Лабораторная работа №3.

**СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ**

**ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА**

**Dallas Lock 8.0**

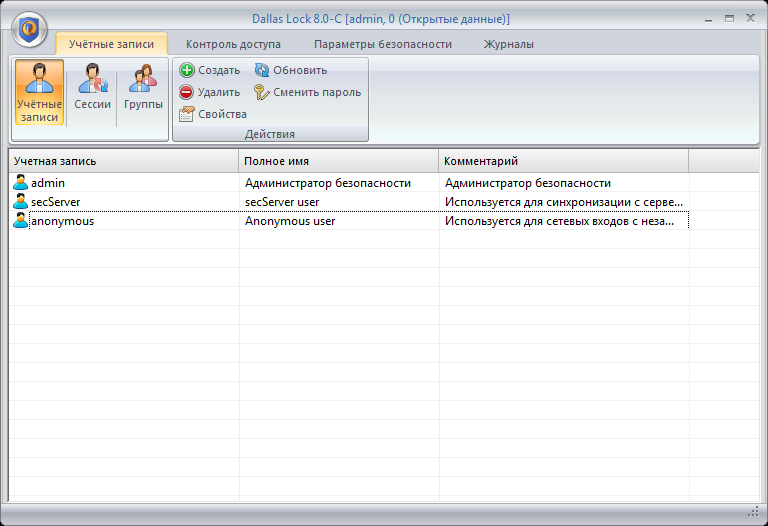
**Лабораторная работа №3**

Санкт-Петербург

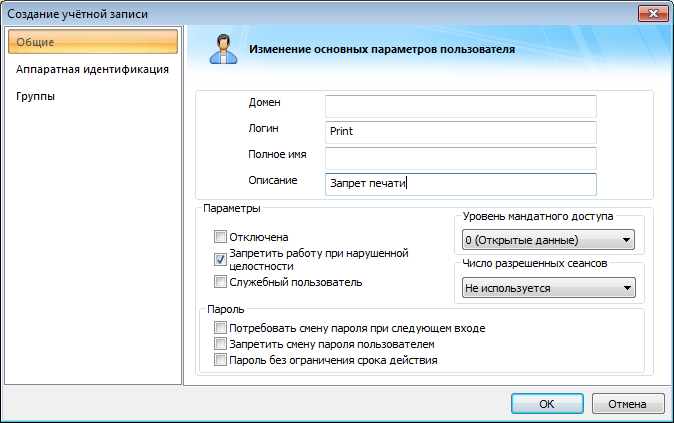
1. **Заходим в «VMware Workstation»**

Выполнить SnapShot «DALLAS» на машинах PAZUSERDALLAS, PAZUSERDALLAS2, PAZUSERDALLAS3 После чего можно запустить машины.

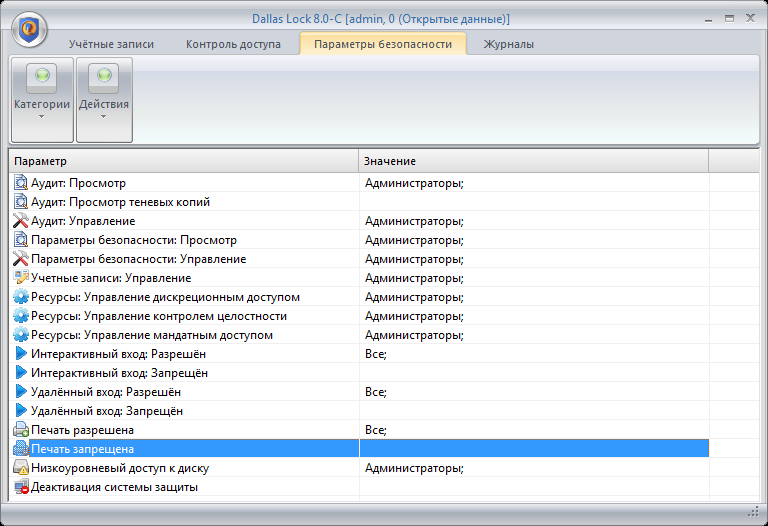
1. Открываем PAZUSERDALLAS (логин – admin, пароль - PAZ\_LOCAL1)
2. **Запрет печати.**
3. Открываем «Администратор Dallas Lock 8.0C»
4. Во вкладке «Учётные записи» создаем новую учётную запись при помощи кнопки «Создать»



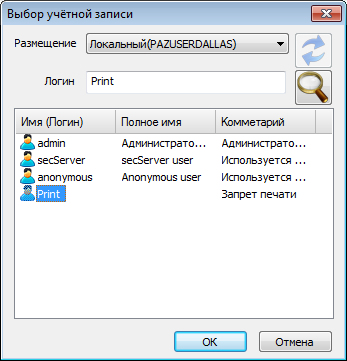
1. Вводим имя и задаем мандатный доступ.



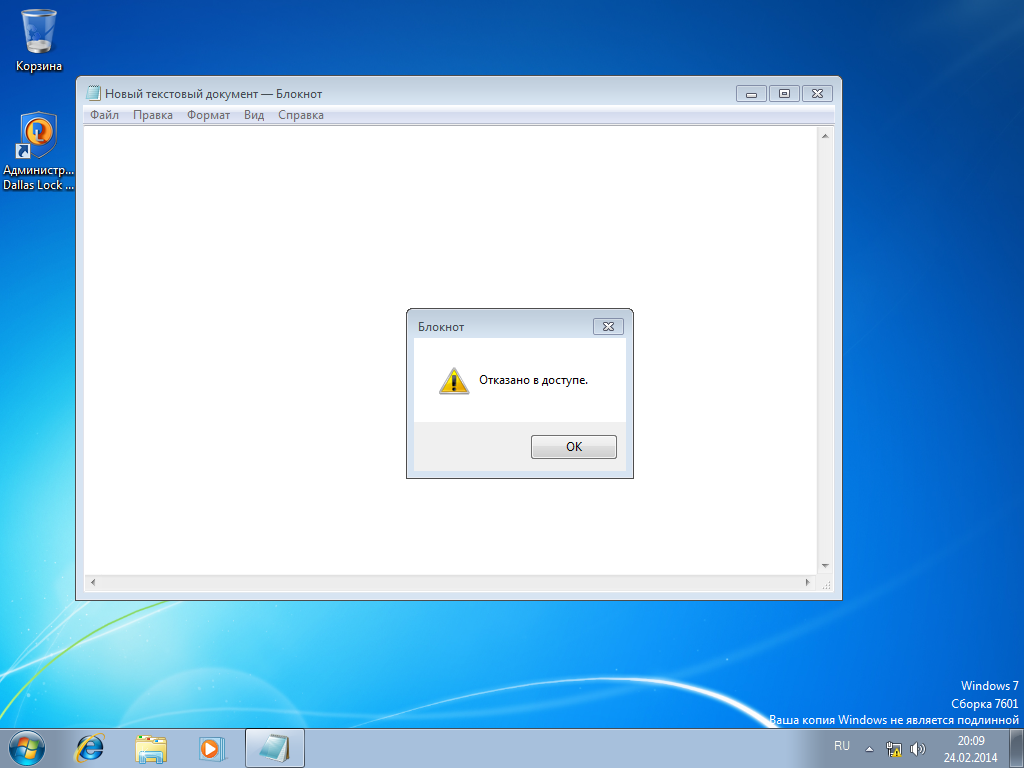
1. Создаем пароль (пароль не забываем).
2. Переходим на вкладку «Политики безопасности» и выбираем «Категории» - > «Права пользователя»



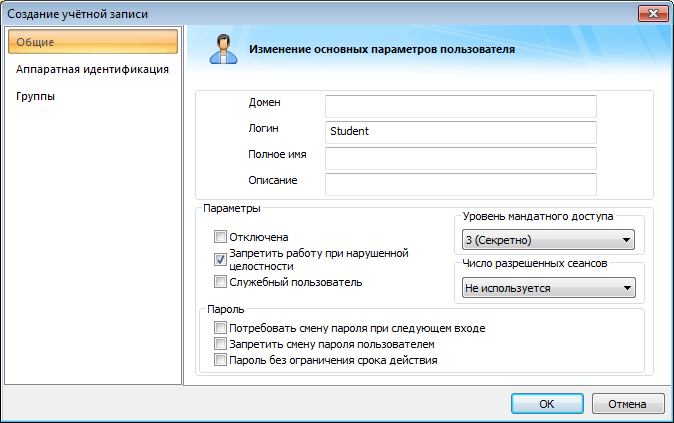
1. Выбираем параметр «Печать запрещена» и добавляем созданную учётную запись.



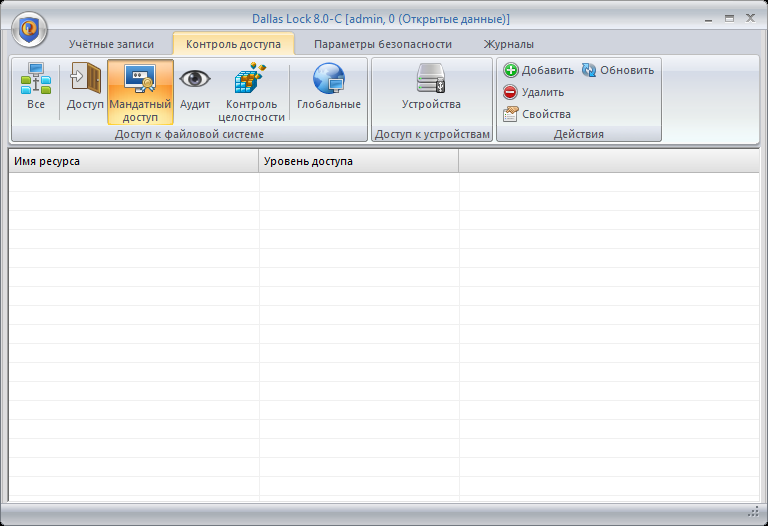
1. Закрываем «Dallas Lock», выходим из данной учётной записи и заходим в систему под учётной записью, которую вы создали.
2. Создаем любой текстовый файл и отправляем его на печать. Пробуем напечатать



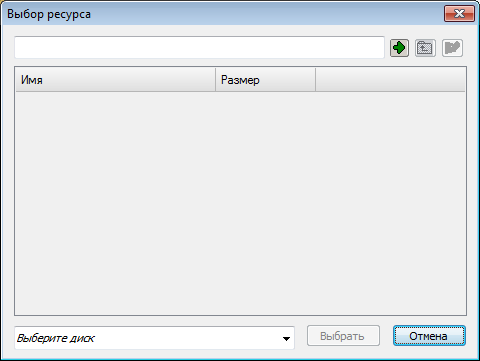
1. **Настройки мандатного доступ.**
2. Заходим под учётной записью «admin»
3. Создаем новую учётную запись в «Администратор Dallas Lock 8.0-C»
4. Присваиваем новой созданной учётной записи уровень мандатного доступа «Секретно».



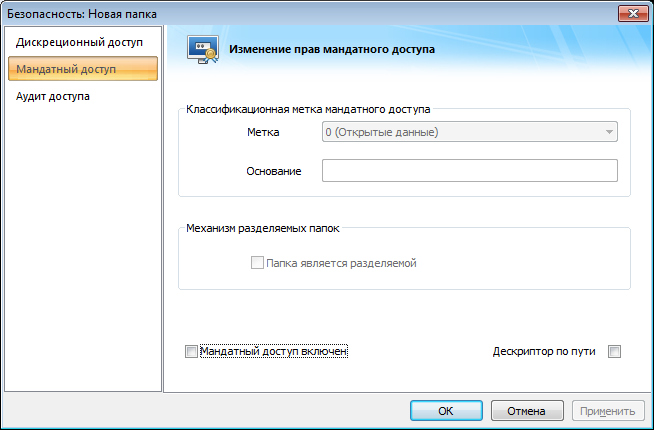
1. Создаем на диске C «Новая папка»
2. В панели Dallas Lock нажимаем «Контроль доступа», далее выбираем «Мандатный доступ». Нажимаем «Добавить»



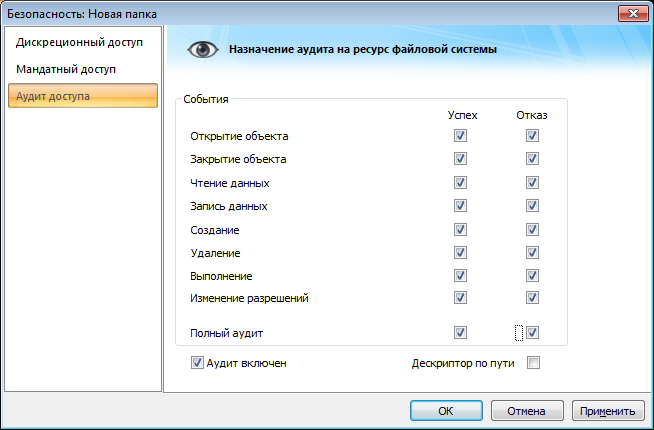
1. В открывшемся окне нажимаем выбрать диск.



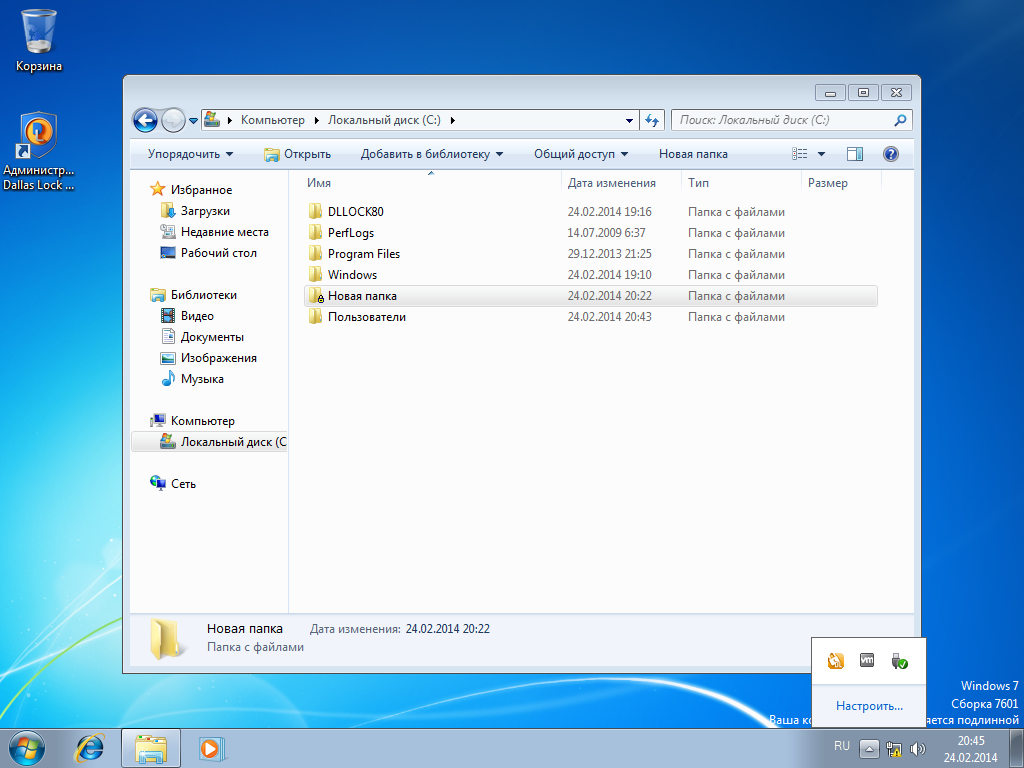
1. Находим созданную папку и добавляем.
2. Переходим во вкладку «Мандатный доступ»



1. Устанавливаем галочку «Мандатный доступ включен» и выбираем Метку «Секретно».
2. Переходим во вкладку «Аудит доступа». Устанавливаем галочки «Аудит включен». Выбираем «Полный аудит» при отказе и при успехе.



1. Заходим под новой учётной записью.
2. Пытаемся зайти в Новую папку. При данных настройках доступ должен быть запрещён.
3. Заходим в трэй, щёлкаем правой кнопкой на значке «Dallas Lock» и выбираем «Свойства пользователя»



1. Выбираем уровень доступа «Секретно»
2. Заходим на диск C и пытаемся зайти в Новую папку. При данных настройках доступ должен быть разрешён.
3. **Контроль целостности**
4. Заходим под учётной записью admin, пароль: PAZ\_LOCAL1
5. Создаем текстовый документ. Что-нибудь в него записываем.
6. Нажимаем правой кнопкой по данному текстовому документу заходим в Права доступа и переходим во вкладку Контроль целостности.
7. Ставим галочку Контроль целостности включен.
8. Выбираем алгоритм расчёта ГОСТ Р34.11-94
9. Нажимаем кнопку пересчитать. После чего происходит расчёт контрольной суммы. Нажимаем ОК.
10. Заходим снова в текстовый файл, редактируем его и сохраняем.
11. Снова щёлкаем правой кнопкой на файле заходим в Контроль целостности. Расчётная контрольная сумма должна измениться. Что это значит?
12. **Ввод компьютера в сервер Dallas Lock**
13. Заходим в компьютер PAZUSERDALLAS2 под учётной записью admin
14. Заходим в консоль сервера безопасности. Пароль всё тот PAZ\_LOCAL1
15. Переходим во вкладку Удалённая установка.
16. Нажимаем Сканировать сеть. Добавляем компьютер PAZUSERDALLAS3
17. Далее нажимаем Включить в Домен Безопасности (ДБ).
18. После чего данный компьютер должен появиться в списке клиентов.
19. Теперь переходим в журнал Сервера безопасности (СБ) Просмотрим его
20. Возвращаемся к PAZUSERDALLAS и снова меняем наш текстовый файл которому был задан контроль целостности. Сохраняем этот файл.
21. Так как работает это тугодумно, чтобы нам увидеть на сервере безопасности, что файл был изменён, щёлкаем правой кнопкой по файлу и снова переходим во вкладку контроль целостности. Видим что наш файл изменен, нажимаем пересчитать.
22. После чего возвращаемся в PAZUSERDALLAS2 и смотрим журнал(При необходимости нажимаем кнопку обновить)
23. **Механизм зачистки остаточной информации**

**Запрет смены пользователя без перезагрузки**

В системе защиты Dallas Lock 8.0-K подсистема очистки остаточной информации реализована механизмом очистки, который гарантирует предотвращение восстановления удаленных данных. Этот механизм позволяет принудительно зачищать определенные файлы и папки, используя соответствующий пункт в контекстном меню проводника (windows explorer).

Так же подсистема очистки остаточной информации с помощью политики «Запрет смены пользователя без перезагрузки» позволяет предотвращать возможность завершения сеанса работы одного пользователя и начала работы другого, что гарантирует освобождение используемых областей оперативной памяти. Удаление файлов и зачистка остаточной информации Большинство операционных систем при удалении файла не удаляют содержимое файла непосредственно, а всего лишь удаляют запись о файле из директории файловой системы.

Реальное содержимое файла остается на запоминающем устройстве, и его можно достаточно легко просмотреть, по крайней мере, до тех пор, пока операционная система заново не использует это пространство для хранения новых данных. Такая остаточная информация может легко привести к непреднамеренному распространению конфиденциальной информации. В СЗИ НСД Dallas Lock 8.0 функция очистки остаточной информации гарантирует предотвращение восстановления удаленных данных. Механизм очистки остаточной информации позволяет: принудительно зачищать определенные файлы и папки, используя соответствующий пункт в контекстном меню проводника;

предотвращать возможность завершения сеанса работы одного пользователя и начала работы другого, что гарантирует освобождение используемых областей оперативной памяти, с помощью политики «Запрет смены пользователя без перезагрузки».

При необходимости удалить какие-либо данные без возможности их восстановления нужно воспользоваться контекстным меню данного объекта файловой системы и выбрать пункт «DL8.0: Удалить и зачистить».



При активации удаления происходит зачистка данного объекта путем однократной перезаписи файла. После однократного цикла перезаписи восстановить хоть сколько-нибудь значимый фрагмент файла становится практически уже невозможно. После успешного удаления объектов система выведет соответствующее подтверждение.



В соответствии с требованиями политик безопасности организации возможно включение запрета смены пользователя компьютером без его перезагрузки. Включение этой политики производится: вкладка «Параметры безопасности» | категория «Вход» | параметр «Вход: запрет смены пользователя без перезагрузки».

Политика может принимать значение «Включен» или «Выключен». Включение данной политики («Вкл») не позволит осуществить смену пользователя без перезагрузки компьютера (рис.).



Если установлено значение «Выключен», то при выборе пункта «Завершение сеанса» в окне «Завершение работы Windows», компьютер автоматически уйдет на перезагрузку.



Данная политика позволяет предотвратить теоретическую возможность извлечения какой-либо информации из оперативной памяти ПЭВМ, оставшуюся там после завершения сеанса работы другого пользователя.