Лабораторная работа №4

НАСТРОЙКА ПОДСИСТЕМА УПРАВЛЕНИЯ ДОСТУПОМ СЗИ НСД DALLAS LOCK

1. **Цель и задачи работы**

Получение навыков работы с учетными записями в системе СЗИ от НСД

2**. Теоретические положения**

СЗИ НСД Dallas Lock 8.0-K может быть использован при создании защищенных автоматизированных систем до класса защищенности 1Г включительно, для обеспечения 1 уровня защищенности персональных данных и в информационных системах 1 класса защищѐнности [1, 8, 18, 20].

Данное средство защиты обладает широкими возможностями, среди которых выделяются следующие функции:

– обеспечение дискреционного и мандатного метода доступа;

– обеспечивает механизм доверенной загрузки;

– обеспечивает контроль целостности программно-аппаратной среды и реестра;

– реализует механизм аппаратной идентификации пользователей с использованием распространенных электронных идентификаторов(USB-Flash-накопители, iButton, Aladdin eToken, Rutoken, JaCarta).

СЗИ Dallas Lock предназначен для использования в ОС семейства Windows. Подсистема разграничения доступа средства защиты интегрируется в операционную систему. В частности это означает, что регистрация новых пользователей и групп в системе Dallas Lock приведет к автоматическому созданию учетных записей в ОС.

Достоинством данного СЗИ является простота установки, многообразие функций по защите информации от несанкционированного доступа, наличие сертификата ФСТЭК.

К недостаткам можно отнести программную реализацию, что предполагает возможность модификации злоумышленником.

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**

1. Установить СЗИ Dallas Lock, в случае если установка не была произведена ранее;
2. Создать учетную запись нового пользователя в СЗИ Dallas Lock;
3. Создать группу и включите в неѐ вновь созданного пользователя.
4. Настроить вход в систему пользователя при помощи аппаратного идентификатора.
5. Проверить корректность работы системы управления доступом, настроенной, на основе пунктов 1-4.

5. **Порядок выполнения работы**

1. Перед установкой системы защиты Dallas Lock 8.0 необходимо выполнить следующие действия:

– если на компьютере уже установлена система защиты, ее необходимо удалить;

– проверить состояние жестких дисков компьютера и устранить выявленные

дефекты;

– рекомендуется произвести дефрагментацию диска;

– проверить компьютер на отсутствие вирусов;

– перед установкой системы защиты необходимо выгрузить из памяти все ре- зидентные антивирусы.

2. Рекомендуется отключить кэширование записи для всех дисков. Для отключения кэширования записи необходимо:

– в консоли управления компьютером открыть «Диспетчер устройств»;

– выбрать в узле дерева консоли «Дисковые устройства» диск, в его контекстном меню выбрать пункт «Свойства» и в появившемся диалоге открыть вкладку «Политика»;

– снять флажок в поле «Разрешить кэширование записи на диск» («Включить кэширование записи») и нажать кнопку «ОК». Повторить вышеуказанные действия для всех дисков.

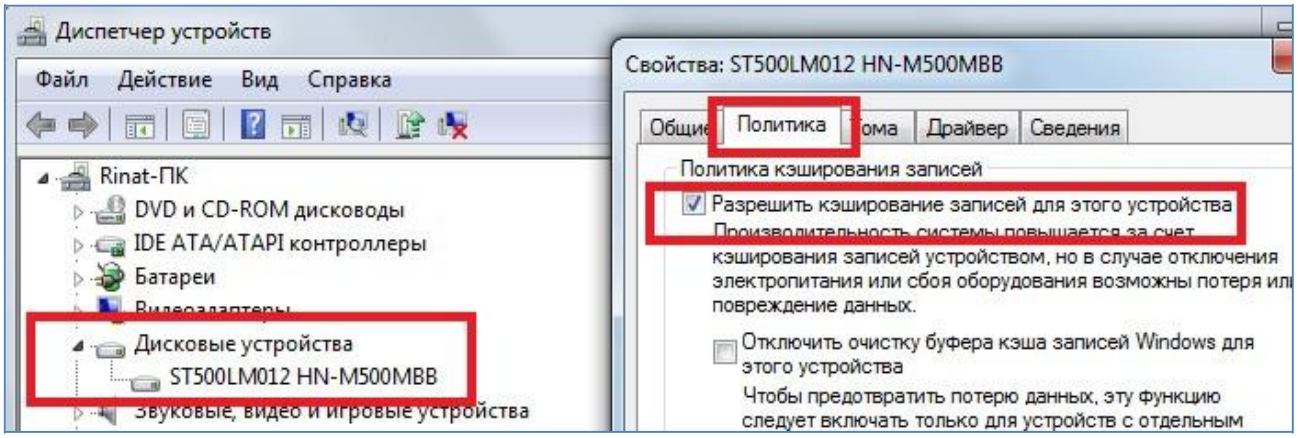

Рисунок 2.1 – Окно отключения кэширования диска

3. Запустите приложение DallasLock8.0C.msi (DallasLock8.0K.msi), которое находится в корневой директории дистрибутива. При установке системы защиты на компьютере с установленной ОС Vista и выше после запуска приложения, на экране будет выведено окно для подтверждения операции.

4. Для установки необходимо нажать кнопку «Начать установку», после чего программа установки приступит к инсталляции.

Введите только серийный но- мер лицензии Dallas Lock 8.0, который указан на обложке компакт-диска с дистри- бутивом в поле «Серийный номер» (например, 99099-1735-646). Остальные поля не заполняйте.

5. После нажатия кнопки «Далее» процесс установки системы защиты будет завершен. Нажмите кнопку «Перезагрузка». После перезагрузки первый вход на за- щищенный компьютер сможет осуществить пользователь, под учетной записью ко- торого выполнялась инсталляция системы защиты Dallas Lock 8.0, как показано на рисунке 2.2.

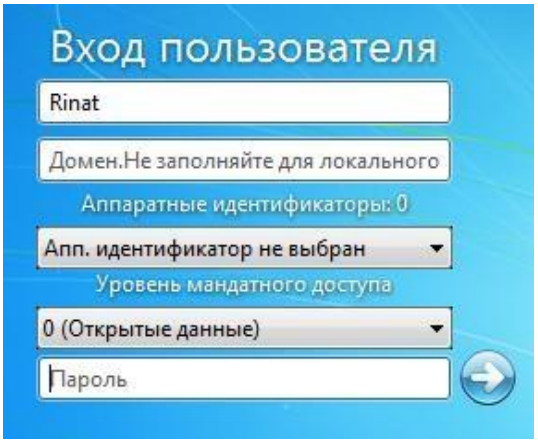

Рисунок 2.2 – Окно входа в систему

6. Вызовите программу администрирования СЗИ Dallas Lock двойным щелч- ком мыши на ее значке, появившемся на рабочем столе, или через меню «Пуск».

7. Выделите категорию «Учетные записи» в оболочке администратора и нажмите кнопку «Создать» в категориях «Действия». В результате появится окно создания новой учетной записи (рисунок 2.3).

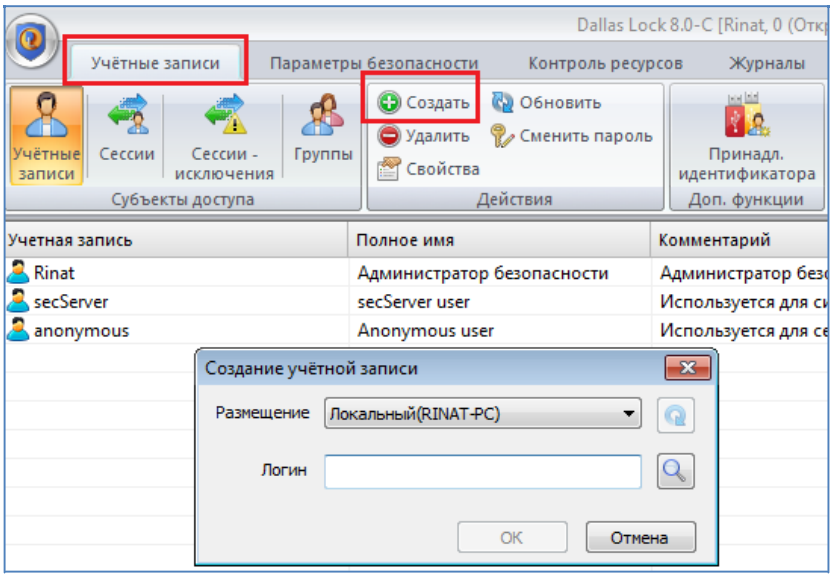

Рисунок 2.3 – Диалоговое окно «Создание учетной записи»

8. В поле «Размещение» укажите значение «Локальный» и введите логин пользователя, например, «pivan» . Нажмите кнопку «OK».

9. В появившемся диалоговом окне перейдите на вкладку «Общие». Поле «Домен» оставляете пустым. В поле «**Полное имя**» вводите имя пользователя. Пример задания параметров пользователя представлен на рисунке 2.4.

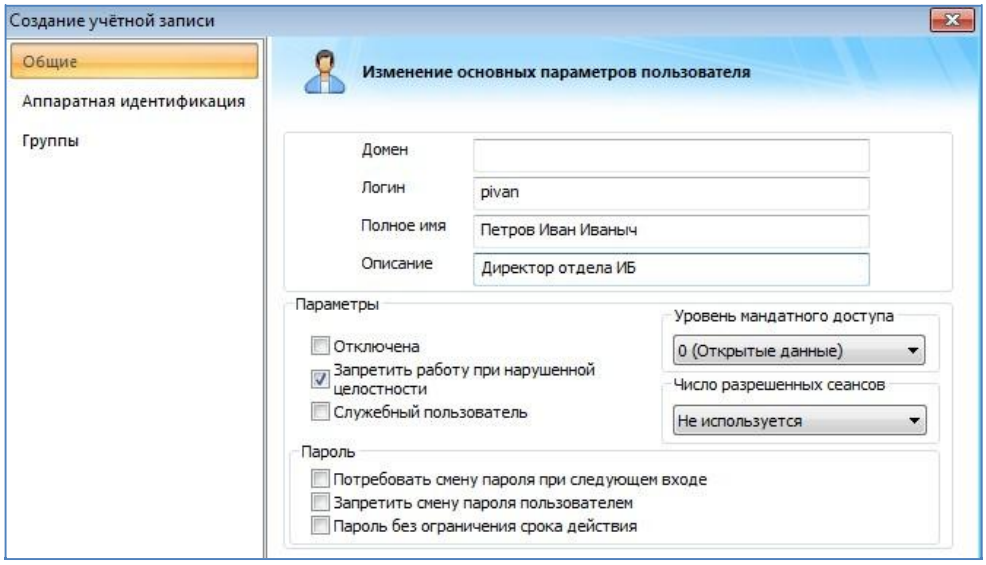

Рисунок 2.4 – Окно задания параметров учетной записи на вкладке «Общие»

10. Перейдите на вкладку «Группы». Нажмите кнопку «Добавить» и в поя- вившемся диалоговом окне «Выбор группы» выберите группу «Администраторы». Подтвердите выбор группы,

нажав кнопку «ОК» (рисунок 2.5).

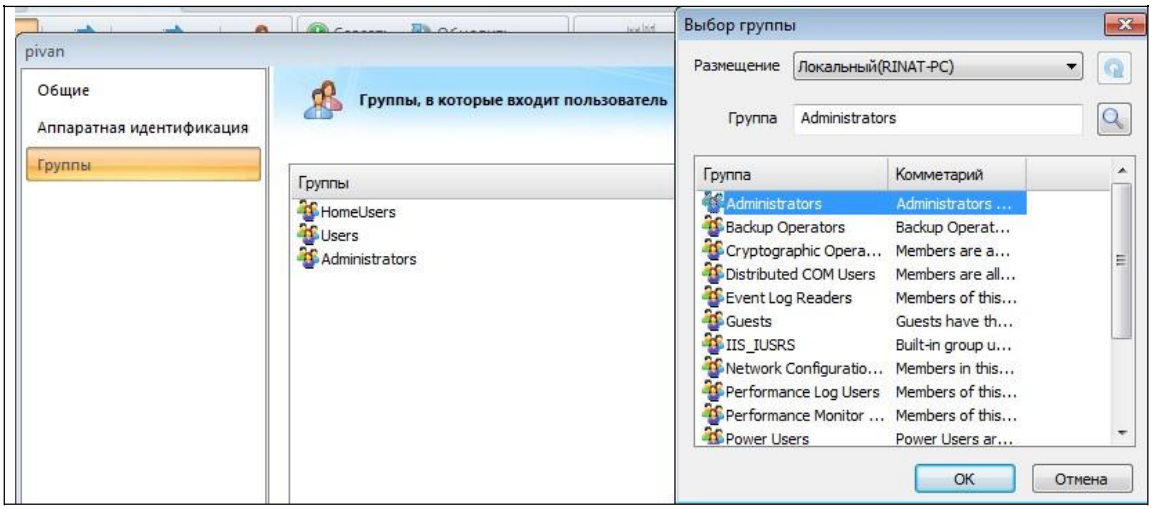

Рисунок 2.5 – Диалоговое окно выбора группы учетной записи

11. Далее нажмите кнопку «ОК», чтобы подтвердить выбранные параметры учетной записи. В появившемся диалоговом окне «Пароль пользователя» нажмите кнопку «Генерация пароля». Введите предложенное значение пароля в поля «Па- роль» и «Подтверждение» (рисунок 2.6).

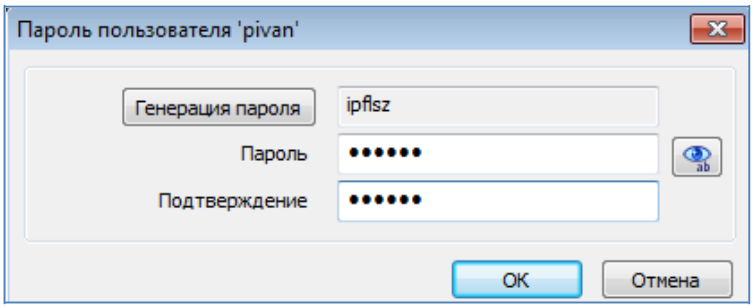

Рисунок 2.6 – Задание пароля пользователя

12. На вкладке «Учетные записи» нажмите на значок «Группы». В области действия выберите значок «Создать». В появившемся окне введите название группы
«Security»и еѐ описание.

13. Нажмите на значок «Учетные записи». В списке ниже выберите пользо- вателя «pivan» и нажмите кнопку «Свойства в области действий». Добавьте данного пользователя в группу «Security».

14. Закройте программу администрирования «Dallas Lock 8.0». Установите драйвер «Рутокен», запустив файл rtDriversxxx.exe.

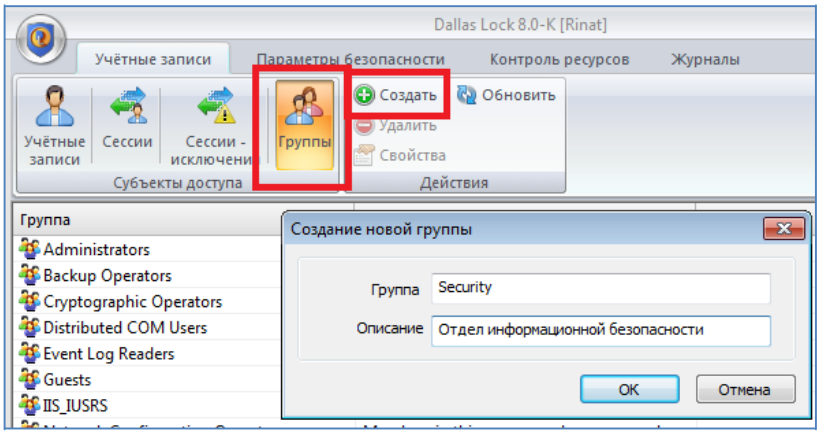

Рисунок 2.7 – Задание пароля пользователя

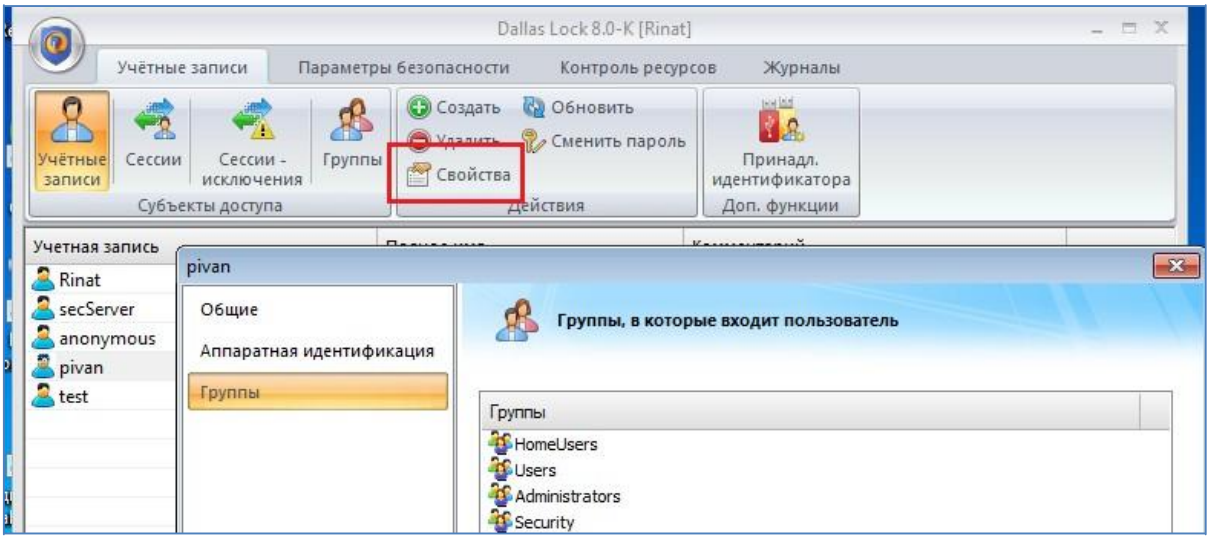

Рисунок 2.8 – Окно редактирования свойств учетной записи

15. Запустите программу администрирования «Dallas Lock 8.0» и перейдите на вкладку «Параметры безопасности». На данной вкладке выберите пункт «Вход». В появившемся ниже списке параметров выберите «Настройка считывателей аппа- ратных идентификаторов» и двойным щелчком ЛК мыши откройте диалоговое окно «Настройка средств аппаратной идентификации» (рисунок 2.9).

16. Выделите считыватели «USB flash drive» и «Рутокен». Подтвердите вы- бор, нажав кнопку «OK». Перезагрузите компьютер.

17. Установите в ПК «Рутокен» или флэш-накопитель .

18. Перейдите на вкладку «Учетные записи» и выберите пользователя «pi- van». Откройте окно редактирования параметров учетной записи, нажав кнопку «Свойства». В открывшемся диалоговом окне выберите пункт

«Аппаратная иденти- фикация». Убедитесь, что значение поля «Предъявленные аппаратные идентификаторы», установлены значение которых больше 0.

19. Если у Вас нет «Рутокен», а только флэш-накопитель, то выберите его и перейдите к шагу 22.

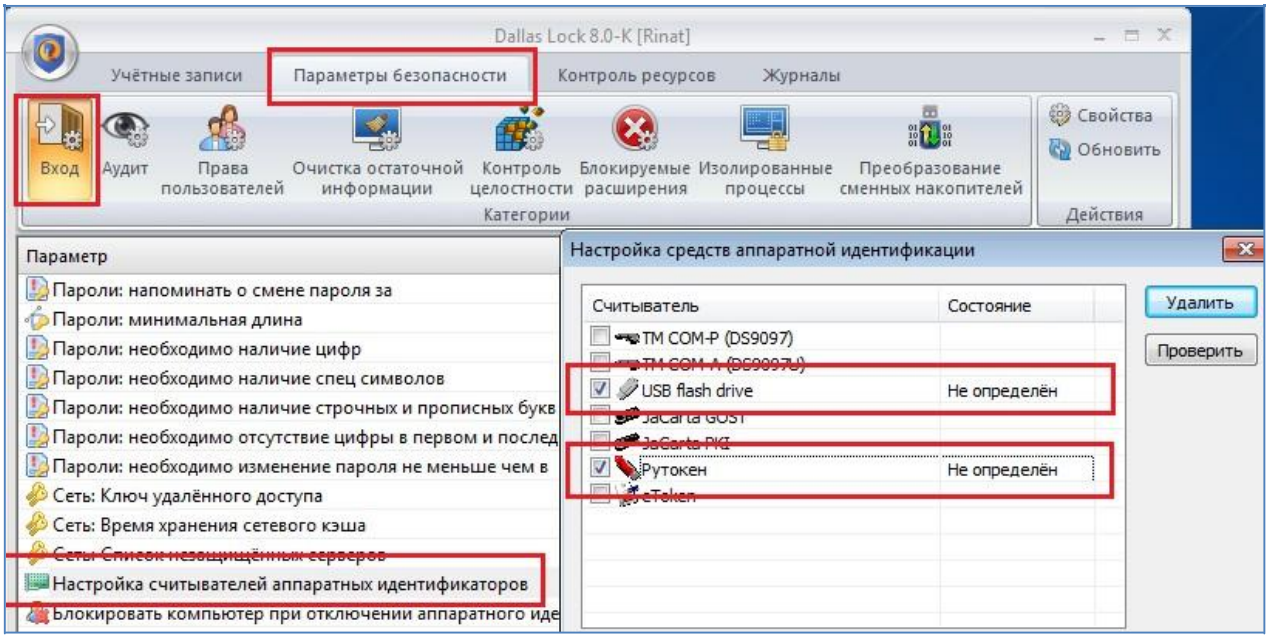

Рисунок 2.9 – Настройка аппаратных считывателей

20. Выберите аппаратный ключ «Рутокен» в поле идентификатор. Выставьте флажки «Пароль хранится в идентификаторе» и «Пароль защищен PIN кодом». Для сохранения пароля на аппаратный носитель нажмите кнопку «Записать» (Рис. 2.10).

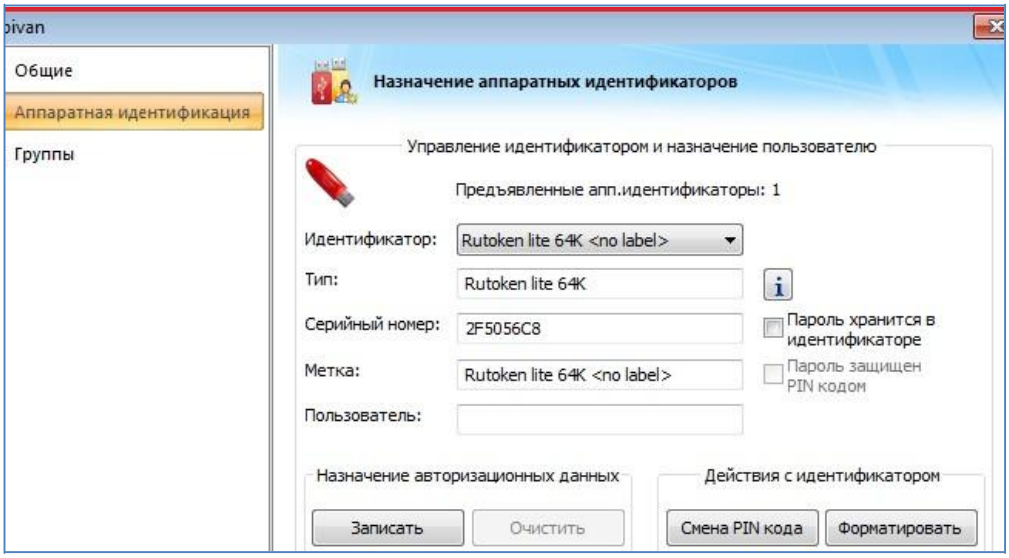

Рисунок 2.10 – Окно настройки аппаратной идентификации

21. В появившемся окне «Ввод дополнительной информации» введите цифровой PIN-код и пароль пользователя (рисунок 2.11). Нажмите кнопку «OK».

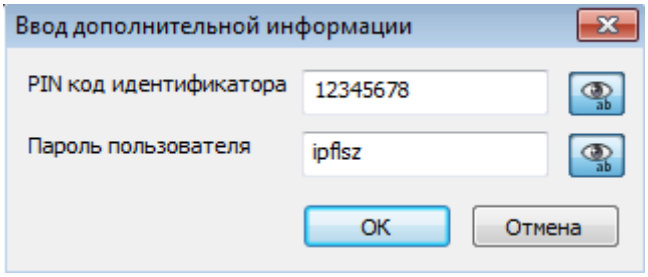

Рисунок 2.11 – Ввод идентификационных данных пользователя

22. В окне настройки учетной записи нажмите кнопки «Apply» и «OK».

23. Закройте программу администрирования Dallas Lock 8.0 и выйдите из операционной системы.

24. В окне входа пользователя в систему в поле «Аппаратный идентифика- тор» выберите «Рутокен» или флэш-накопитель (рисунок 2.12).

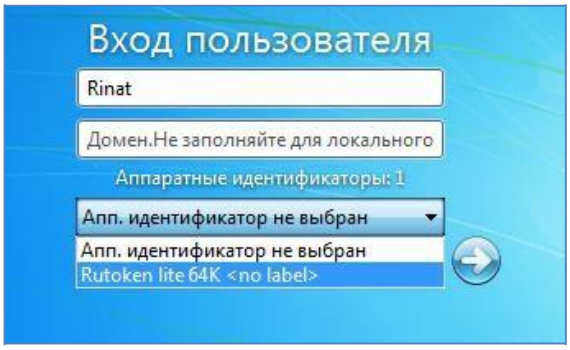

Рисунок 2.12 – Выбор аппаратного идентификатора для входа в ОС

25. При использовании Рутокен необходимо ввести только PIN-код пользователя. В случае использования флэш-накопителя – пароль пользователя.

2.6 Ответить на контрольные вопросы и сделать выводы по работе.

Контрольные вопросы

1. Область применения СЗИ Dallas Lock 8/0-С.
2. Какими возможностями обладает СЗИ Dallas Lock
3. Повышает ли уровень защищенности системы использование механизма аппаратной идентификации
4. В чем недостаток использования USB-Flash-накопителя в качестве электронного идентификаторы
5. Перечислите основные достоинства и недостатки СЗИ Dallas Lock.