

ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ
Сибкон Про

Система авторизации пользователей в сети Windows NT/2000
SecureCard

Руководство пользователя

Иркутск - 2002

Оглавление

Система авторизации пользователей по смарт-карте в сети Windows NT/2000 "SecureCard" ...	3
Назначение	3
Описание системы "SecureCard"	3
Установка системы "SecureCard"	4
Установка аппаратного обеспечения системы	4
Установка программного обеспечения	5
Удаление (деинсталляция) программного обеспечения системы SecureCard	5
Работа с системой "SecureCard"	7
Программа AdminTool	7
Функции, реализованные в программе AdminTool:	7
Работа с программой AdminTool.....	7
Вход в систему	7
Главное окно программы.....	7
Назначение кнопок панели инструментов:	8
Создание нового пользователя.....	8
Регистрация пользователя и запись карты	8
Регистрация пользователя без наличия карты	9
Запись карты для существующего пользователя	10
Изменение владельца карты	11
Смена пароля пользователя	11
Определение владельца карты	12
Удаление пользователя и очистка карты.....	12
Удаление пользователя без наличия карты.....	12
Запрещение/разрешение входа пользователя.....	14
Подсистема входа в сеть и авторизации пользователя	15
Особенности работы с подсистемой входа в сеть и авторизации пользователя	15
Вход в систему при помощи смарт-карты	15
Блокирование компьютера	15
Выход из системы.....	15
Список возможных ошибок.....	17
При создании нового пользователя:.....	17
При смене пароля пользователя:	17
При удалении пользователя при наличии карты:.....	18
При попытке входа в сеть:	19

Система авторизации пользователей по смарт-карте в сети Windows NT/2000 "SecureCard"

Назначение

В качестве защиты от несанкционированного доступа к сети или к конфиденциальной информации очень часто используют систему паролей. Для того чтобы такая защита была действительно надежной, необходимо использовать длинные пароли, содержащие специальные символы, буквы и цифры. Запоминать такие пароли очень не простая задача, кроме того, пароли приходится периодически менять.

Система "SecureCard" позволит в значительной степени облегчить задачу обеспечения безопасности Вашей системы и надежности её парольной защиты. Система "SecureCard" предназначена для записи и хранения паролей пользователя сети на смарт-картах.

В качестве инструмента авторизации пользователя в сети Windows NT/2000 система "SecureCard" позволяет использовать смарт-карту. Пароль пользователя автоматически генерируется системой и записывается на смарт-карту, где надежно хранится. Карта выдается пользователю и используется им для входа в сеть. При входе в систему пароль автоматически считывается со смарт-карты. В случае прерывания сеанса работы, пользователь с помощью смарт-карты может заблокировать компьютер.

Описание системы "SecureCard"

Система "SecureCard" включает в себя аппаратную (устройство чтения/записи смарт-карт) и программную части. Программная часть состоит из ПО администратора сети (**AdminTool**) и клиентского ПО.

ПО администратора устанавливается только на компьютере администратора сети, предназначено для регистрации пользователей, записи данных на смарт-карты и управления смарт-картами в сети.

Клиентское ПО – подсистема входа и авторизации пользователя – устанавливается на компьютер пользователя сети и осуществляет авторизацию и вход пользователя в сеть по смарт-карте. Предусмотрена также возможность входа в систему стандартным способом, принятым в ОС Windows, при помощи ввода имени и пароля с клавиатуры.

ПО AdminTool позволяет администратору сети производить необходимые манипуляции с картами пользователей:

- Регистрация пользователя и запись его карты, при этом программа сама сгенерирует пароль пользователя и произведет запись данных на карту;
- Смена пароля пользователя;
- Блокирование карты и запрещение входа в систему;
- Удаление пользователя и очистка карты.

Рабочая станция пользователя сети оснащается ридером, предназначенным для чтения смарт-карт. С помощью установленного оборудования и клиентского ПО системы, вход пользователя в сеть осуществляется по зарегистрированной смарт-карте, при входе пароль автоматически считывается с карты.

Используемая в системе смарт-карта – контактная чиповая карта памяти с чипом SIEMENS SLE4418/SLE4428.

Установка системы "SecureCard"

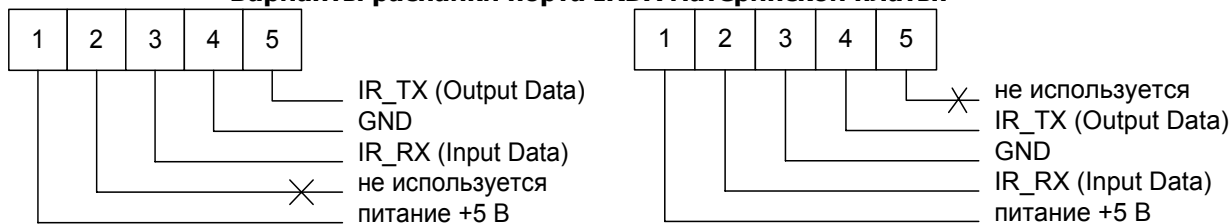
Установка аппаратного обеспечения системы

Ридер с помощью соединительного шлейфа подключается к разъему IrDa материнской платы, а само устройство устанавливается в отсек дисководов 3,5" и располагается внутри корпуса системного блока компьютера.

Перед подключением ридера в документации на материнскую плату необходимо уточнить расположение разъема IrDa порта, нумерацию выводов и способ распайки порта.

В комплекте с ридером поставляются два пронумерованных соединительных шлейфа. В зависимости от распайки порта IRDA для подключения к материнской плате используйте соединитель N1 или N2 (способ распайки порта IrDa материнской платы Вашего компьютера следует уточнить в технической документации).

Варианты распайки порта IRDA материнской платы:



Использовать соединитель № 1

Использовать соединитель № 2

Подключение ридера к порту Irda материнской платы показано на схеме 1. При подключении ридера к порту IrDa первый провод соединительного шлейфа (он отмечен красным цветом) должен быть подключен к контакту номер один разъема Irda порта. К ридеру шлейф подключается таким образом, чтобы первый (красный) провод оказался с крайней стороны разъема ридера.

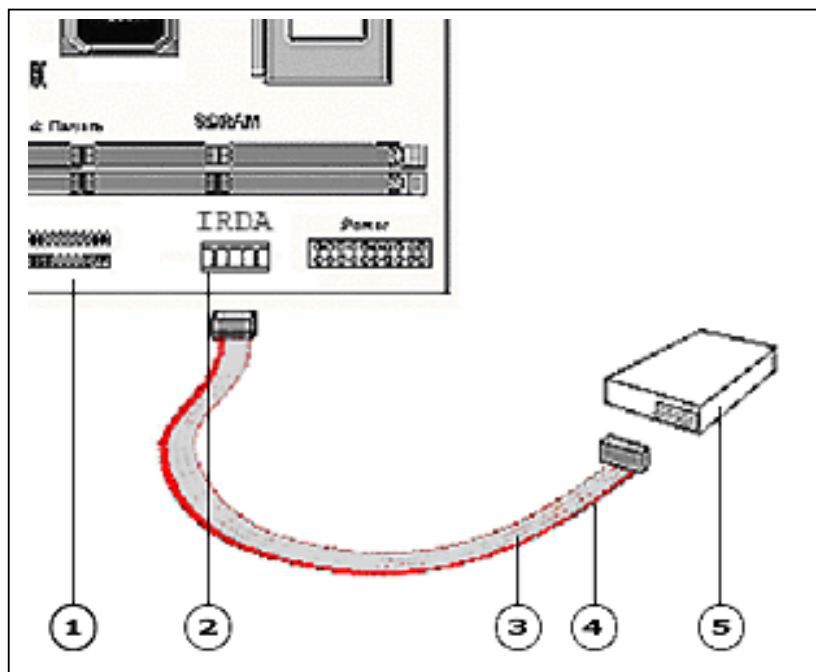


Схема 1. Подключения ридера к разъему Irda порта материнской платы:

1 – материнская плата; **2** – разъем порта Irda; **3** – соединительный шлейф;
4 – первый провод соединительного шлейфа; **5** – ридер.

Внимание ! Неправильное подключение ридера может вывести из строя как сам ридер так и выходы IRDA порта материнской платы.

После подключения ридера, необходимо провести настройку параметров в программе BIOS SETUP, для этого:

1. Перезагрузите компьютер.
2. Войдите в программу SETUP, для чего при загрузке компьютера, после появления в левом нижнем углу монитора приглашения: "Press **DEL** to input **Setup**", нажмите клавишу **Delete**. Вы попадете в меню **Setup**.

Примечание : Для перемещения по пунктам меню используйте клавиши «←», «↑», «→», «↓». Для входа в подменю используйте клавишу «Enter».

Ниже приведен пример настройки параметров для материнских плат Acorp с программой BIOS AWARD.

В подменю "Integrated peripherals" необходимо установить следующие опции:

Onboard Serial Port 2	[2F8/IRQ3]
UART Mode select	[IrDA]
RxD, TxD active	[Hi, Hi]
IR transmission delay	[Enabled]
UR2 Duplex Mode	[Full]
Use IR pins	[IR Rx2Tx2]

Примечание : Настройка параметров для материнских плат некоторых других производителей приведена в **ПРИЛОЖЕНИИ 1**. Настройка BIOS неуказанных производителей производится по аналогии с приведенными примерами.

Установка программного обеспечения

Программная часть системы SecureCard состоит:

- ПО **AdminTool** администратора сети – устанавливается на компьютер администратора сети.
- Клиентского ПО – подсистема входа и авторизации пользователя, устанавливаемого на компьютер пользователя.

Для установки ПО:

1. Вставьте компакт-диск в CD-ROM дисковод.
2. Корневой каталог компакт-диска содержит две папки, называемые AdminTool и Gina.
3. Для установки программного обеспечения следует запустить на исполнение файл SETUP.exe.
 - путь к установочному файлу программы AdminTool из корневого каталога компакт-диска следующий: **AdminTool \ DISK1 \ SETUP.exe**.
 - путь к установочному файлу подсистемы входа и авторизации пользователя из корневого каталога - **\ Gina \ DISK1 \ SETUP.exe**.
4. Во время установки программы AdminTool, вы можете указать директорию хранения программных файлов и изменить название программы. Для быстрого запуска программа AdminTool автоматически размещается в меню **Программы** главного меню системы **Пуск**.
5. После установки программного обеспечения перезагрузите компьютер.

Удаление (деинсталляция) программного обеспечения системы SecureCard

Удаление программы AdminTool осуществляется с помощью пункта «Установка и удаление программ» меню Панели управления ОС Windows.

Для удаления ПО подсистемы входа и авторизации пользователей следует выбрать пункт Uninstall в меню Gina. Путь: **Пуск \ Программы \ Gina \ Uninstall**.

Работа с системой "SecureCard"

Программа AdminTool

Программа AdminTool предназначена для регистрации пользователей, записи и управления картами пользователей в сети. Программа AdminTool позволяет производить необходимые манипуляции с картами пользователей. Так же для удобной и полноценной работы, в программе реализованы некоторые функции администратора сети ОС Windows, такие как регистрация пользователей сети, разрешение и запрещение входа пользователя в сеть. Дополнительные атрибуты пользователю устанавливаются с помощью инструментов администратора сети ОС Windows.

Функции, реализованные в программе AdminTool:

- Регистрация пользователя;
- Запись карты пользователя;
- Смена пароля пользователя;
- Блокирование карты и запрещение входа в систему;
- Удаление пользователя и очистка карты.

Работа с программой AdminTool

Вход в систему

Для работы с программой AdminTool, Вам следует войти в систему, не используя карты, а ввести пароль с клавиатуры. Поэтому после загрузки компьютера, нажмите последовательно клавиши Ctrl + Alt + Delete. Появится стандартное окно, приглашающее к вводу имени и пароля.

Войдя в систему, запустите программу AdminTool на исполнение – путь: Пуск \ Программы \ AdminTool \ AdminTool.

Главное окно программы

Главное окно программы (Рис.1) включает панель инструментов и два поля.

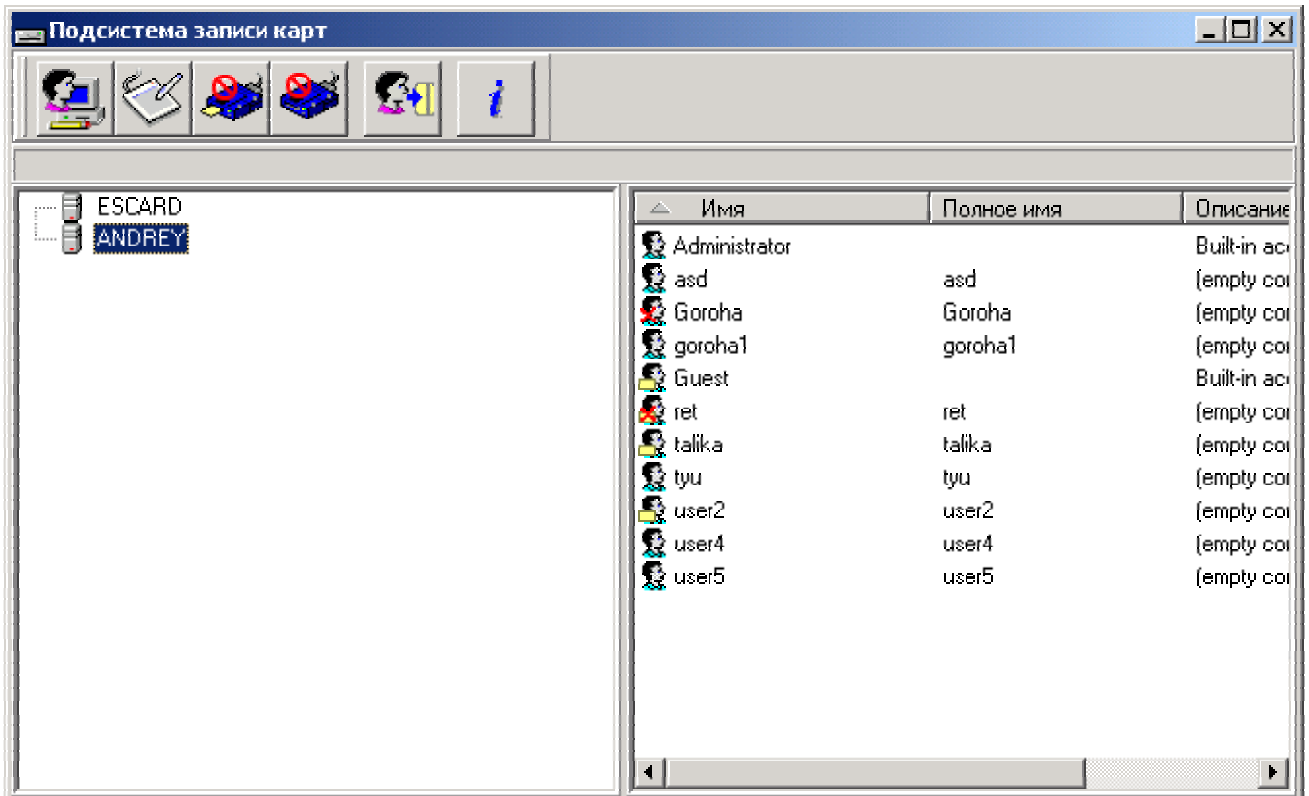








Рис. 1



Панель инструментов, располагающаяся в верхней части окна, состоит из шести кнопок. Для того чтобы определить команду, выполняемую кнопкой, наведите на неё указатель мыши. В строке ниже появится сообщение, содержащее команду.



Назначение кнопок панели инструментов:

-  - создание нового пользователя в текущем домене и запись карты;
-  - смена пароля пользователя и запись пароля на карту;
-  - удаление пользователя и очистка карты;
-  - удаление пользователя из базы данных и запрещение входа пользователя в систему;
-  - запись карты для существующего пользователя;
-  - считать имя пользователя.

Левое поле окна содержит список доменов сети, каждый пользователь сети регистрируется только на одном домене.

Правое поле окна содержит список имен пользователей, зарегистрированных в текущем домене. Каждое имя пользователя помечено соответствующей пиктограммой, позволяющей быстро определить: имеет ли пользователь карту и доступ в сеть.


Вход пользователя разрешен:
 пользователь имеет карту
 пользователь не имеет карты

Вход пользователя запрещен:
 пользователь имеет карту входа
 пользователь не имеет карты

Создание нового пользователя

Операция регистрации пользователя и запись его карты производится программой последовательно, т.е. сначала происходит регистрация пользователя, а затем запись его карты. Это дает возможность зарегистрировать пользователя, как при наличии карты, так и без неё.

Регистрация пользователя и запись карты

1. В главном окне программы укажите домен, в котором будет зарегистрирован пользователь.
2. Далее вставьте карту в ридер.
3. На панели инструментов нажмите кнопку .
4. В открывшемся окне в поле Пользователь введите сетевое имя пользователя, в поле Примечание можете внести дополнительную информацию о регистрируемом пользователе (его фамилию, имя, должность и пр.).

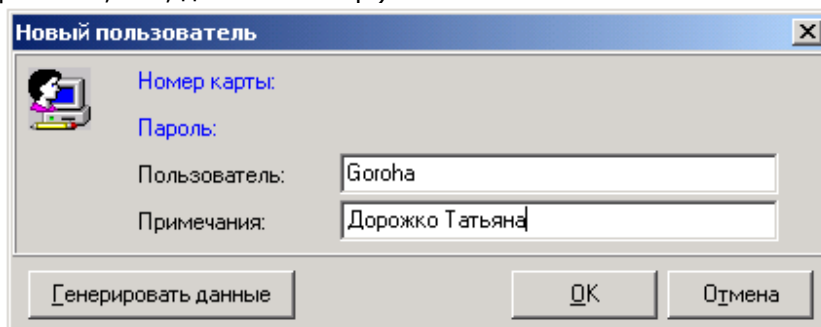


Рис. 2

5. Нажмите кнопку **Генерировать данные**, программа сгенерирует пароль и номер карты. После завершения операции, в окне (Рис.3) в поле Номер будет выведен номер карты, а в поле Пароль слово Генерирован.

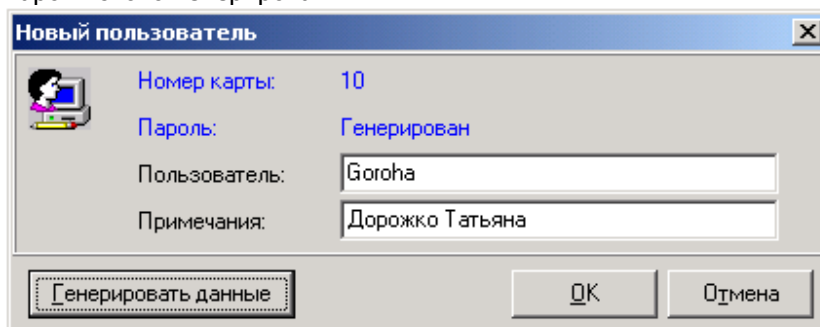


Рис. 3

6. Теперь следует зарегистрировать пользователя и записать данные на карту, для этого нажмите **OK**.

Программа проверит уникальность имени пользователя в сети и сообщит о выполнении операции

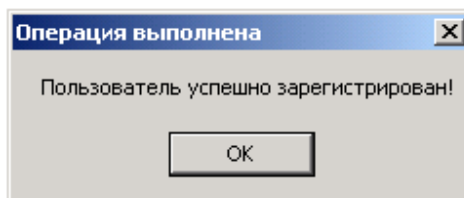


Рис.4

Затем, будет произведена запись карты пользователя. Имя нового пользователя появится в списке пользователей текущего домена.

Регистрация пользователя без наличия карты

1. Укажите домен, на котором будет зарегистрирован пользователь.

2. Нажмите кнопку 

3. Перед Вами откроется окно (Рис.5), введите сетевое имя пользователя, а в поле Примечание внесите дополнительную информацию о пользователе (его фамилию и имя, должность и пр.).

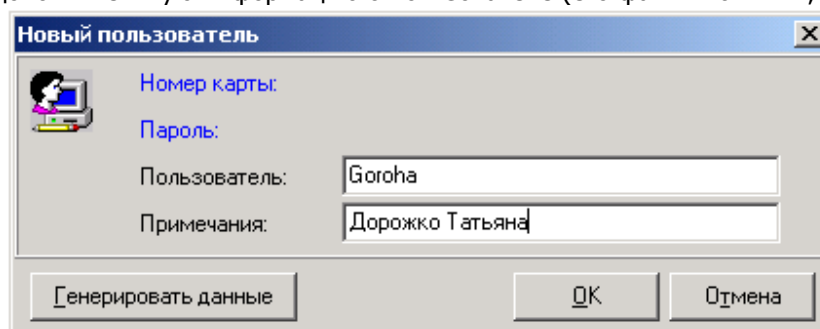


Рис.5

4. Нажмите кнопку с надписью **Генерировать данные**, программа сгенерирует номер карты и пароль пользователя и заполнит соответствующие поля окна.

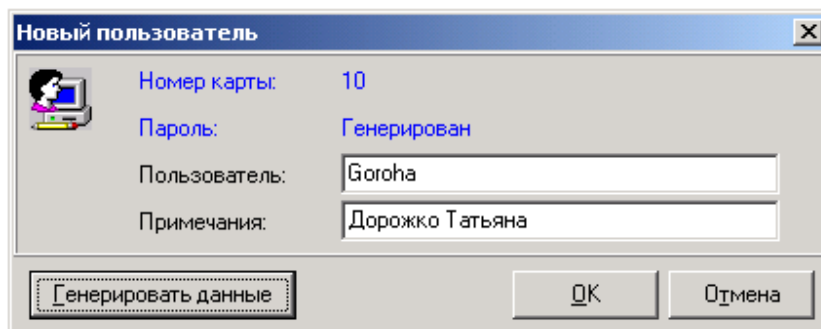


Рис.6

- Нажмите **OK**, программа проверит уникальность имени пользователя в сети и сообщит о выполнении операции

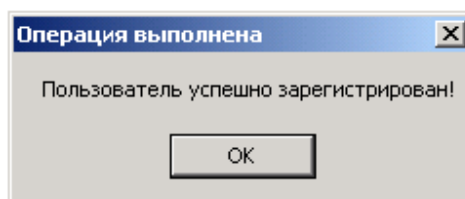


Рис.7

- Далее, программа будет пытаться произвести запись данных на карту. Не обнаружив карту в ридере, программа выведет следующее сообщение об ошибке (Рис.8). Нажмите **OK**.

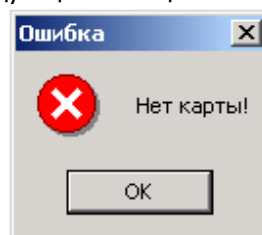




Рис.8

Операция регистрации пользователя будет завершена, его имя, помеченное пиктограммой , появится в списке пользователей текущего домена.

Примечание: Произвести запись карты для данного пользователя можно позже (см. п. Запись карты для существующего пользователя).

Запись карты для существующего пользователя

Для того, что бы записать карту для существующего пользователя:

- Вставьте карту в ридер.
- Укажите пользователя.
- Нажмите кнопку  или щелкните правой кнопкой мыши на имени пользователя.

Раскроется контекстное меню (Рис.9) выберите соответствующую команду.

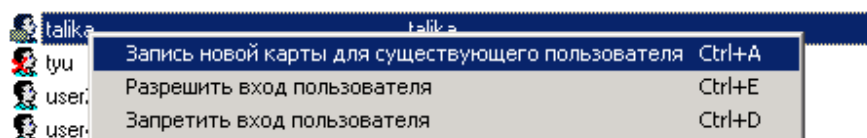


Рис.9

В результате, программа сгенерирует номер карты и пароль пользователя, произведет запись карты и сообщит об успешном завершении операции.

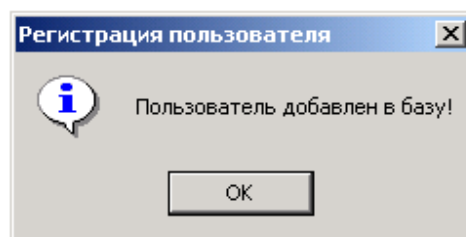


Рис.10

Нажмите **ОК**.

Изменение владельца карты

При записи карты для регистрируемого Вами пользователя или при записи карты для существующего пользователя, Вы можете воспользоваться картой, принадлежащей другому пользователю. В этом случае, будет выведено предупреждение (Рис.11) и запрос на удаление из базы данных программы текущего пользователя карты.

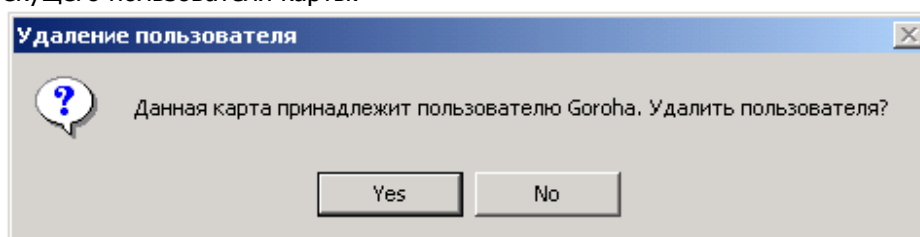


Рис.11

В случае отрицательного ответа, операция будет завершена, перезапись данных карты произведено не будет и карта останется за прежнем владельцем.

Если Вы ответили положительно, текущий владелец карты будет удален из локальной базы данных программы, а его карта очищена. Далее, программой будет выведен запрос на запрещение входа данного пользователя в сеть.

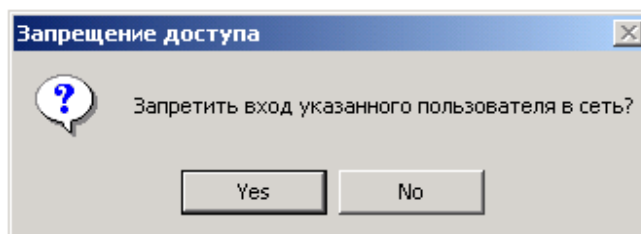


Рис.12

В зависимости от Вашего ответа, вход в сеть удаленного пользователя будет либо запрещен, либо разрешен соответственно.

В результате, на карту, прежнем владельцем которой являлся удаленный пользователь, будут записаны данные нового пользователя.

Смена пароля пользователя

Чтобы сменить пароль пользователя:

1. Вставьте карту в ридер.
2. Воспользуйтесь кнопкой



3. Программа сгенерирует новый пароль и произведет запись карты, сообщит об успешном завершении операции.

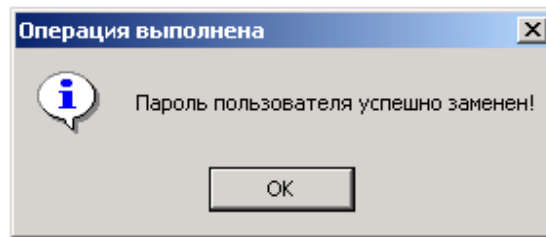



Рис.13

Определение владельца карты

Для того чтобы определить владельца карты:

1. Вставьте карту в ридер.
2. И воспользуйтесь кнопкой 

На экране монитора появится сообщение (Рис.14), содержащее имя владельца карты.

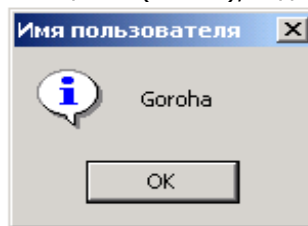



Рис.14

Удаление пользователя и очистка карты

Для того чтобы удалить пользователя:

1. Вставьте карту пользователя в ридер.
2. Нажмите кнопку 

Программа удалит пользователя из локальной базы программы, очистит карту и сообщит об успешном завершении операции.

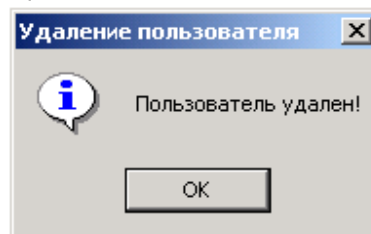



Рис.15

Удаление пользователя без наличия карты

Данная функция программы дает возможность удалить пользователя, карта которого утеряна или испорчена и не пригодна для чтения. Вы можете заблокировать карту пользователя, удалив его из локальной базы программы, а так же можете запретить вход пользователя в сеть.

Для того чтобы удалить пользователя, не имея в наличии его карты:

1. Нажмите кнопку 

Перед Вами откроется окно (Рис.16), содержащее список пользователей, входящих в сеть по карте.

Список пользователей			
Номер карты	Пользователь	Описание	Домен
2	User1		ASGARD
4	carder3		\\ESCARD2
5	carder2		\\ESCARD2
7	user5		ANDREY
8	user3		ANDREY
9	Goroha		ANDREY

Рис.16

- Укажите имя пользователя и нажмите кнопку **Удалить**. Программа потребует подтверждения в проведении операции.

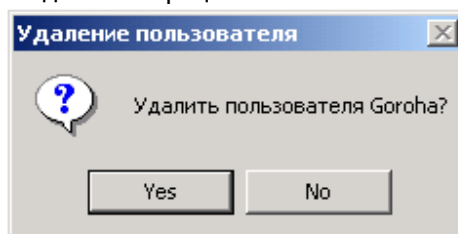


Рис.17

- В случае отрицательного ответа, операция будет завершена. Если Вы ответили положительно, программа удалит пользователя из локальной базы, а его карта будет заблокирована.
- Далее, программой будет выведен запрос на запрещение входа данного пользователя в сеть.

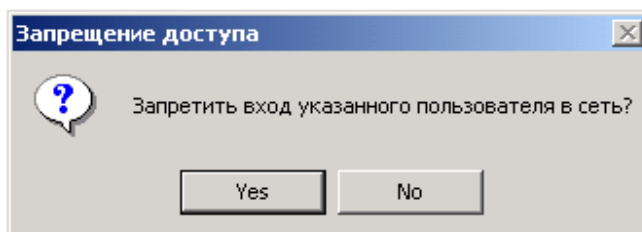


Рис.18

Если Вы ответили положительно, в результате проведенной операции, пользователь будет удален из локальной базы данных, его карта будет заблокирована, вход в сеть запрещен. Программа сообщит об успешном завершении операции.

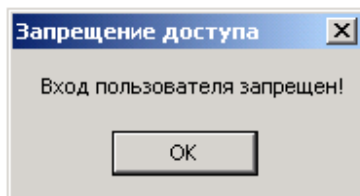




Рис.18



В случае отрицательного ответа, в результате проведенной операции, пользователь будет удален из локальной базы данных программы, его карты будет заблокирована, вход в сеть для данного пользователя запрещен не будет.

Примечание: Под блокированием карты в данном случае понимается блокирование входа указанного пользователя в сеть по карте.

Запрещение/разрешение входа пользователя

Определить запрещен или разрешен вход в сеть данного пользователя можно с помощью пиктограммы, которой помечено его имя:

Вход пользователя разрешен:
 пользователь имеет карту
 пользователь не имеет карты

Вход пользователя запрещен:
 пользователь имеет карту входа
 пользователь не имеет карты

Для того чтобы запретить/разрешить вход пользователю:

1. На имени пользователя щелкните правой кнопкой мыши.
2. В открывшемся контекстном меню выберите соответствующую команду.

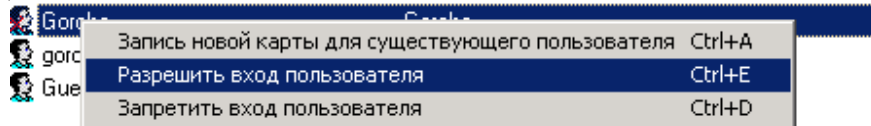


Рис.19

В результате, программа сообщит о завершении операции и имя пользователя в списке будет помечено соответствующей пиктограммой.

Подсистема входа в сеть и авторизации пользователя

Данная программа заменяет стандартную подсистему ОС Windows авторизации и входа пользователя в сеть и обеспечивает вход пользователя по смарт-карте.

Смарт-карта пользователя регистрируется администратором сети. При регистрации на карту записывается идентификационная информация пользователя: номер карты, имя пользователя и пароль. С помощью данной программы и устройства чтения/записи смарт-карт, установленных на компьютер пользователя, информация автоматически считывается с карты и осуществляется вход пользователя с сеть.

Особенности работы с подсистемой входа в сеть и авторизации пользователя

Вход в систему при помощи смарт-карты

После загрузки системы, на экран монитора будет выведено

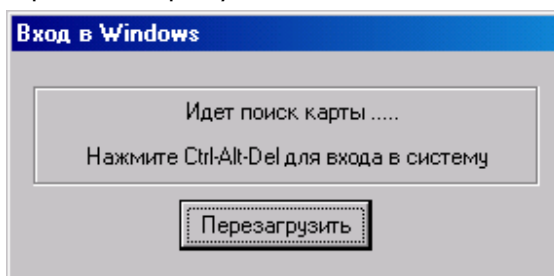


Рис.20

Вставьте карту в ридер, будет произведено считывание пароля с карты и осуществлен вход в систему.

Примечание: Карта вставляется контактами микросхемы вверх.

Блокирование компьютера

Если необходимо прервать сеанс работы на компьютере, выньте карту из ридера. Компьютер будет заблокирован и не доступен для других пользователей, на экране монитора появится окно, сообщающее об этом

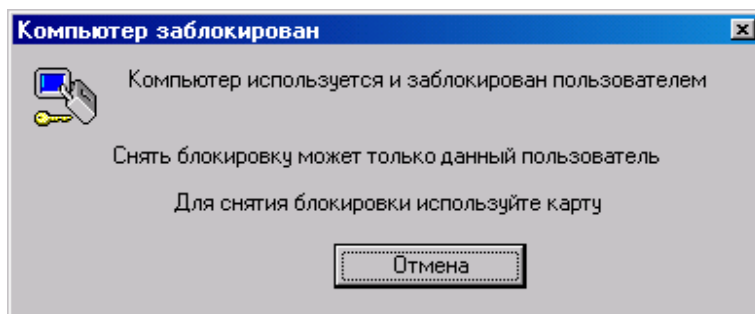


Рис.21

Разблокировать компьютер можно, вставив карту в ридер. Разблокировать компьютер можно только той картой, которой он был заблокирован. При попытке разблокировать компьютер другой картой, в выполнении действия будет отказано.

Выход из системы

Выход из системы осуществляется стандартным способом через кнопку **Пуск**, в меню выберите команду **Завершение сеанса**.

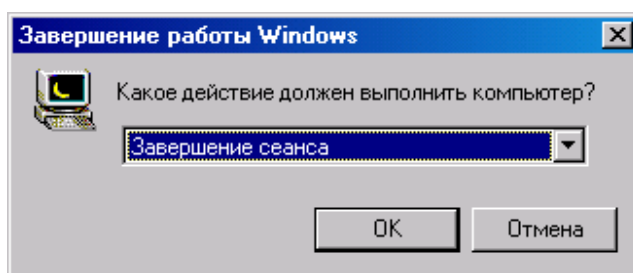


Рис.22

На экране монитора появится сообщение. Выньте карту и выключите компьютер.

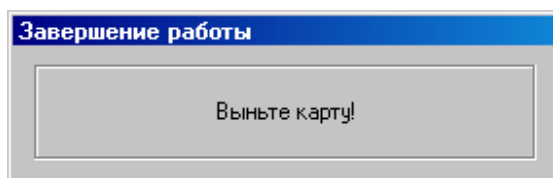


Рис.23

Список возможных ошибок

При проведении различных операций с картой пользователя могут возникнуть следующие ошибочные ситуации.

При создании нового пользователя:

1. Пользователь с таким именем зарегистрирован в сети, будет выведено сообщение об ошибке (Рис.24). В регистрации пользователя будет отказано.

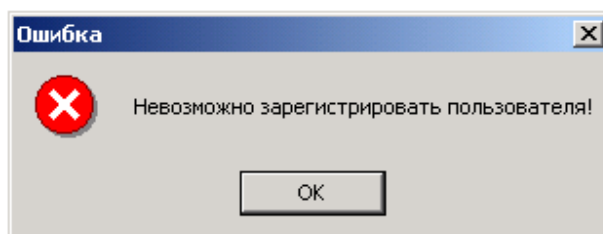


Рис.24

2. При записи карты пользователя, карта может быть не правильно вставлена в ридер, в этом случае будет выведена ошибка (Рис.25)

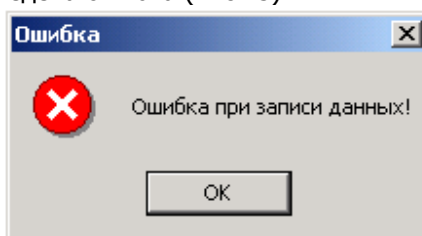


Рис.25

Так как операция регистрации пользователя и запись карты производится последовательно, в этом случае, пользователь будет зарегистрирован в текущем домене, но запись данных на карту не будет произведена. Записать карту для данного пользователя можно позже (см. п. Запись карты для существующего пользователя).

При смене пароля пользователя:

1. Карта не вставлена в ридер - появится сообщение (Рис.26). Вставьте карту и повторите попытку.

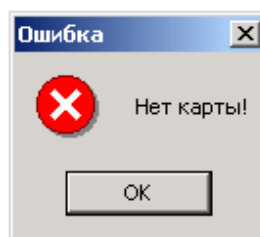


Рис.26

Примечание : Карта вставляется в ридер контактами микросхемы вверх.

2. Карта не зарегистрирована в сети - появится сообщение (Рис.27). В проведении операции будет отказано.

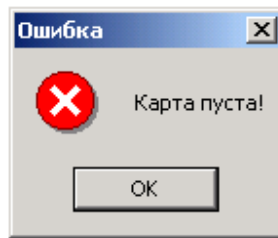


Рис.27

3. Карта принадлежит пользователю, удаленному из локальной базы программы или карта пользователя повреждена. В этом случае, будет выведено сообщение (Рис.28) и в проведении операции будет отказано.

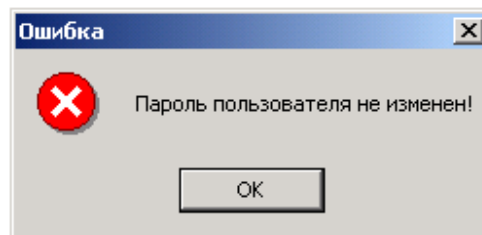


Рис.28

При удалении пользователя при наличии карты:

1. Карта не вставлена в ридер - появится сообщение (Рис.29). Вставьте карту в ридер и повторите попытку.

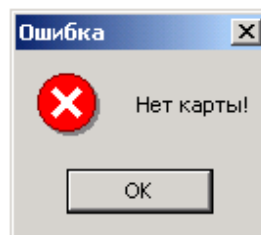


Рис.29

2. Карта не зарегистрирована в сети - появится сообщение (Рис.30). В проведении операции будет отказано.

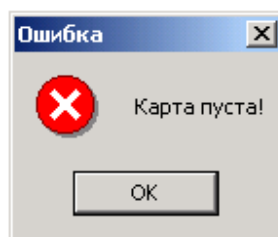


Рис.30

3. Карта принадлежит пользователя, удаленному из локальной базы программы. В этом случае, будет выведено сообщение (Рис.31) и в проведении операции будет отказано.

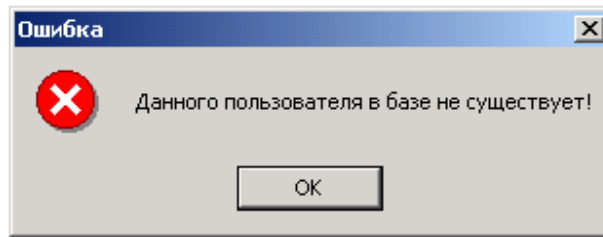


Рис.31

При попытке входа в сеть:

1. Карта не зарегистрирована в системе – появится окно (Рис.32). Обратитесь к администратору сети.

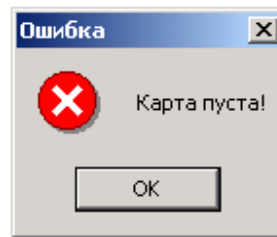


Рис.32

2. Карта не правильно вставлена в ридер - появится окно с сообщением (Рис.33), выньте карту и повторите попытку, вставляя карту внимательней.

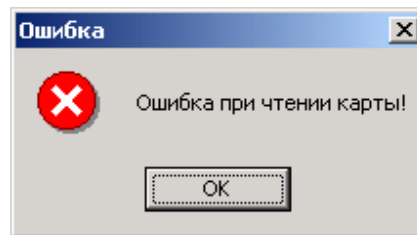


Рис.33