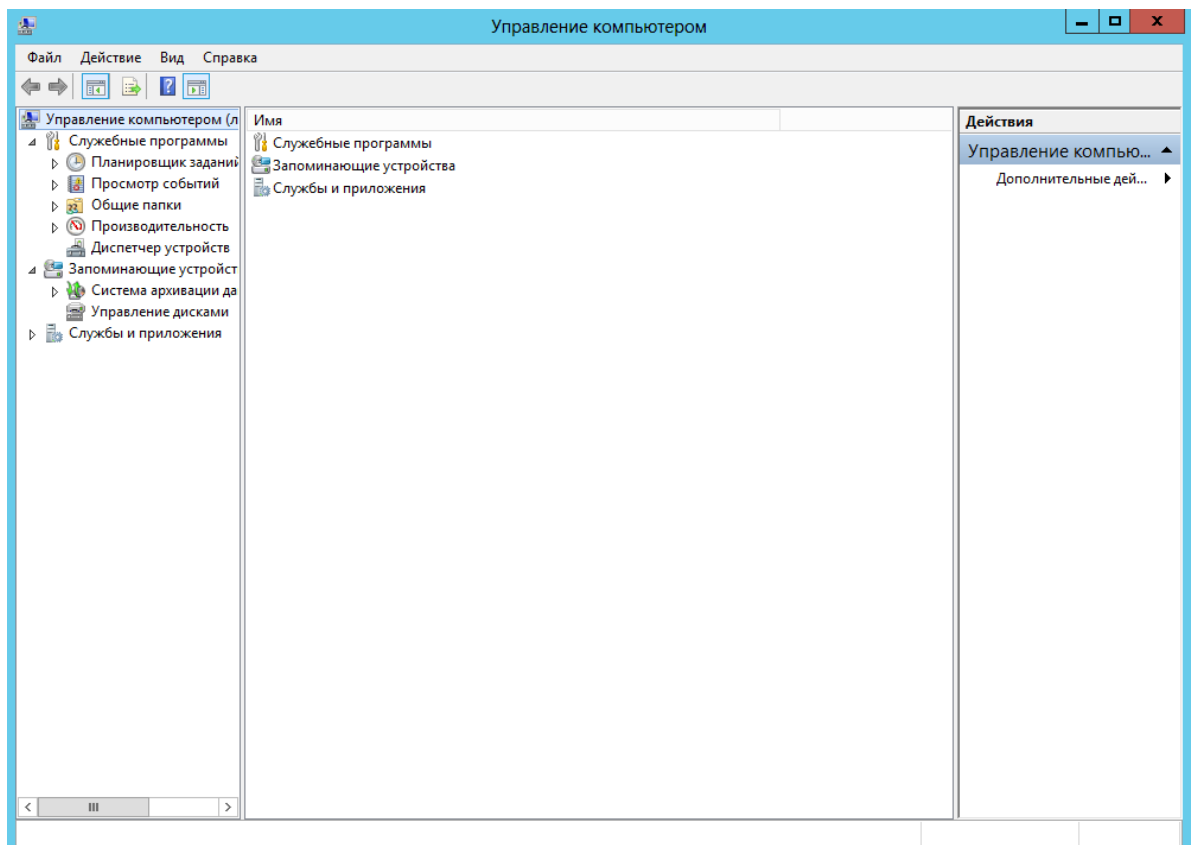


Рисунок В.7 – Диалоговое окно управления компьютером

Откройте вкладку *Общие папки* и в правой части окна выберите вкладку *Общие ресурсы*. По умолчанию открываются папки локального компьютера. Для подключения к компьютеру с ОС Windows 7 щелкните правой кнопкой

мышью по вкладке *Управление компьютером* и выберите пункт *Подключиться к другому компьютеру...* Откроется диалоговое окно выбора компьютера, показанное на рисунке В.8.

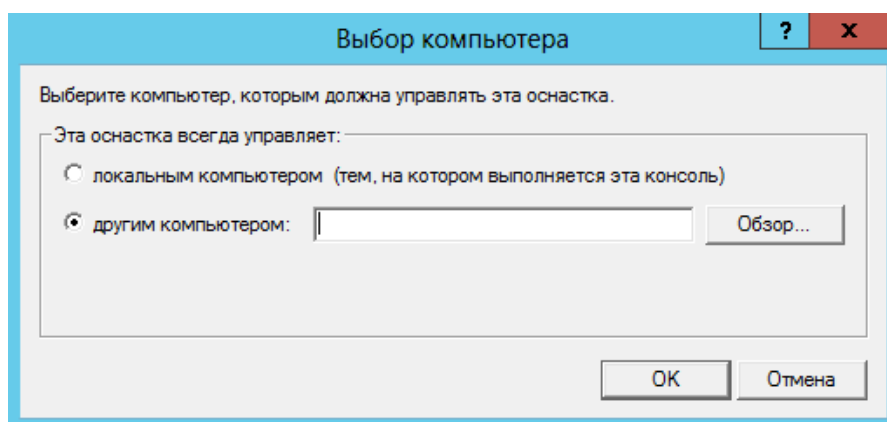


Рисунок В.8 – Диалоговое окно выбора компьютера

Нажмите кнопку *Обзор...*, в появившемся диалоговом окне введите имя компьютера ADMIN-PC, нажмите кнопку *Проверить имена* и нажмите кнопку *ОК*. Нажмите кнопку *ОК* еще раз.

Откройте вкладку *Служебные программы/Общие папки/Общие ресурсы*. В правой части окна щелкните правой кнопкой мыши и выберите пункт *Новый общий ресурс...* Запустится «Мастер создания общих ресурсов», что показано на рисунке В.9.

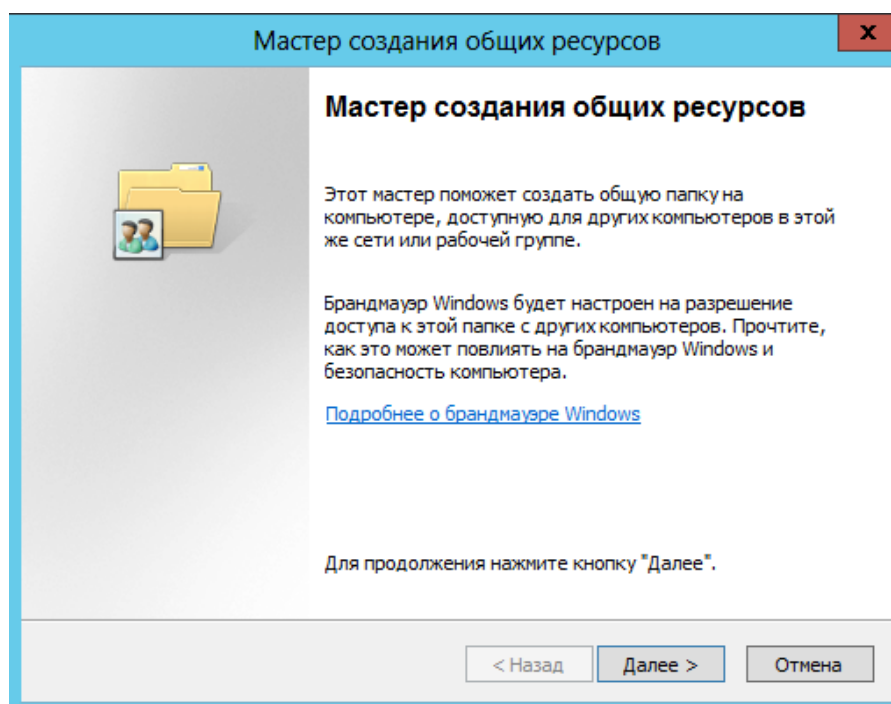


Рисунок В.9 – Мастер создания общих ресурсов

Нажмите кнопку *Далее*. В поле *Путь к папке* введите путь в виде *C:\Имя папки* и нажмите кнопку *Далее*. На следующем шаге создания общего ресурса оставьте все без изменений и нажмите кнопку *Далее*. На следующем шаге нужно выбрать вид разрешений для общей папки. Выберите вид разрешений, как показано на рисунке В.10, и нажмите кнопку *Готово*. Нажмите *Готово* еще раз.

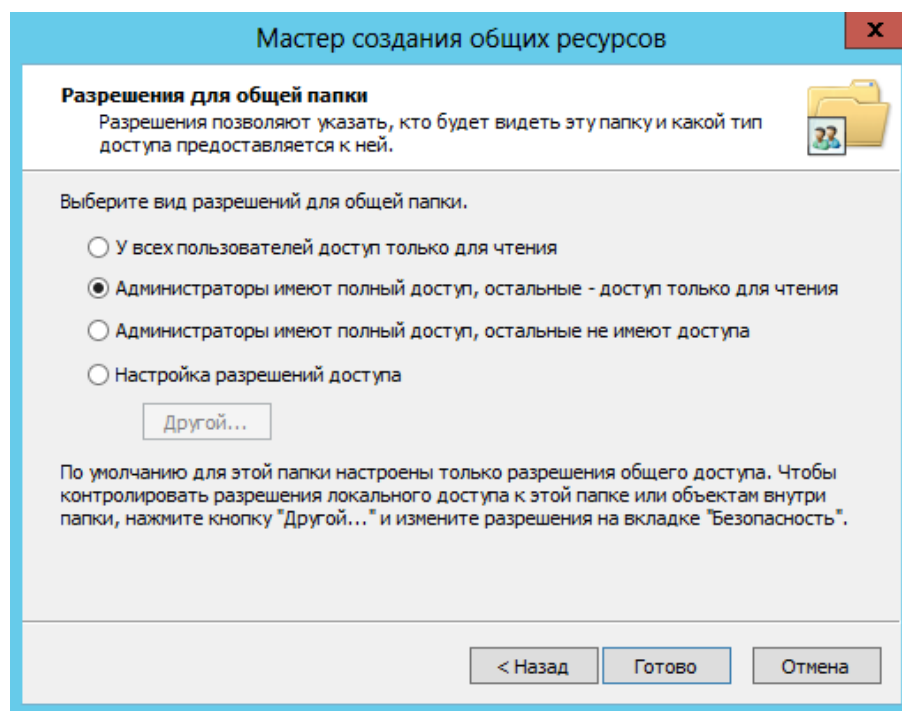


Рисунок В.10 – Выбор вида разрешений

В.2.3.2 Для проверки назначенных прав сначала нужно изменить локальную политику безопасности домена, так как по умолчанию локальная политика безопасности домена запрещает обычным пользователям вход на контроллер домена. Для этого откройте консоль «Диспетчер серверов». В правом верхнем углу откройте вкладку *Средства* и выберите пункт *Локальная политика безопасности*, появится диалоговое окно, представленное на рисунке В.11.

Откройте вкладку *Локальные политики/Назначение прав пользователя*. В правой части окна выберите пункт *Локальный вход в систему*. Откроется диалоговое окно, представленное на рисунке В.12.

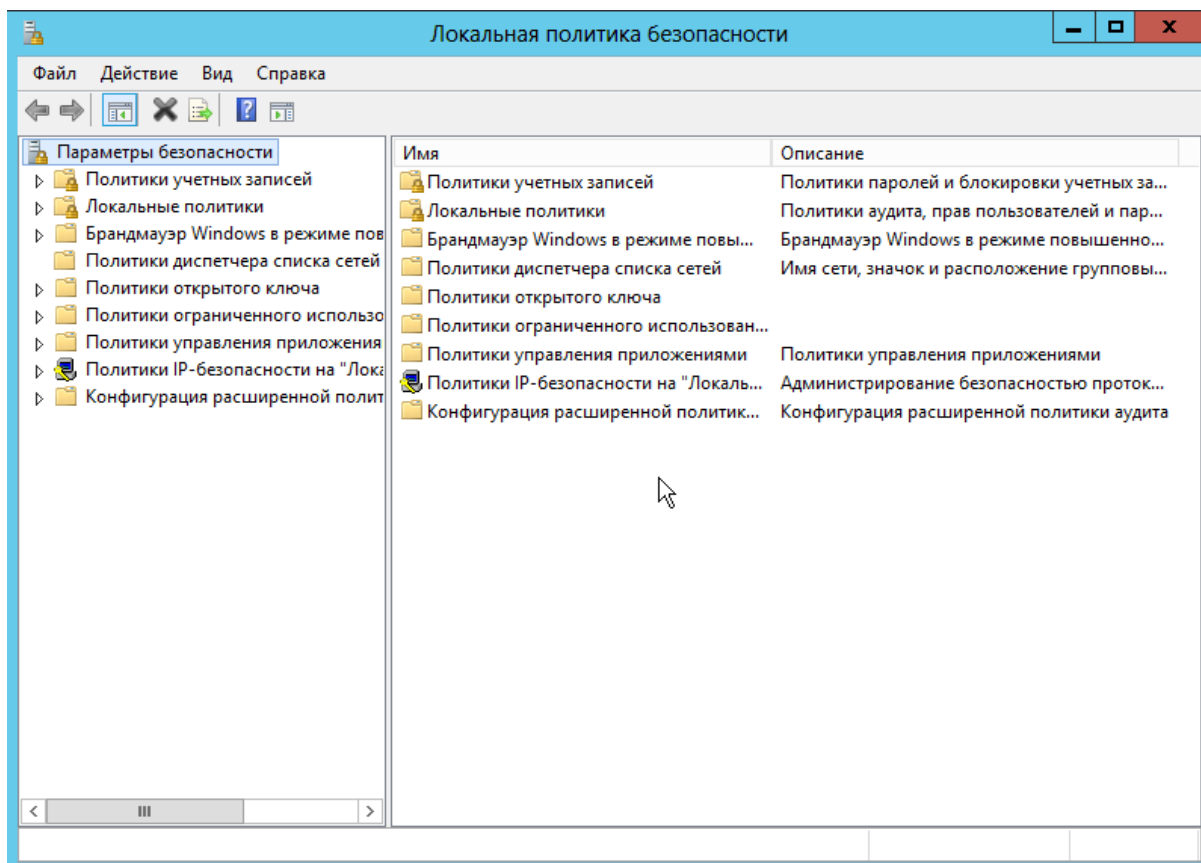


Рисунок В.11 – Диалоговое окно локальной политики безопасности

Нажмите кнопку *Добавить пользователя или группу....* Добавьте учетную запись пользователя. Примените изменения.

В.2.3.3 Войдите на контроллер домена под учетной записью пользователя. Через консоль «Компьютер» откройте сетевое окружение и откройте общую папку. Попробуйте создать текстовый файл. Убедитесь, что у Вас нет прав на совершение этого действия.

Войдите на контроллер домена под учетной записью администратора. Отредактируйте сетевые разрешения для общей папки таким образом, чтобы все пользователи имели разрешение *Полный доступ*.

Войдите на контроллер домена под учетной записью пользователя. Через консоль «Компьютер» откройте сетевое окружение и откройте общую папку. Попробуйте создать текстовый файл, изменить его содержимое и удалить его. Данные действия должны завершиться успехом.

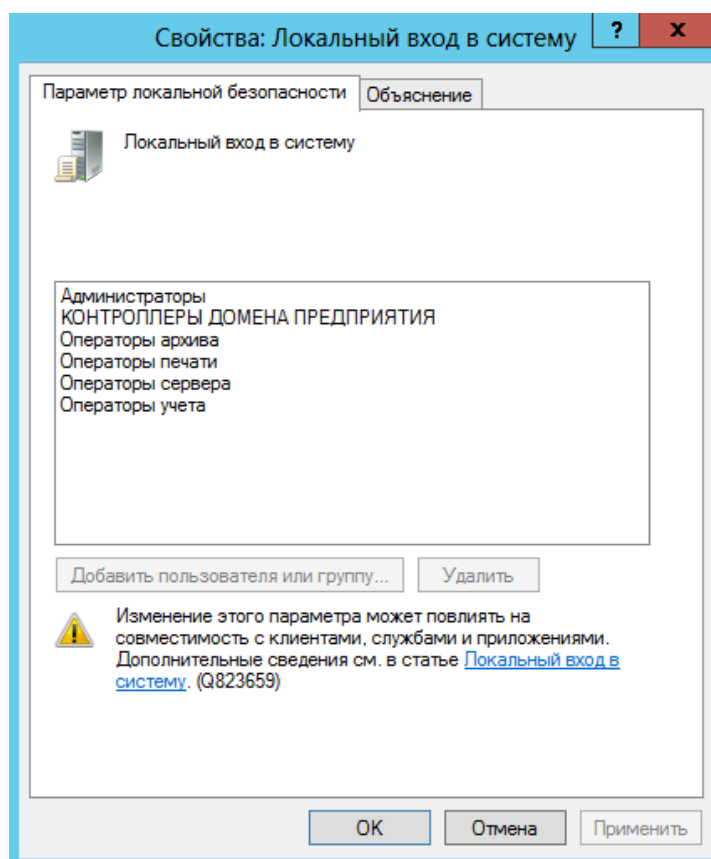


Рисунок В.12 – Диалоговое окно политики локального входа в систему

Таблица В.1 – Варианты заданий

Вариант	Название общего ресурса	Разрешения для пользователя
1	Документы	Полный доступ
2	Отчеты	—
3	Бухгалтерия	Чтение и выполнение
4	Программы	—
5	Положения	Чтение и выполнение
6	Заявки	Запись
7	База данных	Полный доступ
8	Интернет	Чтение и выполнение
9	Продукция	Запись
10	Финансы	Запись

Приложение Г

(обязательное)

Протокол проверки на оригинальность в системе «Антиплагиат.ВУЗ»

Ректору Пензенского
государственного университета
А. Д. Гулякову
студента 6 курса ФПИТЭ
очной формы обучения
Горбунова Максима Александровича

ЗАЯВЛЕНИЕ

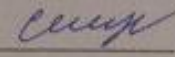
Я, Горбунов Максим Александрович, студент 6 курса очной формы обучения направления подготовки 10.05.02 – «Информационная безопасность телекоммуникационных систем», прошу провести проверку с использованием системы «Антиплагиат» дипломного проекта на тему «Лабораторный практикум по изучению механизмов обеспечения безопасности доступа к локальным и сетевым ресурсам в операционных системах семейства Windows», выполненного мной самостоятельно, на содержание элементов плагиата.

Все прямые заимствования из печатных и электронных источников, а также из защищенных ранее выпускных квалификационных работ, кандидатских и докторских диссертаций имеют соответствующие ссылки.

Я ознакомлен с действующим Стандартом университета «Выпускная квалификационная работа обучающихся по образовательным программам высшего образования – программам бакалавриата, программам специалитета и программам магистратуры», согласно которому обнаружение плагиата является основанием для недопуска ВКР к защите и отчисления из университета.


«22» 01 2018г

ВКР представлена на проверку «22» 01 2018г

Руководитель ВКР  С.Н. Шумкин

Протокол

проверки на оригинальность в системе «Антиплагиат.ВУЗ» выпускной квалификационной работы на тему «Лабораторный практикум по изучению механизмов обеспечения безопасности доступа к локальным и сетевым ресурсам в операционных системах семейства Windows» студента 6 курса Горбунова Максима Александровича

Специальность 10.05.02 – Информационная безопасность телекоммуникационных систем

Специализация – Разработка защищенных телекоммуникационных систем

Руководитель ВКР к.т.н., доцент кафедры ИБСТ Шумкин С.Н.

Отчет о проверке на заимствования

Автор: Горбунов Максим Александрович garbunovmaxim1995@mail.ru / ID: 698

Проверяющий: Ватеев Алексей Григорьевич vat@ascp.ru / ID: 393

Организация: Пензенский гос. университет

Отчет предоставлен сервисом «Антиплагиат.ВУЗ» - <http://propry.ascp.ru>

ИНФОРМАЦИЯ О ДОКУМЕНТЕ

№ документа: 45
Начало загрузки: 23.01.2018 18:04:23
Длительность загрузки: 00:00:06
Имя исходного файла: Горбунов Максим Александрович ВКР_12071_Горбунов.docx
Размер текста: 3799 кб
Тип документа: Выпускная квалификационная работа
Символов в тексте: 67879
Слов в тексте: 8411
Число предложений: 588

ИНФОРМАЦИЯ ОБ ОТЧЕТЕ

Последний готовый отчет (ред.)
Начало проверки: 23.01.2018 23:20:53
Длительность проверки: 00:00:25
Комментарий: не указан
Модули поиска: Модуль поиска ЯСЦ "БиблиоРоссийка", Модуль поиска ЯСЦ "BOOK.ru", Коллекция PTS, Цитирование, Модуль поиска ЯСЦ "Университетская библиотека онлайн", Коллекция eLIBRARY.RU, Модуль поиска ЯСЦ "Айбук", Модуль поиска Интернет, Модуль поиска ЯСЦ "Пань", Модуль поиска "ТЕУ", Коллоз вузов

ЗАИМСТВОВАНИЯ	ЦИТИРОВАНИЕ	ОРИГИНАЛЬНОСТЬ
17.22%	0%	82.78%



24.01.2018

С.Н. Шумкин