Санкт-Петербургский Национальный Исследовательский Университет Информационных технологий, механики и оптики

**Лабораторная работа 4**

**Настройка доступа и безопасности к ресурсам**

Выполнил: Фисенко

Максим Вячеславович

Шкода Глеб Ярославович

Группа № К34211

Проверила: Казанова

Полина Петровна

Санкт-Петербург

2024

**Цель работы:**

Настроить доступ к ресурсам и обеспечить их безопасность.

**Задачи:**

1. Настроить безопасность доступа в компьютер.
2. Настроить безопасность локальных ресурсов и общий доступ к сетевым устройствам.
3. Настроить безопасность файлов при помощи шифрования.
4. Настроить доступ к сетевому принтеру.

**Ход работы:**

**1. Настройка безопасности доступа к компьютеру**

Для выполнения лабораторной работы первым делом необходимо было создать две локальные учетные записи пользователя на первой виртуальной машине, что было сделано успешно. На рисунке 1 можно увидеть диалоговое окно, в котором создавались обе учетные записи одна за другой.

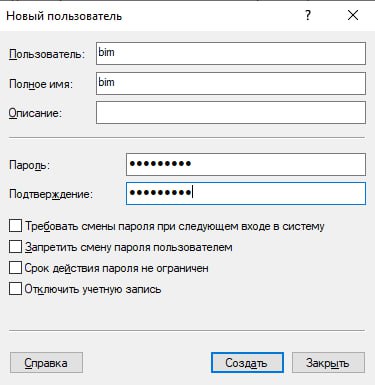


Рисунок 1 – Окно создания учетной записи

После этого была создана локальная группа *PrintUsers*, в которую были добавлена два только что созданных пользователя (рисунок 2).

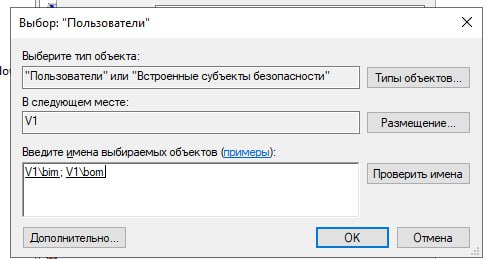


Рисунок 2 – Добавление пользователей в локальную группу

Далее было необходимо предоставить этим пользователем разрешение на подключение через удаленный рабочий стол – для этого оба пользователя были добавлены в группу *«Пользователи удаленного рабочего стола»* (рисунок 3).

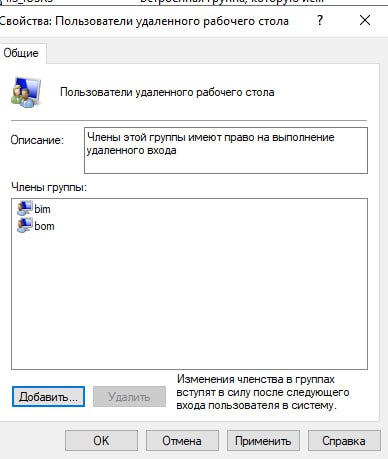


Рисунок 3 – Пользователи удаленного рабочего стола

Аналогичным образом на виртуальной машине *v2* были созданы еще две учетные записи. Они были добавлены в локальную группу *«Managers»*, и им также был предоставлен доступ к удаленному рабочему столу.

**2. Настройка безопасности локальных ресурсов и общего доступа к сетевым ресурсам**

На обеих виртуальных машинах на диске *K:* были созданы каталоги в соответствии с инструкцией к лабораторной работе – это можно увидеть на рисунке 4 и рисунке 5.

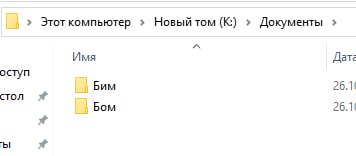


Рисунок 4 – Каталоги в v1

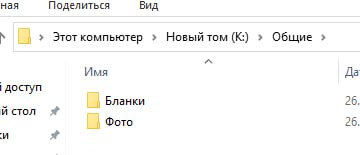


Рисунок 5 – Каталоги в v2

Затем ко всем 6 созданным папкам были предоставлены доступы для пользователей в соответствии с инструкцией к лабораторной работе. Так, на рисунке 6 можно увидеть настройки безопасности для каталога *«Общие»* на виртуальной машине *v2*.

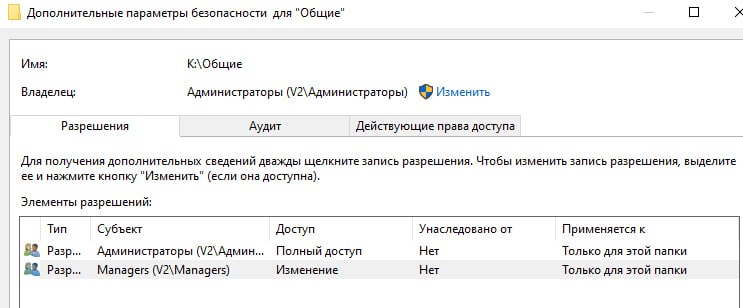


Рисунок 6 – Настройки доступа папки «Общие»

Также согласно таблице из инструкции к лабораторной работе были предоставлены общие доступы к некоторым сетевым ресурсам. Например, на рисунке 7 можно заметить, что к папке *«Документы»* открыт общий доступ с уровнем *«Полный доступ»*.

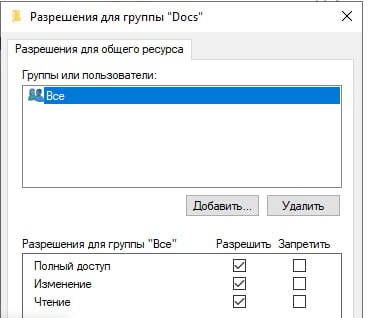


Рисунок 7 – Общий доступ к папке «Документы»

Далее была осуществлена проверка доступа к данным папкам. Был осуществлен вход с учетных записей разных пользователей, и затем с каждой из них были предприняты попытки создать файлы в папках, удалить их, а также открыть сами папки и подключиться к ним по сети, добавить по сети файлы. Результаты данной проверки представлены в таблице 1, в которой «+» обозначает успешную попытку выполнить определенное действие, а «-» - неуспешное.

Таблица 1 - Проверка доступа пользователей

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Папка | Пользователь | Создавать внутри | Удалять внутри | Удалить саму папку | Подключение по сети | Добавление файлов по сети |
| Документы-Бим | bim | + | + | + | + | + |
|  | bom | - | - | - | - | - |
| Документы-Бом | bim | - | - | - | - | - |
|  | bom | + | + | + | + | + |
| Общие-Фото | pit | - | - | - | - | - |
|  | bim | - | - | - | - | - |
| Общие-Бланки | pit | - | - | - | + | - |
|  | bim | - | - | - | - | - |

Как видно из таблицы, пользователи *bim* и *bom* могут делать всё в «своих» папках *«Бим»* и *«Бом»*, так как ранее данным пользователям был дан доступ к папкам с уровнем *«Изменение»*. При этом с «чужими» папками данные пользователи сделать ничего не могут, ведь никаких соответствующих разрешений прописано не было. Пользователь *pit* также может подключиться по сети к папке *«Бланки»*, так как у него проставлено разрешение на чтение, однако больше в данной папке он ничего сделать не может. Пользователь *bim* во второй виртуальной машине также не может ничего сделать в папках *«Фото»* и *«Бланки»*, так как никаких разрешений ему дано не было.

**3. Настройка безопасности файлов при помощи шифрования**

На данном этапе первым делом на второй машине под пользователем *bim* в папке *«Общие»* было создано два текстовых файла (рисунок 8).

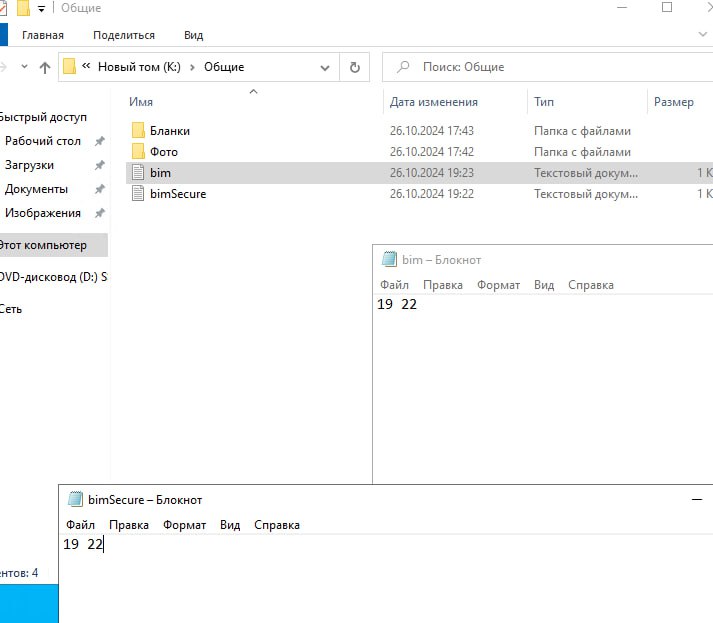


Рисунок 8 – Созданные текстовые файлы

Далее через удаленное подключение был осуществлен вход в систему под пользователем *pit*, и была предпринята попытка отредактировать и сохранить данные текстовые файлы. Это успешно получилось сделать, так как до этого у папки *«Общие»* были настроены разрешения для полного доступа в пределах локальной сети (рисунок 9).

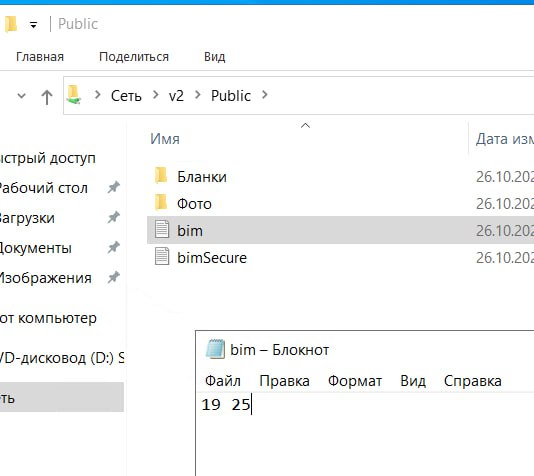


Рисунок 9 – Успешное редактирование файла под другим пользователем

Затем один из текстовых файлов был зашифрован пользователем, создавшим его. После этого второй пользователь уже не смог внести изменения в файл (рисунок 10).

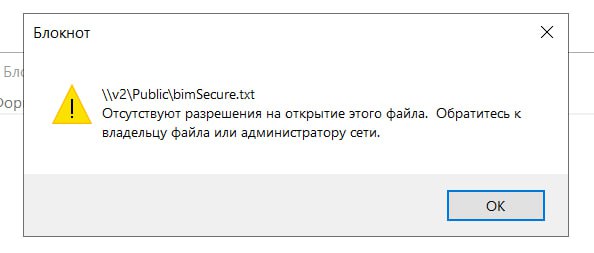


Рисунок 10 – Неудачная попытка открыть файл после шифрования

**4. Настройка доступа к сетевому принтеру**

На данном этапе первым делом в устройства компьютера был добавлен принтер с заданным IP-адресом (рисунок 11), после чего к нему сразу же был добавлен общий доступ.

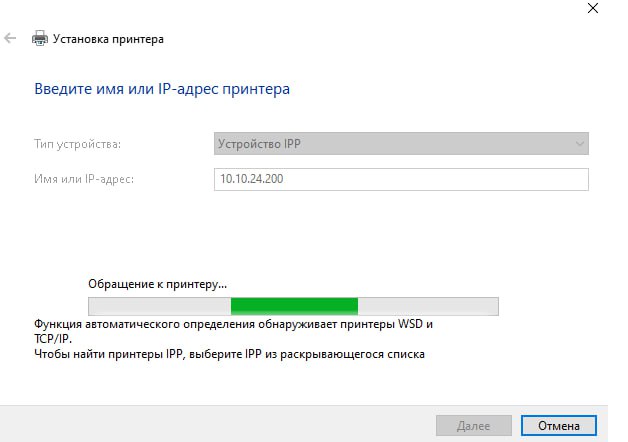


Рисунок 11 – Добавление принтера

После завершения установки драйвера в настройках безопасности вместо группы *Все* была добавлена созданная до этого группа *PrintUsers*: ей был дан доступ на печать (рисунок 12).

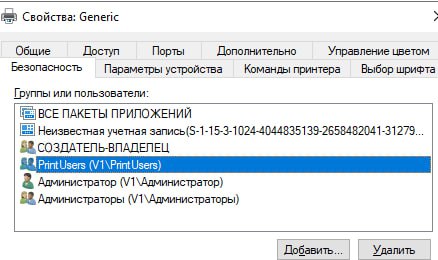


Рисунок 12 – Доступ группы PrintUsers

После этого доступ к принтеру был протестирован со стороны пользователей виртуальной машины *v1*, к которой был подключен принтер, а также со стороны одного из пользователей машины *v2*. Во всех случаях доступ к принтеру появился (рисунок 13), что говорит о том, что настройки доступа были выданы правильно.

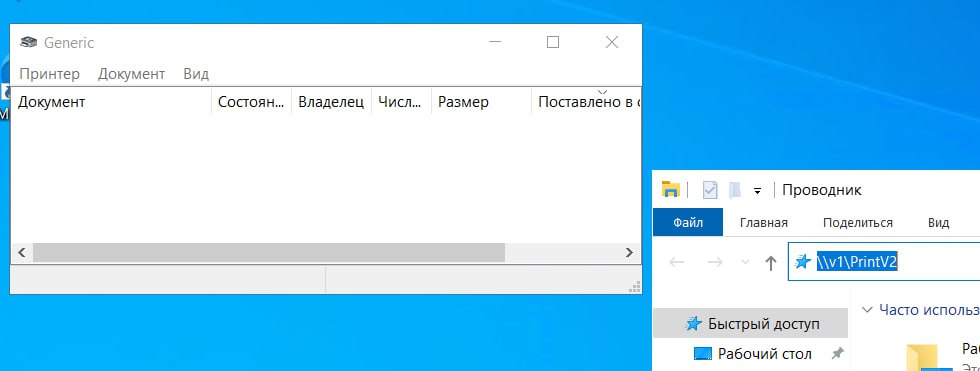


Рисунок 13 – Полученный доступ к принтеру

**Вывод:**

В ходе выполнения лабораторной работы были произведены настройки доступа и безопасности к различным ресурсам операционной системы. Первым делом были созданы учетные записи пользователей, затем были созданы каталоги и настроены уровни доступа к ним, в том числе и при работе через локальную сеть. Также была обеспечена безопасность файла с помощью его шифрования пользователем и, наконец, был подключен принтер с заданными настройкам доступа.

**Ответы на контрольные вопросы:**

*1. Можно ли с помощью учет. записи bim зайти на вирт. машину v2? Почему?*

Да, так как на v2 создана локальная учётная запись bim.

*2. Можно ли добавить учет. запись pit в группу PrintUsers? Почему?*

Нет, так как группа PrintUsers, находится на v1, а pit на v2.

*3. Смог ли пользователь bim получить доступ к папке \\v1\Docs\Бим? Почему?*

Смог, потому что в настройках доступа к этой папке был указан данный пользователь

*4. Как называется компьютер, который управляет подключением принтеров, предоставлением доступа к принтерам?*

Сервер печати.

*5. Что необходимо сделать, чтобы учет. запись pit с компьютера v2 получила доступ к ресурсам компьютера v1?*

Завести на v1 локальную учётную запись pit.

*6. Кто из пользователей bim, bom, pit получил доступ к принтеру? Почему?*

bim и bom - члены группы PrintUsers.