Лабораторная работа №6

РЕАЛИЗАЦИЯ МОДЕЛИ УПРАВЛЕНИЯ ДОСТУПОМ ПРИ ПОМОЩИ СЗИ НСД DALLAS LOCK

1. Цель и задачи работы

Получение навыков организации дискреционной и мандатной моделей доступа к объектам системы при помощи СЗИ НСД Dallas Lock

2. Теоретические положения

В качестве, целевого объекта на котором должна быть развёрнута система управления доступом выступает некоторое предприятие «Омега», в которой работают несколько групп специалистов, занятых работой над самостоятельными инженерными проектами. Документация проектов представляет собой ряд текстовых и графических электронных документов, обрабатываемых в единой компьютерной системе и имеющих различный уровень конфиденциальности: «открытые данные»,
«конфиденциально» и «строго конфиденциально».

Руководитель организации Клинов А.В. имеет максимальный уровень допуска к информации любого проекта. Экономист Ювченко А.Н. работает над проектом «Продажи». Администратор компьютерной системы Чистяков А.В. имеет полный доступ к любым документам, имеет возможность управлять настройками компьютерной системы и реализует на практике политику безопасности предприятия.

Для удобства работы всех пользователей автоматизированной системы в ее состав включена база данных, содержащая нормативно-правовые документы, требования единой системы программной документации (ЕСПД), технические справочники. Администратор следит за состоянием базы данных, своевременно обновляет ее.

Руководитель предприятия издает приказы и указания и размещает их в электронном виде в соответствующем каталоге. Сотрудники предприятия могут беспрепятственно знакомиться с содержимым базы данных и распоряжениями руководи-

теля предприятия, копировать необходимую им информацию, но вносить изменения в эти каталоги они не имеют право.

Уровни допуска сотрудников к секретной, для служебного пользования (ДСП), и несекретной информации представлены в таблице 4.1.

Таблица 4.1 -Уровни допуска сотрудников

Уровень допуска	Сотрудники
Несекретно	С.Ю. Соколов
ДСП	П.А. Савин, А.Н. Ювченко
Секретно	А.В. Свалов, А.В. Клинов, А.В. Чистяков

В зависимости от своих функциональных обязанностей сотрудники могут осуществлять различные действия с документами проекта: редактировать, просматривать, удалять, копировать, распечатывать.

В общем случае специалисты организации одновременно могут работать над несколькими проектами, но в нашем примере инженеры А.В. Свалов, П.А. Савин и С.Ю. Соколов заняты только проектом «Полет» и только к нему имеют доступ. В то же время они выполняют весь необходимый объем работы по данному проекту, поэтому доступ остальных инженеров предприятия к его документации запрещен.

Для предварительной проработки проектной документации инженеры могут создавать черновики документов. Черновики создаются в специальном каталоге для индивидуального пользования, они доступны только авторам, администратору и руководителю предприятия.

Права доступа сотрудников к документации предприятия разрешенного уровня конфиденциальности находят свое отражение в матрице доступа, которая вместе с установленной системой допусков и уровней конфиденциальности информационных ресурсов формализует политику разграничения доступа.

Возможный вариант матрицы, приведен в таблице 4.2, где буквой «П» обозначен тип доступа полный доступ, буквой «Ч» — только чтение, пробелом — запрет доступа.

Таблица 4.2 - Матрица доступа предприятия

Каталог	Соколов (инженер)	Савин (инженер)	Свалов (инженер)	Чистяков (администратор)	Ювченко (экономист)	Клинов (директор)
1	2	3	4	5	6	7
С:\Экономика\Канцелярские товары (НС)				П	П	П
С:\ Экономика\Продажи (ДСП)				П	П	П
С:\ Приказы и распоряжения	Ч	Ч	Ч	П	Ч	П
С:\ База данных (Консультант Плюс)	Ч	Ч	Ч	П	Ч	Ч
С:\Проекты\Полет\ Графические документы \Несекретно	П	П	П	П		П
С:\Проекты\Полет\ Графические документы \ДСП		П	П	П		П
С:\Проекты\Полет\ Графические документы \Секретно			П	П		П
С:\Проекты\Полет\ Текстовые документы \Несекретно	П	П	П	П		П
С:\Проекты\Полет\ Текстовые документы \ДСП		П	П	П		П
С:\Проекты\Полет\ Текстовые документы \Секретно			П	П		П
С:\Проекты\Полет\ Черновики\Соколов	П			П		П
С:\Проекты\Полет\ Черновики\Савин		П		П		П
С:\Проекты\Полет\ Черновики\Свалов			П	П		П

3. **Системные требования**
   1. Компьютер IBM PC, x86 или x64.
   2. Процессор не менее Pentium D с частотой не менее 1.7 ГГц.
   3. Не менее 2 ГБ ОЗУ
   4. Не менее 20 Гб ПЗУ.
   5. ОС Windows 7, или более новая разрядностью 32 или 64 бита.
   6. Наличие USB порта версии не менее 2.0
   7. Наличие открытого порта 80.
   8. Поддержка протокола TCP/IP.

9. Наличие установленной СЗИ Dallas Lock 8.0, или комплекта ПО, позволяющего произвести установку СЗИ Dallas Lock 8.0 на выбранный ПК.

4. **Постановка задачи**

Реализовать при помощи СЗИ Dallas Lock 8.0-C для компьютерной системы:

1. Дискреционную модель доступа;
2. Мандатную модель доступа.

Организацию можете выбрать на свое усмотрение, использовать вымышленную, или реальную, или использовать пример из теоретической части.

5. **Порядок выполнения работы**

Задача 1.

1. Зайдите в операционную систему с правами администратора. Создайте в системе каталоги, представленные в таблице 4.2. На рисунке 4.1 представлен результат формирования данных папок.

2. Создайте учетные записи для всех сотрудников организации, представленных в таблице 4.2 в программе администрирования «Dallas Lock». Информация по созданию учетных записей была рассмотрена в работе 3. Для директора организации и администратора предусмотрите использование аппаратной идентификации. На рисунке 4.2 представлен возможный результат создания учетных записей.

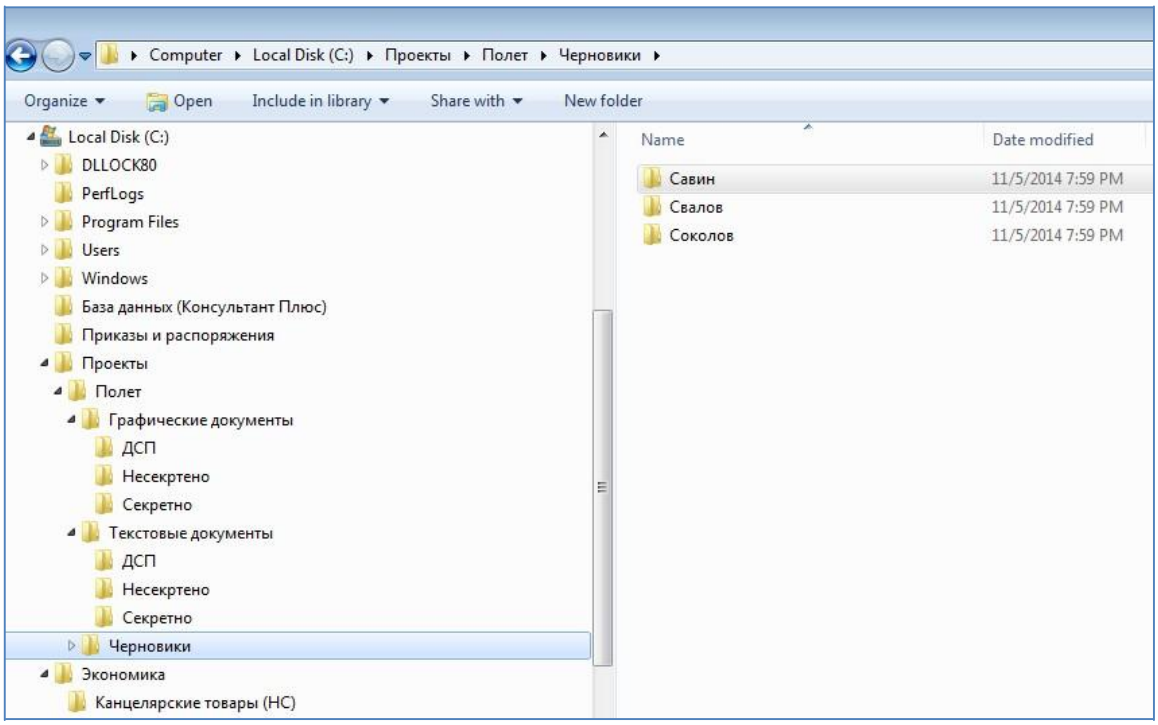

Рисунок 4.1 – Окно проводника Windows

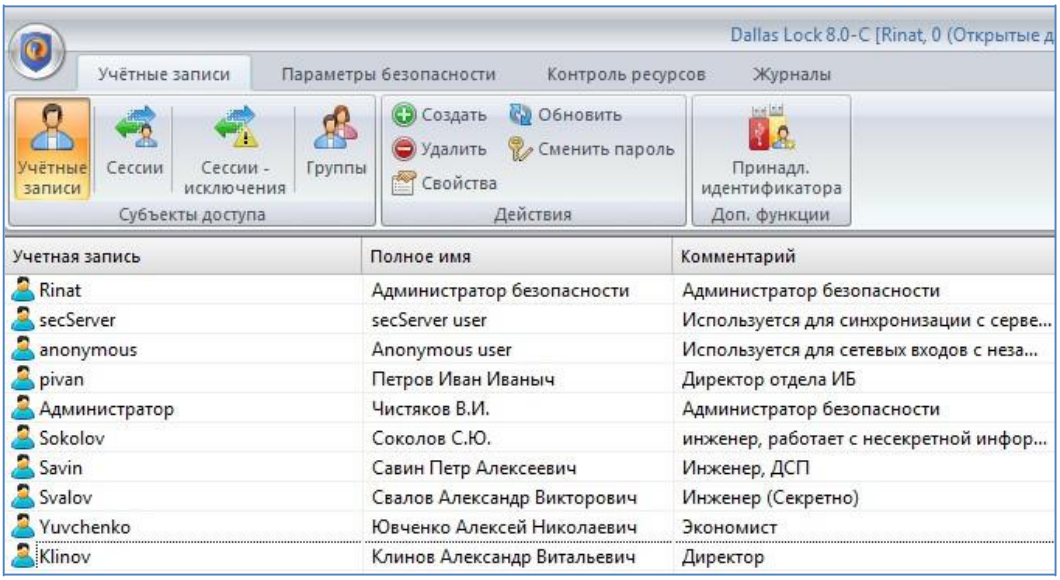

Рисунок 4.2 – Список учетных записей системы

3. Разграничьте права доступа пользователей к каталогу «C:\Экономика\Канцелярские товары (НС)» с учетом данных таблицы 4.2. Для этого перейдите к данному каталогу в проводнике Windows и нажатием ПК мыши вызовите контекстное меню, результат показан на рисунке 4.3.

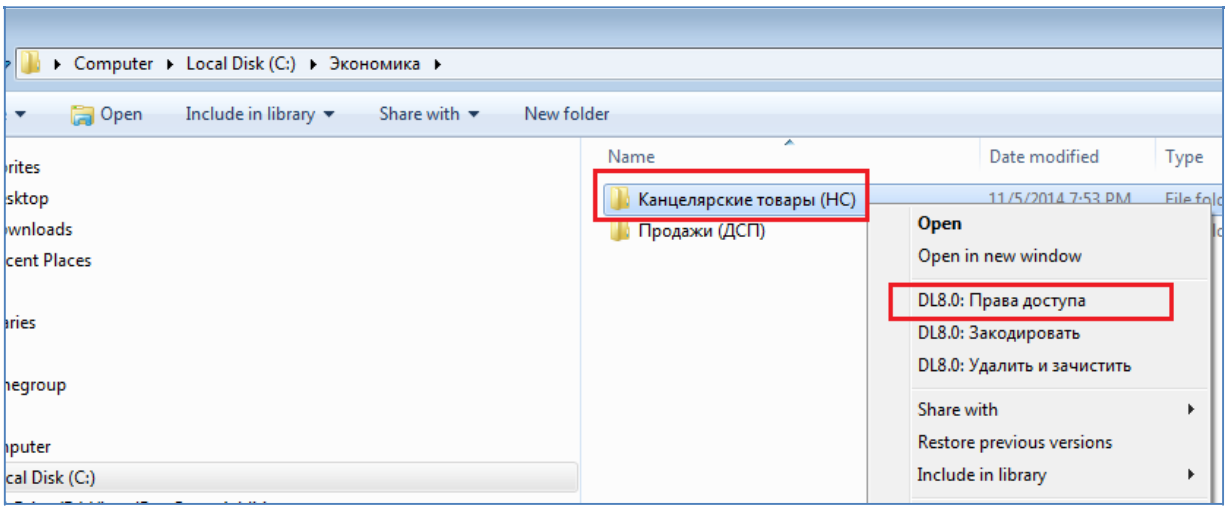

Рисунок 4.3 – Выбор команды «Права доступа»

4. В появившемся диалоговом окне выберите раздел «Дискреционный доступ». Нажмите на кнопку «Пользователи» для выбора учетной записи сотрудника. В списке учетных записей укажите определенного пользователя и нажмите кнопку «ОК». Таким образом, выберите учетные записи всех сотрудников организации из таблицы 4.2, для которых определены права доступа.

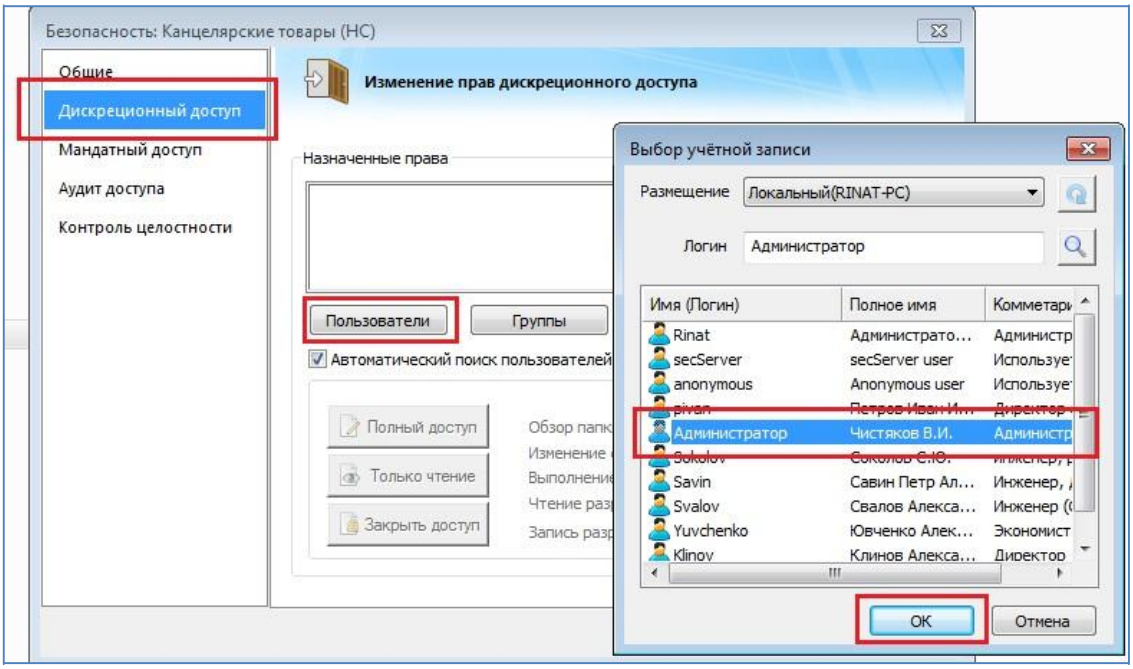

Рисунок 4.4 – Выбор учетной записи сотрудника

5. Нажмите кнопку «Все» для добавления в поле списка группы «Все(Everyone)».

6. Выделите учетную запись пользователя, которому нужно назначить права, и в поле разрешения/запрета операций с объектом выставьте значения флажков

согласно таблице 4.2. Для установки флажков прав доступа для типичных схем можно воспользоваться кнопками «Полный доступ», «Только чтение» и «Закрыть доступ». В частности, для пользователя «Администратор» назначьте права доступа нажатием кнопки «Полный доступ», как показано на рисунке 4.5.

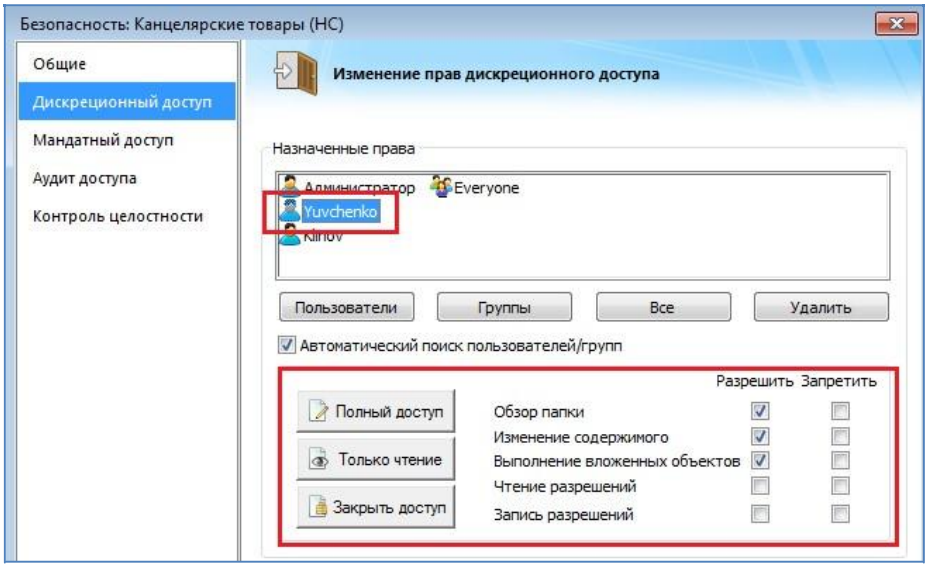

Рисунок 4.5 – Окно назначение прав доступа к объекту

7. Для группы «Все» выберите схему «Закрыть доступ».

8. Для пользователей директор и экономист разрешите все операции, кроме прав «Чтение разрешений» и «Запись разрешений».

9. Нажмите кнопки «Apply» и «OK» для подтверждения выбранных прав доступа пользователей к каталогу.

10. Аналогично, определите права доступа сотрудников к остальным папкам из таблицы 4.2. После назначения прав доступа пользователей в СЗИ Dallas Lock к графическому обозначению папки добавляется значок в виде замка, как показано на рисунке 4.6.

11. Выйдите из системы и зайдите под учетной записью пользователя Ювченко и просмотрите содержимое каталога «C:\Экономика». Убедитесь, что каталог «C:\Проекты\Полет\Графические документы\Не секретно» для этого пользователя недоступен. В результате вы должны получить сообщение о запрете доступа к папке, как показано на рисунке 4.7.

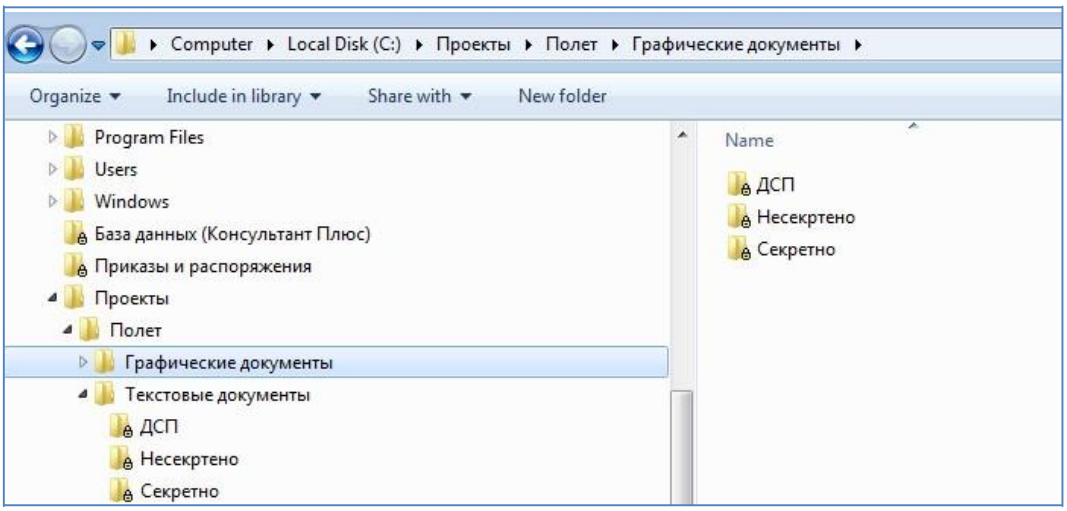

Рисунок 4.6 – Список каталогов с разграниченными правами доступа

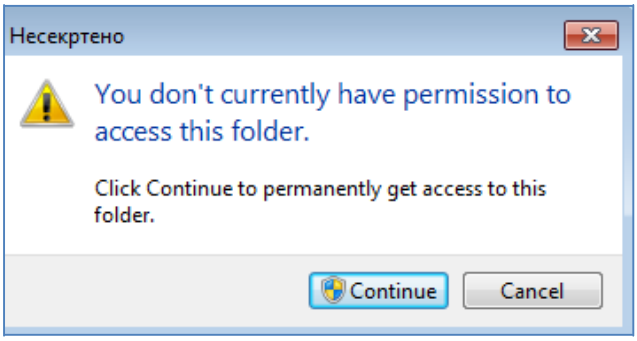

Рисунок 4.7 – Сообщение о запрете доступа к папке

12. Выйдите из системы и зайдите под учетной записью пользователя Свалов и просмотрите содержимое каталога «C:\Проекты\Полет\Текстовые документы \Секретно». Убедитесь, что каталог «C:\Экономика» недоступен.

13. Выйдите из системы и зайдите под учетной записью пользователя Клинов. Создайте в каталоге «C:\Приказы и распоряжения» текстовый файл «Приказ1.txt» с приказом об увольнении Савина.

14. Убедитесь, что Савин сможет прочитать приказ о своем увольнении, но не сможет изменить его.

Задача 2.

15. Зайдите в операционную систему с правами администратора. Запустите программу администрирования «Dallas Lock» и перейдите на вкладку «Учетные записи». Выберите пользователя «Администратор». Нажмите на кнопку «Свойства» и установите уровень мандатного доступа «Секретно», как показано на рисунке 4.8.

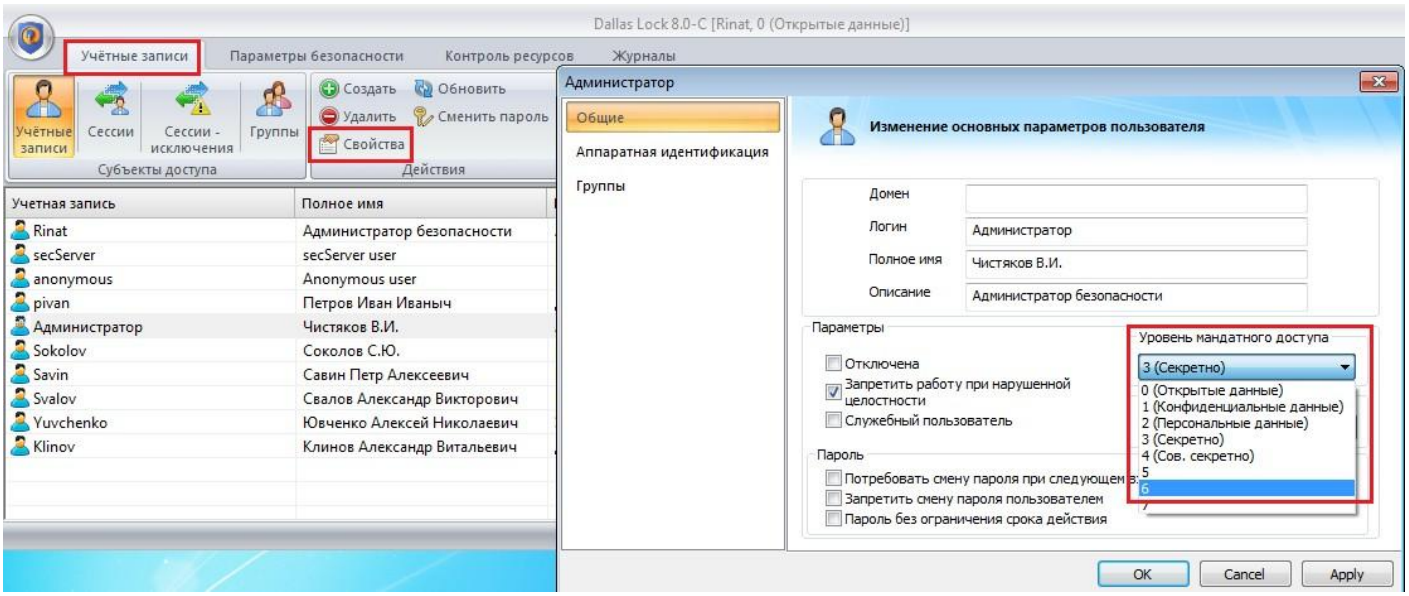

Рисунок 4.8 – Окно изменения свойств учетной записи

16. Назначьте уровни мандатного доступа для остальных сотрудников организации согласно таблице 4.1. В работе предлагается использовать стандартные уровни «Открытые данные», «Конфиденциальные данные» и «Секретно».

17. Перейдите при помощи проводника Windows к каталогу «C:\Проекты\Полет\ Графические документы \Несекретно» и нажмите ПК мыши. В появившемся контекстном меню выберите пункт «DL8.0: Права доступа».

18. В появившемся диалоговом окне выберите раздел «Мандатный доступ». В основной области окна выставьте флажок «Мандатный доступ включен» и выберите метку мандатного доступа «Открытые данные». Нажмите кнопку «OK».

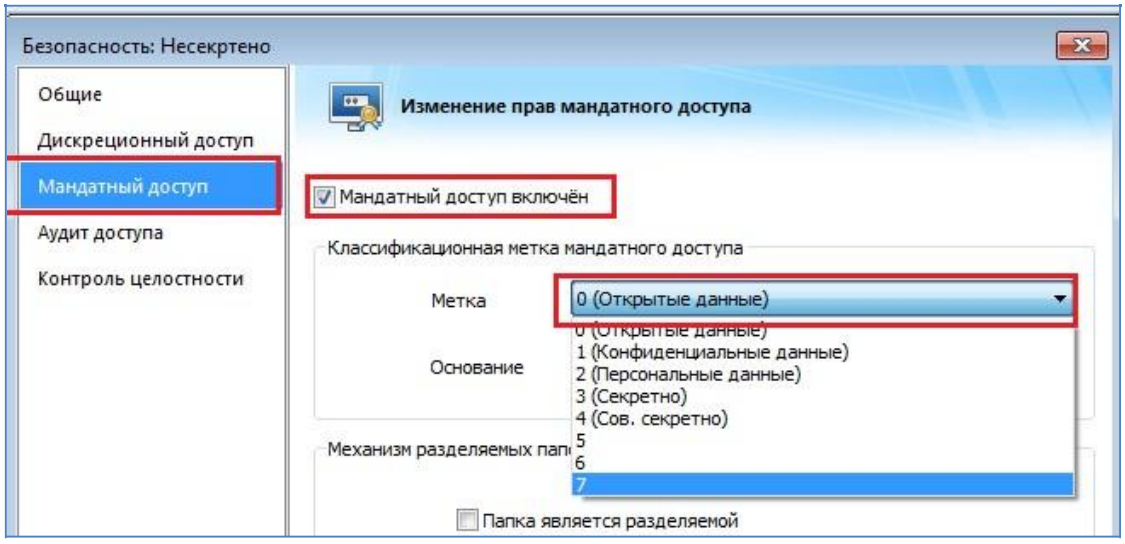

Рисунок 4.9 – Выбор метки доступа объекта файловой системы

19. Аналогично, определите метки доступа остальных каталогов из таблицы 4.2.

20. Просмотрите список ресурсов, для которых установлены метки доступа. Для этого перейдите на вкладку «Контроль ресурсов» и нажмите на кнопку «Мандатный доступ». На рисунке 4.10 представлен вариант определения меток доступа к определенным каталогам системы.

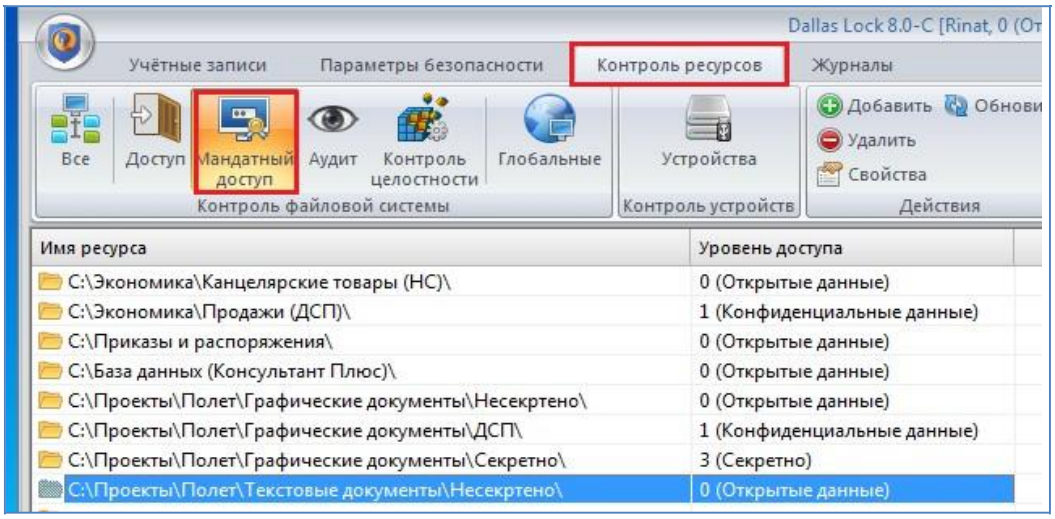

Рисунок 4.10 – Список ресурсов с метками доступа

21. Выйдите из системы и зайдите под пользователем Клинов, выбрав уровень допуска «Секретно», как показано на рисунке 4.11. Запустите «Проводник», просмотрите содержимое созданных каталогов. Все ли каталоги отображаются? Разрешено ли открыть данные каталоги?

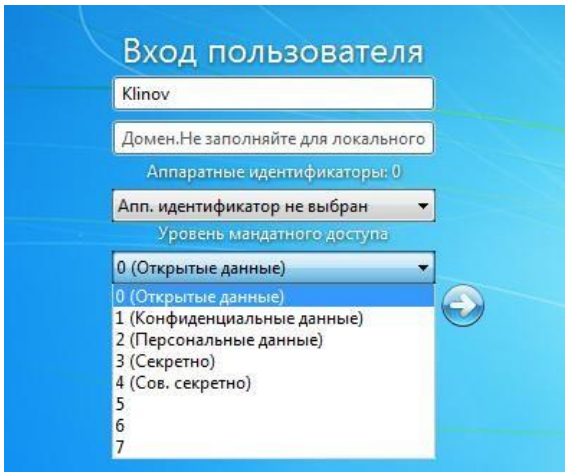

Рисунок 4.11 – Выбор метками доступа при входе в систему

22. Выйдите из системы и зайдите под учетной записью пользователя Соколов, выбрав уровень допуска «Конфиденциальные данные». Возможно ли это при

условии, что Соколов имеет допуск лишь к несекретным документам? При помощи

«Проводника» просмотреть содержимое созданных каталогов. Какие каталоги отображаются? Содержимое каких каталогов доступно данному пользователю?

23. Работая под учетной записью пользователя Соколов, создайте текстовый документ «Соколов.txt» и сохранить его в каталоге «C:\Проекты\ Полет\Текстовые документы\Несекретно».

24. Зайдите в систему под учтенной записью пользователя Свалов с макси- мальным текущим допуском («Секретно»), создайте текстовый документ «Свалов.txt» и попытайтесь сохранить его в каталог «C:\Проекты\Полет\Текстовыедокументы\Несекретно».
Получилось ли это? Сохраните документ в каталоге «C:\Проекты\ Полет\Текстовые документы\Секретно».

Контрольные вопросы

1. Дайте понятие дискреционной модели разграничения доступа.
2. Перечислите основные отличия механизмов дискреционной модели разграничения доступа СЗИ Dallas Lock и операционной системы семейства Windows
3. Какие основные операции с объектами файловой системы определены в СЗИ Dallas Lock.
4. Определите приоритеты применения прав доступа в дискреционной моде ли СЗИ Dallas Lock при пересечении на различных уровнях : файл, каталог, глобальные настройки.
5. В чем особенность разграничения прав доступа к сетевым ресурсам в СЗИ Dallas Lock?
6. В каких случаях для разграничения доступа к объектам файловой системы лучше использовать дескриптор по пути?